Diversitas Journal
ISSN 2525-5215
Volume 11, Number Special 1 (Mar./Apr. 2026) p. 088 – 101
https://diversitasjournal.com.br/diversitas_journal

Application of Data Security Models in Zero - Trust Architecture from the Data Assets Perspectives

HU, Fangshu[1]; FESTIJO, Jessa Frida T.[2]

[1] 0009-0007-1983-2586; Lyceum of the Philippines University, Manila, Philippines. fangshu.hu@gmail.com
[2] 0000-0003-3612-0277; Doctor of Philosophy, Lyceum of the Philippines University, Manila, Philippines. frida.festijo@lpu.edu.ph

A B S T R A C T

Today, data assets have become the core assets of enterprises and organizations, and their security is of utmost importance. The traditional network security architecture has revealed many limitations in protecting data assets, giving rise to the zero - trust architecture. This paper deeply analyzes the data security model of the zero - trust architecture from the perspective of data assets, and elaborates on its design key points, including data classification and grading, identity and access management, etc. At the same time, it explores its applications in scenarios such as enterprise data centers and cloud computing, analyzes the challenges in technology, management, and legal compliance during the implementation process, and proposes corresponding countermeasures. The aim is to provide a reference for enterprises and organizations to protect the security of data assets. Traditional network security architectures revealed significant limitations in protecting data assets, particularly in an increasingly interconnected and global environment. The need for zero-trust architecture has emerged as a promising paradigm, highlighting the "never trust, always verify" principles to ensure data assets security. The study investigates the application of zero-trust architecture in practical scenarios, including enterprise data centers and cloud computing environments, etc, which are increasingly critical in modern IT infrastructures. It also explored on the challenges that organizations faced in implementing zero-trust architecture, especially in areas of technology, management, and legal compliance. To address these issues, the paper proposed countermeasure mechanisms that support sustainable and resilient operations in the digital age.

ARTICLE INFORMATION

Article process:
Submitted: 11/25/2025
Approved: 03/13/2025
Published: 03/15/2025

Keywords:
data assets; zero-trust architecture; data security model; access control; security policy

RESUMO

Atualmente, os dados se tornaram ativos essenciais para empresas e organizações, e sua segurança é de suma importância. A arquitetura tradicional de segurança de rede revelou diversas limitações na proteção de dados, dando origem à arquitetura de confiança zero. Este artigo analisa profundamente o modelo de segurança de dados da arquitetura de confiança zero sob a perspectiva dos dados, detalhando seus principais pontos de projeto, incluindo classificação e gradação de dados, gerenciamento de identidade e acesso, entre outros. Ao mesmo tempo, explora suas aplicações em cenários como data centers corporativos e computação em nuvem, analisa os desafios tecnológicos, de gestão e de conformidade legal durante o processo de implementação e propõe contramedidas adequadas. O objetivo é fornecer uma referência para que empresas e organizações protejam a segurança de seus dados.

As arquiteturas tradicionais de segurança de rede revelaram limitações significativas na proteção de ativos de dados, particularmente em um ambiente cada vez mais interconectado e global. A necessidade de uma arquitetura de confiança zero emergiu como um paradigma promissor, destacando os princípios de "nunca confiar, sempre verificar" para garantir a segurança dos ativos de dados. Este estudo investiga a aplicação da arquitetura de confiança zero em cenários práticos, incluindo data centers corporativos e ambientes de computação em nuvem, que são cada vez mais críticos nas infraestruturas de TI modernas. Também explorou os desafios que as organizações enfrentam na implementação da arquitetura de confiança zero, especialmente nas áreas de tecnologia, gestão e conformidade legal. Para abordar essas questões, o artigo propõe mecanismos de contramedida que apoiam operações sustentáveis e resilientes na era digital.

Keywords:
ativos de dados; arquitetura de confiança zero; modelo de segurança de dados; controle de acesso; política de segurança

DOI: 10.48017/dj.v11iSpecial_1.3741

Introduction

At present, under the application and promotion of mobile Internet and digital technology, the data generated by enterprises using the Internet of Things, the data generated by using artificial intelligence, and the data generated by enterprises' own operations are growing rapidly, which promotes the exponential growth of enterprises' data assets. Data assets are the most important core assets of enterprises, and digital assets have become the key to enterprises' core competitiveness.According to IDC's forecast, the total data volume will reach 175ZB by 2025 (IDC, 2024). The data assets owned by enterprises will directly determine the success or failure of the enterprise, and determine the key to its development and improvement of core competitiveness. Therefore, the security of data assets will also become the most important research topic.

However, in the face of increasingly complex network environments and multi-mode complex architectures in network construction, as well as the continuous upgrading of attack techniques and methods. The traditional boundary based security protection mode can no longer meet the security protection requirements of enterprise data assets. The traditional security mode based on "internal trust" has exposed obvious deficiencies and shortcomings. This mode defaults to the security of data assets that are logically isolated within the enterprise. However, with the advancement of technology, this model clearly has vulnerabilities that do not take into account internal behaviors such as abuse of internal personnel permissions and malicious tampering, as well as external behaviors such as emerging attack methods and security threats.

Both internal and external actions may lead to the leakage of enterprise data assets. According to IBM statistics, approximately 30% of data breaches are caused by internal personnel (IBM, 2024). Nowadays, it is difficult for enterprises to restrict the improper operation or intentional leakage of enterprise data assets by internal personnel using traditional network security protection architecture and network environment, nor can they effectively prevent external hackers from exploiting various vulnerabilities for attacks. Among them, the control of internal personnel is the most difficult, often due to inadequate internal monitoring. They use legitimate identities to access core data assets and intentionally engage in improper operations, resulting in the leakage of enterprise data assets. Therefore, the traditional boundary based security model is no longer able to protect the security of enterprise data assets, which has led to the birth of zero trust architecture.

Zero Trust Architecture (ZTA) utilizes an advanced network security architecture of "never trust, always verify" to conduct strict identity authentication and continuous verification checks from the perspectives of users, devices, applications, and network access, completely abandoning the traditional network boundary security model. It adopts the principle of minimum privilege, micro segmentation, and real-time monitoring to deal with

internal and external risks, and only compliant devices can access specific enterprise data assets during designated periods. At the same time, fine-grained access control technology is used to accurately set permissions for individual files or API interfaces, greatly reducing the risk of data leakage. Then, a dynamic authentication mechanism is integrated with multiple verification dimensions such as user behavior characteristics, device security status, and access time and space to achieve real-time evaluation of user credibility.

At the same time, a continuous risk monitoring system and situational awareness system are used to monitor potential threats throughout the entire lifecycle of access. When a change in risk level is detected, permissions are immediately adjusted to mitigate potential threats. The zero trust architecture effectively addresses internal threats, external attacks, and security challenges through advanced technology, multiple verifications, and a combination of effective monitoring, safeguarding enterprise data assets.

This paper examined the design principles and application scenarios of ZTA's data security models from the unique perspective of data assets, integrating the latest global research advancements. It analyzes implementation challenges in detail and proposes targeted countermeasures. The goal is to provide enterprises with systematic theoretical references for building highly resilient data security systems, enabling practical and effective application of ZTA to safeguard data assets. It addressed the issue by fortifying the security foundation for enterprises undergoing digital transformation and sustainable development.

Overview of Zero-Trust Architecture

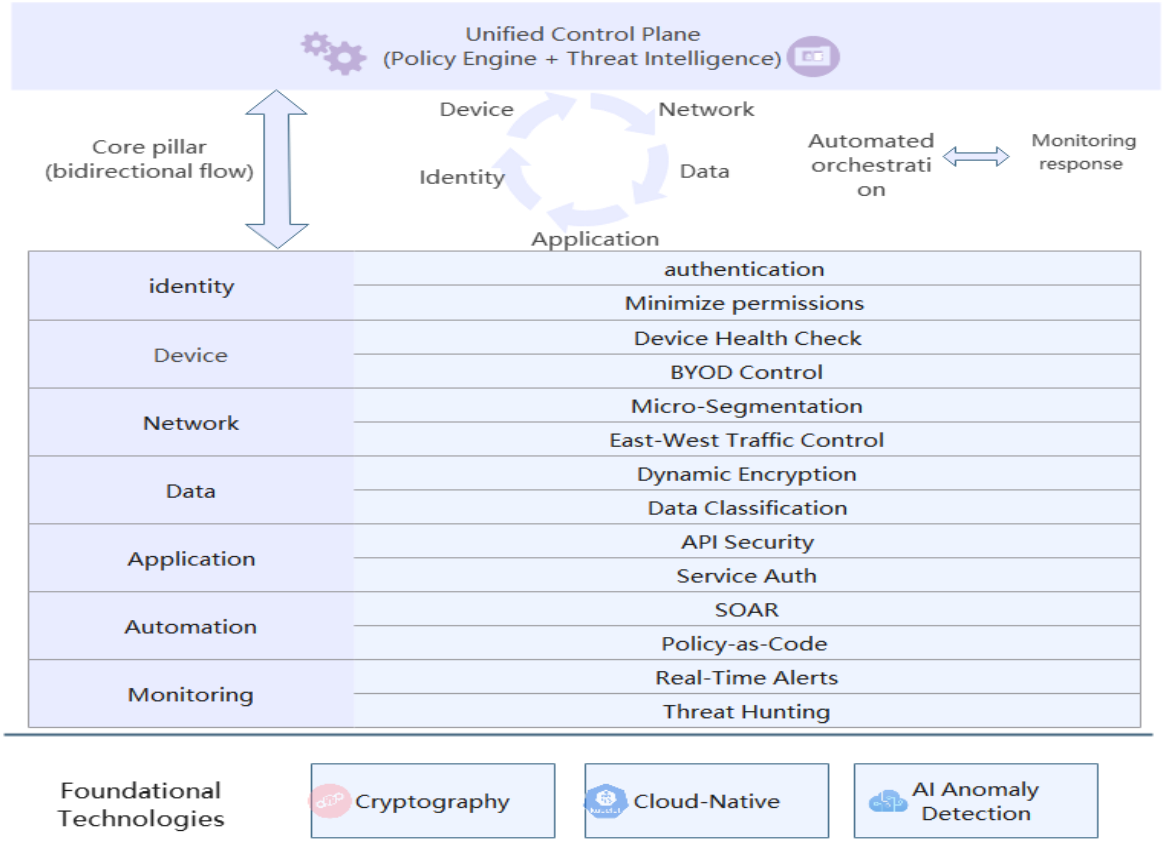
The concept of Zero Trust Architecture (ZTA) was first proposed by Forrester analyst John Kindervag in 2010 (Kindervag, 2010). Its core philosophy eliminates default trust in internal and external networks, requiring dynamic verification for all access requests. It assumes a significant role in network security by moving away from the traditional perimeter-based approach. The National Institute of Standards and Technology (NIST) further defined seven pillars of ZTA in SP 800-207: user, device, network, data, application and workload, automation and orchestration, and monitoring and response (NIST, 2020). Primary mechanisms include strong identity and access management (MFA, behavior-based authentication), micro-segmentation, encryption, and real-time analytics to detect anomalies and limit lateral movement (Ejiofor et.al, 2025; Alebiosu et.al, 2025).

The seven pillars of ZTA provide objective lens and verifiable process to ensure that processes undergo through continuous authentication, contextual policy enforcement, and real-time monitoring. The identity pillar guides how users are authenticated, authorized, and governed over time. Rigorous authentication and authorization processes for all users, services, and devices are necessary to enforce least privilege for every request (Ejiofor et.al, 2025). Multi-factor authentication (MFA) and risk-based adaptive policies dynamically adjust

access privileges based on contextual factors such as geolocation, time, and behavioral patterns. In terms of technical implementation, identity federation protocols (e.g., OAuth 2.0, SAML) and continuous trust evaluation are widely deployed through behavioral analytics to adjust authorization privileges.

Figure 1.

The Seven Pillars of Zero-Trust Architecture



The device pillar focuses on validation of trustworthiness of endpoints connected to the network before granting access. There is a need for continuous diagnostics systems that will monitor devised and feed data into policy engines so that access decisions changes as device risk changes (Cao et.al, 2024; Prajapati, 2025). For technical implementation, boot mechanisms, hardware-based root of trust, and endpoint telemetry collection must be secured for real-time device posture assessment.

The network pillar represents another critical dimension of ZTA fundamentally redefining how connectivity and communication are managed within digital infrastructures. Rather than relying on perimeter firewalls and trusted internal networks, it adopts micro segmentation strategies that divide networks into smaller, isolated security zones.

Traffic between segments is brokered through policy enforcement points, with encryption in transit and strict control of east-west movement to reduce lateral spread of attacks Syed et.al, 2022). Software-defined networking (SDN) for policy-driven traffic

isolation, and zero-trust network access (ZTNA) to replace traditional VPNs with context-aware connectivity (Pokhrel et.al, 2025).

The application pillar focuses on application-centric policies that ensure only authorized users and services can invoke specific APIs or functions, limiting exploitation of vulnerable components. Dynamic access controls are based on application sensitivity and runtime behavior, ensuring workloads operate within predefined security boundaries (Pokhrel et.al, 2025). It works for service meshes for mutual TLS (mTLS) enforcement, and runtime security controls embedded directly into application code.

The data pillar involves classification, encryption, and lineage tracking of data at rest, in transit, and during processing. It involves automated data labeling using machine learning, quantum-resistant encryption algorithms, and distributed ledger technologies for immutable audit trails. Automation and orchestration coordinate policy-as-code, configuration, and response across all other pillars (Prajapati 2025).

Security orchestration platforms integrate threat intelligence, automate incident response workflows, and optimize remediation actions. AI-driven policy enforcement and threat response reduces reliance on manual intervention. Visibility and analytics aggregate logsand behavioral data from identities, devices, networks, applications, and data flows. Centralized analytics—often AI-driven—perform anomaly detection, identity analytics, and threat hunting to support continuous verification and rapid incident response (Oloumachi et.al, 2025; Syed et.al, 2022).

The core concept of "never trust, always verify" in the ZTA runs through the entire process of the seven pillars, and is transformed into practical security implementation strategies through the five core principles. These principles are interconnected and mutually supportive, jointly building a three-dimensional security protection architecture.

The transition from traditional perimeter-based security models to Zero-Trust Architecture introduces profound changes in how access control, trust validation, and network segmentation are implemented. One of the most significant shifts is the adoption of the principle of least privilege, which ensures that users and systems receive only the minimum access necessary to perform their tasks. In Zero-Trust environments, access decisions are context-aware and dynamically evaluated through mechanisms such as Attribute-Based Access Control (ABAC).

Unlike Role-Based Access Control (RBAC), which assigns static permissions to user groups, ABAC evaluates multiple attributes—including user identity, device health, data classification, and environmental conditions—to determine access eligibility. Additionally, Just-in-Time (JIT) access mechanisms grant temporary permissions for specific tasks and automatically revoke privileges once the activity is completed, thereby minimizing the risks associated with overprivileged accounts.

Methodological Procedures

This article systematically reviews and analyzes ZTA's data security model and its applications in various complex scenarios. A comprehensive literature search was conducted across over 170 million research papers using Consensus, where data search generated from academic databases such as Semantic Scholar, Sage, Science Direct, and PubMed.

The search strategy involved targeted queries on Zero Trust pillars and their role in addressing cybersecurity research gaps. In total, 1123 papers were identified; after screening for relevance and quality, 954 were screened further, 579 were deemed eligible, and the top 50 most relevant papers were included in this review. Eight unique search groups were used to ensure broad coverage of foundational models, critiques, adjacent frameworks (e.g., SASE), gap types (scalability, regulation), and interdisciplinary perspectives.

Results and Discussions

Design of Data Security Models in Zero-Trust Architecture

As a key component of ZTA, data classification and grading form the foundation of dynamic security policies. The traditional static classification methods that relied on manual labeling one by one in the past are no longer able to meet the dynamic characteristics and complex requirements of modern data ecology.

Therefore, a neural network-based real-time classification engine has proposed a new approach for dynamic data classification. The engine can build an association graph architecture based on the associations between users, documents, and devices, and update classification labels in real-time according to specific contexts. For example, if a financial document is frequently accessed across departments, the real-time classification engine of the neural network will automatically raise its security level from "internal" to "confidential", thereby initiating a more rigorous access control process. Therefore, the real-time classification engine of neural networks is the key to dynamic data classification, and it is crucial to study the pattern of the real-time classification engine of neural networks.

The real-time classification engine of neural networks dynamically adjusts data labels by integrating contextual data such as access frequency, user behavior patterns, and business scenarios. For example, in the financial industry, when a customer transaction detail data is used for cross regional utilization, the real-time classification engine of the neural network will automatically adjust it from the "ordinary internal" label to the "high-sensitivity business" label based on the transaction amount, transaction region, and other business context

information involved in the transaction detail data. The tag change will be linked to the corresponding access control policy and immediately respond. In addition to regular identity verification, it will also trigger a secondary verification of the visitor's business operation qualifications.

Only personnel who pass the verification can continue to access transaction data. Dynamic data classification and labeling analyze the content of the data itself, as well as contextual information such as file metadata and access patterns, to distinguish data assets into different sensitivity levels such as public, internal, confidential, and restricted, and label them accordingly. Taking Microsoft Azure Web Tools as an example, it uses graph-based analysis methods to annotate data in real time, enabling policy execution to have situational awareness (Microsoft, 2023).

Table 1.

Advantages Over Traditional Methods

Aspect	***Traditional Methods***	***GCE-Driven Approach***
Adaptability	*Relies on predefined rules; struggles with new data types.*	*Dynamically adapts to evolving data relationships and threats.*
Accuracy	*Prone to human error and oversights in labeling.*	*Automates classification using AI, reducing mislabeling by 60% (AWS, 2023).*
Scalability	*Limited to structured data and small-scale systems.*	*Handles petabytes of unstructured data across hybrid environments.*
Response Time	*Manual policy updates take hours or days.*	*Real-time label adjustments and policy enforcement (sub-second latency).*

Dynamic Identity and Access Management (IAM)

The ZTA has achieved a breakthrough transformation from traditional patterns to behavior driven authorization (BDA) in dynamic identity and access management. In the past, identity and access management, whether based on role-based access control (RBAC) or attribute access control (ABAC), relied on static permissions and preset attributes to complete, which makes them inadequate in addressing security challenges in today's complex environments. However, the BDA model is completely different. It dynamically calculates risks and flexibly adjusts access permissions by analyzing a series of user behaviors in real time, such as login time, operation frequency, device interaction mode, and contextual metadata (Mangla, 2025). For example, when a user repeatedly attempts to access sensitive databases with unauthenticated devices during non-working hours, even if their role permissions have

been approved, BDA will temporarily restrict access permissions and force multi factor authentication such as biometric verification (Yao et.al, 2020).

The core of BDA lies in comprehensive behavioral data collection and accurate risk assessment. Firstly, starting from the collection of behavioral data, capture fine-grained behavioral data from multiple channels such as devices, applications, and network traffic. At the same time, external signals such as geographic location, threat intelligence sources, project phases, and compliance requirements will be integrated to enhance context.

Then, through a risk scoring engine and advanced technologies such as machine learning, abnormal behavior is detected using its self-learning ability, and behavioral deviations are identified and calibrated (Liu et.al, 2025). The risk score is then calculated in real-time based on factors such as device compliance and credibility, operational necessity and criticality, and temporal context. Finally, the adaptive access control capability of dynamic policies is used to control risks. For high-risk operations such as accessing financial records, identity verification is gradually upgraded to trigger multi factor authentication or biometric checks.

In addition, BDA is integrated with an automated orchestration, monitoring, and response platform. Once a threat is detected, it automatically isolates or revokes permissions for the threatened account to minimize security risks (Liu et.al, 2025).

Table 2.

Comparative Analysis: BDA vs. Traditional Models

Criteria	RBAC/ABAC	BDA
Decision Basis	Static roles/attributes.	Real-time behavior and contextual risk.
Adaptability	Limited to predefined rules.	Dynamically adjusts to evolving threats.
False Positives	High (e.g., legitimate users blocked).	Reduced by 55% through AI-driven analytics (Darktrace, 2023).
Compliance Alignment	Manual audits required.	Automated logging and audit trails.

End-to-End Encryption and Data Lineage Tracking

The zero trust architecture utilizes advanced technologies such as blockchain to break the previous situation of passive protection to active traceability. Although end-to-end encryption can ensure data transmission security, it still faces problems such as key lifecycle management and cross domain data traceability.

To address this issue, quantum secure key encryption technology has shifted from traditional, self built models to cloud based and service-oriented approaches. It relies on

blockchain technology to host key usage logs on quantum secure hardware modules, fundamentally ensuring that keys are not tampered with (Hariharan, 2025).

At the same time, with the help of data traceability graph technology, such as the use of Neo4j, cross system tracking can be achieved, and the entire lifecycle of files flowing from the cloud to edge devices can be clearly depicted, and potential leakage risk points can be accurately marked.

Table 3.

Comparative Analysis

Aspect	Traditional E2EE	QS-KaaS + AI Lineage
Key Management	Manual rotation; vulnerable to quantum attacks.	Automated, quantum-safe rotation with blockchain auditing.
Data Visibility	Siloed logs; limited cross-system tracing.	Unified lineage graphs with AI-driven anomaly detection.
Compliance	Reactive audits; prone to gaps.	Proactive, blockchain-verified compliance.
Response Time	Hours to days for breach attribution.	Minutes via real-time graph analytics.

Continuous Monitoring and Adaptive Response

Existing security orchestration, automation, and response (SOAR) platforms depend on predefined rules, limiting their effectiveness against unknown threats. A generative adversarial network (GAN)-driven adaptive response system can simulate attacker behaviors, autonomously generate defense strategies, and validate their efficacy (Bhatt & Indra, 2024). A causal inference engine further prioritizes responses by analyzing causal relationships between security events (e.g., whether a data breach resulted from misconfigured permissions).

Table 4.

Comparative Analysis: Traditional vs. AI-Driven SOAR

Criteria	Rule-Driven SOAR	GAN + CIE-Driven SOAR
Threat Coverage	Limited to known IOCs/TTPs.	Detects novel and evolving threats.
Response Flexibility	Static playbooks require manual updates.	Dynamic playbooks adapt to attack evolution.
False Positives	High due to rigid rules.	Reduced by 40% via causal prioritization.
Compliance Alignment	Reactive compliance checks.	Proactive risk mitigation with audit trails.

Countermeasures on Technical and Organizational Challenges

1)Fragmented Data Environments. Enterprise data is scattered across on-premises systems, multi-cloud platforms, and edge nodes, forming "data silos" that hinder the implementation of unified policies. For example, unstructured data (e.g., logs, documents) lacks standardized labels, impeding the precise execution of dynamic access controls. To countermeasure, there must be a cross-platform data governance framework using metadata federation. For instance, develop lightweight data brokers (Data Brokers) to synchronize classification labels and permission policies across different storage systems in real time, ensuring seamless coverage of zero-trust rules (Khumar et.al, 2025).

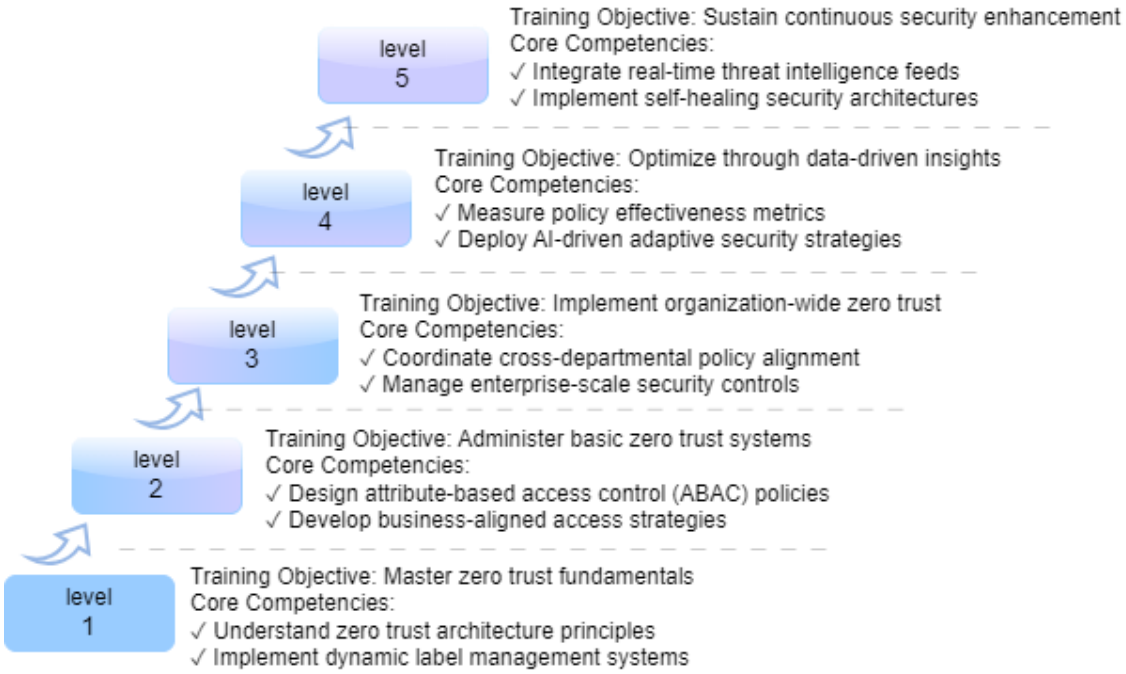
2)Real-Time vs. Security Trade-offs. Continuous verification mechanisms (e.g., dynamic permission checks occurring thousands of times per second) may introduce latency, particularly affecting user experience in high-concurrency scenarios such as financial transaction systems. To solve this, edge computing and distributed policy engines must be deployed to offload permission decisions to nodes closer to data sources. Additionally, adopt incremental verification (Incremental Verification), where full-process verification is triggered only for critical operations (e.g., exporting sensitive data), reducing system overhead.

3)Security vs. Business Agility. Zero-trust's strict controls may slow the pace of business innovation. For example, development teams frequently need to request permission adjustments to support new feature rollouts, leading to procedural rigidity. By embedding permission management rules into daily development processes and implementing a "Security-as-Code" model, permission rules can be automatically tested and deployed. In this way, security protection and rapid business iteration can develop in synergy (Adebayo et.al, 2023).

4)Skill Gaps. Nowadays, IT personnel are familiar with traditional boundary protection methods, but they are unable to handle the professional content of zero trust and fine control, which can lead to configuration problems or permissions exceeding actual needs, thus bringing security risks (Zhou et.al, 2023). There must be a zero trust capability maturity model, focusing on cultivating basic knowledge and skills in the initial stage, understanding and mastering the relevant knowledge points and applications of the zero trust capability maturity model in detail, and then gradually transitioning to higher-level strategy implementation to avoid problems caused by sudden changes in a gradual manner.

Figure 2.

Zero-Trust Capability Maturity Model (ZT-CMM)



5)Cross-Border Data Flow Regulations. Regional systems and requirements vary. Some countries require data to be stored locally, while others have proprietary requirements such as the EU's General Data Protection Regulation (GDPR). These systems and requirements limit the uniformity of zero trust architecture strategy design. Adopting a policy matrix flexible adaptation mechanism, utilizing digital twin technology are needed to simulate the compliance and compatibility of laws, and verifying relevant national policies in advance to ensure compliance with local legal requirements (Nadipalli, 2025).

6)Ambiguous Liability. The ZTA involves many stakeholders, so there is a possibility of data leakage for all parties involved. Therefore, a data leakage event may lead to liability disputes. Clear responsibilities of all parties through contracts or agreements should be enforced and then track and record the execution status and path of the terms, as well as related activities, through intelligent systems, so that disputes can be traced and responsibilities of all parties can be clearly defined.

.

Conclusions and Future Directions

This paper systematically analyzes ZTA's data security models and their applications in complex scenarios. Results demonstrate that ZTA revolutionizes data protection through dynamic access control, data classification, and end-to-end encryption. In addressing internal threats, lateral movement attacks, and cross-border data flow risks, ZTA exhibits exceptional

capabilities. ZTA has undergone significant changes compared to traditional boundary defense models. Following the principle of "never trust, always verify", the security focus is placed on the data itself. Through dynamic access control, data classification, continuous monitoring, and adaptive response capabilities, ZTA fundamentally changes the approach to data protection. In dynamic network environments, when dealing with internal and external threats, hacker attacks, and cross-border data flow security risks, the ZTA can fully meet security protection requirements.

However, the successful application of ZTA in complex scenarios is not an easy task and requires joint linkage and collaboration from various aspects such as technology, management, and law. Only by integrating dispersed data environments technically, comprehensively promoting and utilizing advanced machine learning and artificial intelligence technologies, can real-time operational efficiency and security protection be improved; Thoroughly address the imbalance and lack of coordination in data resource security and business collaboration development at the organizational level, while enhancing the team's professional and technical capabilities; From a legal perspective, challenges such as cross-border data flow regulations and liability ambiguities must be navigated. Only by comprehensively addressing these issues can ZTA achieve its full potential, establishing robust data security defenses for enterprises and organizations.

Funding Agency

The researchers like to thank the Research and Innovation Center of the Lyceum of the Philippines for funding the researchers' conference paper.

EFERENCES

Adebayo, A., Afuwape, A., Akindemowo, A., Erigha, E., Obuse, E., Ajayi, J., & Soneye, O. (2023). A Conceptual Model for Secure DevOps Architecture Using Jenkins, Terraform, and Kubernetes. International Journal of Multidisciplinary Research and Growth Evaluation. https://doi.org/10.54660/.ijmrge.2023.4.1.1300-1317.

Alebiosu, J., Anadozie, C., Ayodele, G., Abdulrahman, I., & Isaiah, T. (2025). Zero Trust Architecture: Beyond Perimeter Security – Implementing Continuous Authentication and Least Privilege Access. International Journal of Advances in Engineering and Management. https://doi.org/10.35629/5252-0704829841.

AWS. (2023).AWS Key Management Service Best Practices. https://aws.amazon.com/kms/

ARM. (2023). RISC-V Optimization for IoT Security. ARM Holdings.

Bhatt, R., & Indra, G. (2024). Detecting the undetectable: GAN-based strategies for network intrusion detection. International Journal of Information Technology, 16, 5231 - 5237. https://doi.org/10.1007/s41870-024-02172-7.

Cao, Y., Pokhrel, S., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. Machine Intelligence Research, 21, 294 - 317. https://doi.org/10.1007/s11633-023-1456-2.

Darktrace. (2023). AI-Driven Threat Detection Report.

Ejiofor, O., Olusoga, O., & Akinsola, A. (2025). Zero trust architecture: A paradigm shift in network security. Computer Science & IT Research Journal. https://doi.org/10.51594/csitrj.v6i3.1871.

FireEye. (2020). Sunburst: Sophisticated Cyber Espionage Attack. FireEye Threat Research.

Gartner. (2023). Market Guide for Zero Trust Network Access.

Hariharan, R. (2025). AI-Driven Identity and Access Management in Enterprise Systems. International journal of IoT. https://doi.org/10.55640/ijiot-05-01-05.

Istio. (2023). Service Mesh Security Documentation. https://istio.io/latest/docs/concepts/security/

IBM. (2023). Cost of a Data Breach Report. IBM Security.

IDC. (2023). Worldwide DataSphere Forecast, 2023–2027. International Data Corporation.

Kindervag, J. (2010). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research.

Kumar, A., Merlin, J., Jenitha, M., & Gladence, M. (2025). An Analysis on Generative Adversarial Networks Integrated Network Intrusion Detection System. 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), 707-714. https://doi.org/10.1109/icsadl65848.2025.10933451.

Liu, J., Kong, L., Yang, H., & Wang, Y. (2025). Adaptive Access Control Model Based on Activity and Trust in Social Internet of Things. Journal of Artificial Intelligence Practice. https://doi.org/10.23977/jaip.2025.080204.

Mangla, M. (2025). Behavioral Analytics and AI in Zero Trust Security: A Framework for Adaptive Identity and Access Management. International Journal Science and Technology. https://doi.org/10.56127/ijst.v4i1.2275.

Microsoft. (2023). Azure Purview Data Governance.https://azure.microsoft.com/en-us/products/purview

Nadipalli, R. (2025). Zero Trust Security Implementation Using DevSecOps in Cloud-Native Applications. International Journal of Computing and Engineering. https://doi.org/10.47941/ijce.3195.

NIST. (2020). SP 800-207: Zero Trust Architecture. U.S. Department of Commerce.

NIST. (2023). Post-Quantum Cryptography Standards. National Institute of Standards and Technology.

Prajapati, V. (2025). Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-23902.

Pokhrel, S., Li, G., Doss, R., & Nepal, S. (2025). Toward Decentralized Operationalization of Zero Trust Architecture for Next Generation Networks. IEEE Journal on Selected Areas in Communications, 43, 1998-2010. https://doi.org/10.1109/jsac.2025.3560039.

Siemens. (2023). IoT Security in Edge Computing. https://siemens.com/iot-security.

Syed, N., Shah, S., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, 57143-57179. https://doi.org/10.1109/access.2022.3174679.

Wang, Y., & Zhang, L. (2022). Consumer Preferences for Home Decoration Materials in Different Regions. Journal of Consumer Behavior Research, 18(3), 45-60.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2023). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.

Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic Access Control and Authorization System based on Zero-trust architecture. Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System. https://doi.org/10.1145/3437802.3437824.

Yue, S. & Qiang, Z. (2022). Analysis of Consumer Purchase decision-making Process in Home improvement Market. Monthly Journal of Market Research, 35 (6), 78-90.

Zhang S., & Li, S. (2023). Research on Market Trend of Aluminum Alloy Home Decoration Doors and Windows. Journal of Architectural Decoration Materials, 21 (2), 123-135.

Zhou, X., Mao, R., Zhang, H., Dai, Q., Huang, H., Shen, H., Li, J., & Rong, G. (2023). Revisit security in the era of DevOps: An evidence-based inquiry into DevSecOps industry. IET Softw., 17, 435-454. https://doi.org/10.1049/sfw2.12132.