Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.15, No.1, 2025

Overview of Zero Trust Architecture Trend and Advancement in Information Security

Mobolaji D. Ogunbadejo[1], Oluwatobi A. Ayilara-Adewale[2], Olanrewaju E. Alade[3]

1. Department of Information System Management, Stanton University, 888 Disneyland Dr #400, Anaheim, California 92802, USA.
2. Department of Information Technology, Osun State University, P.M.B. 4494, Oke Baale Road, Osogbo, Nigeria.
3. Department of Information System Management, Stanton University, 888 Disneyland Dr #400, Anaheim, California 92802, USA.

*Email address of the corresponding author: mogunbadejo24@stanton.edu

Abstract
Zero Trust Architecture (ZTA) has become a trending and revolutionary architecture in information security, transitioning from the conventional concept of perimeter security to a 'never trust, always verify' model. This study examines the concepts of ZTA, technological advancements and ZTA implementation in various sectors like finance, healthcare, and government. ZTA transformation technological innovation domains are 5G, the blockchain, and quantum computing, which define the future of ZTA adaptability. Similarly, this study aims to establish the role of ZTA in mitigating insider threats, its position on compliance with regulatory frameworks, and its relevance as a cybersecurity standard among various industries. Principles such as least privilege, continuous verification, encryption, least privilege, and multi-factor authentication allow ZTA to validate each access request quickly, regardless of the location. The evolution from the traditional security model tackles the susceptibilities inherent in remote access, cloud computing and mobile workforce. The ZTA technique has mitigated insider risks, lateral movement attacks and advanced persistent threats by imposing stern access control and continuous monitoring. ZTA enhances security environments and improves organization's tenacity since it enhances Least-Privilege access and real-time threat detection. This study seeks to establish how organizations can benefit from ZTA in safeguarding important assets in today's dynamic technological environment.
Keywords: Zero trust, inside threat**.** threats detection, cybersecurity, micro-segmentation, information security.
DOI: 10.7176/JIEA/15-1-03
Publication date: February 28th 2025

1. Introduction

One of the cutting-edge security frameworks founded on the tenet of "never trust, always verify" principle is the Zero Trust Architecture (ZTA). It works on the concept that threats can be present internally and externally in an organization's network; this creates a stance that trust should not be by default, even if the device or user is inside or outside the network (Tyler and Viana, 2021, Buck et al., 2021). The core principles in implementing ZTA are multi-factor authentication (MFA), least privilege, encryption, and continuous verification (Syed et al., 2022, Fernandez and Brazhuk, 2024). One technique for ensuring that only an authorized user has access is to use authentication, authorization, and encryption, which is enforced before access is granted to users or devices.

Perimeter-based security also called the conventional security model, depends significantly on creating a perimeter to prevent threats around a network (Makhdoom et al., 2018, Azad et al., 2024). These models adopt intrusion detection systems (IDS), virtual private networks (VPNs), and firewalls to guard an organization's internal assets. However, the evolution of the mobile workforce, cloud computing, and remote work has undermined this model's efficiency. As perimeter-based security becomes more vulnerable and flexible, cybercriminals can bypass external defences, and if successful, they often gain unrestricted access to critical resources (El-Amir, 2023, Bell et al., 2024). The rigid nature of perimeter-based security exposes an organization's vulnerability to internal threats, advanced persistent threats (APTs), and lateral movement attacks.

The rapid sophistication and occurrence of cyber threats demonstrate that the concept of perimeter security solutions is insufficient. Ransomware, data breaches, and phishing attacks have become more frequent, which exposes sensitive data even in a well-secured network (Puat and Abd Rahman, 2020, Abrera, 2024). The move towards cloud services, remote work, and bring-your-own-device (BYOD) policies, especially during and after the COVID-19 pandemic, has substantially expanded the attack surface (Bispham et al., 2021, Pósa and Grossklags, 2022, Rah, 2023). These trends explain why a proactive approach such as Zero Trust is urgent and

must continuously be adopted to verify and authenticate all access points concerning the device or location. However, Zero Trust handles these current-day dilemmas by applying the principle of no implicit trust, beginning with the initial step and extending to the final step, where each action is closely questioned.

This article reviewed prevailing trends in zero-trust architecture and the impact on information security practices. Section 2 reviews the literature, discusses the evolution and operation of ZTA, and compares ZTA with the traditional network security model and the current trends driving the implementation of ZTA across industries were discussed. Section 3 discusses the impact of ZTA on information security, while Section 4 highlights the challenges and future of ZTA in Information Security. Section 5 concludes the study.

2. Literature Review

This section reviews and analyzes Zero Trust principles, starting from their origin to their essential elements and modern developments. In addition, the implementation of ZTA among different industries was discussed.

2.1. Review of Zero Trust Architecture

Zero Trust Architecture has captured substantial interest among researchers, industry practitioners and policymakers because it strengthens information security. However, there are a lot of misconceptions and gaps in knowledge regarding ZTA. In order to bridge this gap, (Edo et al., 2022) adopted a literature review technique to give an insight into the effectiveness and successful implementation of ZTA. The study focused on how ZTA mitigates traditional security deficits but did not critique other frameworks.(Gellert et al., 2023) emphasized the impact and importance of ZTA in healthcare systems. The study discussed the deficiency of the traditional perimeter-based technique in mitigating the increase in cyberattacks, evolving threats, and compliance standards. The research concludes that healthcare systems could be secured from data breaches and vulnerabilities if they adopt ZTA principles.

(Chaudhry and Hydros, 2023) proposes integration of blockchain technology and ZTA into the banking sector. The study disclosed that enforcing these techniques can enhance secured transaction and prevent malicious actors as well as ensure data integrity and confidentiality. The study proposed a consensus algorithm which is adopted in blockchain transactions to certify decentralization and immutability combined with Zero-Trust principles to strengthen integrity and confidentiality. The study concluded that combining these approaches gives a secured and robust model for this present-day banking transaction. Due to the security challenges such as insider attacks, weak access management and lateral movement which is encountered in cloud networks, (Ahmadi, 2024) proposes the adoption of ZTA which can be combined with artificial intelligence and machine learning to eradicate these challenges. The findings revealed that ZTA significantly improves cloud security and strengthens identity and access management as well as network micro-segmentation.

ZTA have been adopted in IoT systems (Ameer et al., 2024) and the study introduced ZTA access control framework (ZTA-IoT-ACF) to sustain interactions of devices within the IoT networks. The research developed a ZTA score-based authorization model (ZTA-IoT-OL-SAF) to manage object-level access and also presented a usage control model to regulator device to object relationship and user-to-object within the IoT networks. The study established that combining ZTA-IoT-ACF and ZTA-IoT-OL-SAF framework enhanced security and access control due to its ability to enforce authorization using Zero trust principles. (Veeramachaneni, 2025) proposed the integration of zero trust principles to identity and access management (IAM) frameworks to improve security in a hybrid and multi-cloud environments. The research aimed to substitute the traditional perimeter-based security models with ZTA. The experimental result showed that zero trust IAM framework improved the cloud security in terms of prompt threat detection and response time in the cloud networks.

2.2. Evolution of Zero Trust Architecture

The zero Trust concept originated from Stephen Paul Marsh in 1994, and it gained popularity through John Kindervag in 2010 (Seymour, 2023, Tanque and Foxwell, 2023, Roy and Phadke, 2023). The Zero Trust Architecture is developed on never trusting any device, network, or user and always verifying before access is granted, unlike conventional security models that automatically believe that any device or user within the network is safe. The Zero Trust model operates such that every interaction is treated as a potential threat. It requires authentication and validation for all requests, whether they originated from inside or outside the network, before access is granted.

Zero Trust is built on the following basic assumptions and principles: Firstly, zero trust assumes that there is no implicit trust, which implies that no entity should be trusted automatically (Stafford, 2020, Dimitrakos et al.,

2020). Trust must be earned through continuous authentication, authorization process, and the continual verification of behaviors. In addition, ZTA believes that a network is always hostile, such that the network cannot be trusted internally or externally. This is against the conventional notion that the internal network is secured, so it is overlooked. On the other hand, Zero Trust believes that an attacker may already be inside the network or could penetrate the network at any time (Ferretti et al., 2021, Alevizos et al., 2022). Therefore, network location or previous authentication status cannot be the sole criterion for access to sensitive resources.

Similarly, ZTA believes that insiders are equally dangerous as external attackers because compromised credentials, malicious insiders, and misconfigured devices can be a significant security risk (Aslan et al., 2023, Jimmy, 2024). In the ZTA model, internal threats are no different from external ones; therefore, any activity and all the access requests in the internal network have to be dutifully checked. Furthermore, Zero Trust recognizes that data, devices, and users are no longer confined but are now distributed across multiple environments such as on-premises networks, hybrid, and cloud environments (Dongiovanni, 2024, Itodo, 2024). The growth of remote working, IoT devices, and cloud services implies that the conventional network is no longer defined. Therefore, it is pertinent that devices and users are secured regardless of their location rather than enforced on a particular physical network.

Based on the assumptions stated, the zero-trust model is considered to conform to the following ZTA fundamental principles: The zero-trust foundational principle is based on the concept of "Never Trust, Always Verify". It implies that no entity, whether inside or outside, should be trusted even if it has been previously authenticated. Each access request must come from a user, device, or application and must always be authenticated, authorized, and monitored. Location, activity history, or even references from other people were never enough reasons to trust. Another principle is Least Privilege, where ZTA restricts the user's or a device's access to the bare minimum required to carry out its activities. This minimizes the possibilities because it determines the range of actions a potential attacker or a user already in the network can take. Users are allowed to access only the required resources for their responsibilities, and more importantly, all access and use of resources are controlled and monitored.

Furthermore, the micro-segmentation technique used in Zero Trust to control the transfer of adversaries laterally throughout a network segmentation breaks a network into smaller isolated segments (Jebbar and Al-Zubaidie, 2024). If this technique is adopted and implemented, the network segment is designed to stop attackers from moving to another part of the network, even if they have compromised a segment (Bush and Mashatan, 2022, Ahmadi, 2024). It was also useful in segmenting the networks to provide different security measures depending on the sensitivity and risks of diverse network sections. Similarly, the ZTA adopt the continuous authentication and monitoring approach where rather than just applying a classic one-time authentication when the user logs into the network, ZTA applies the authentication process multiple times within a given user or device session. However, once a user is permitted to access the network, ZTA follows the user activity and health state of the user devices for any unusual activity. Some situations require extra identification measures, like if there are attempts to access from different locations or devices than those expected, or if a device is disconnected from the network and then reconnects, it may be denied access.

Another principle ZTA uses is real-time analytics and threat detection, which employs detailed analytics, machine learning, and behavioral assessment to identify threats on a real-time basis. Zero Trust systems can detect behaviors, network traffic, and activity that deviates from the normal to suggest an intrusion (Gudala et al., 2021). This implies that it allows the automation of responses, which can help contain or mitigate threats before they escalate and cause significant harm. The ZTA architecture is developed with the assumption that breaches are unavoidable; therefore, it focuses on how to minimize the impact if peradventure it happened (Pakmehr et al., 2022, Davis et al., 2024).

2.3 Operations of Zero Trust Architecture

Zero Trust and zero trust architecture operations are in compliance with the guidelines of the National Institute of Standards and Technology (NIST), which regulates the procedures and standards in technology (Kerman et al., 2020, Syed et al., 2022). The Zero Trust architecture (ZTA) is a security model based on authenticating identities and ensuring that permissions at every resource access level are checked. It consists of various components meant to provide an access control decision appropriate to identity, context, and security policies. The policy engine, policy administrator, policy enforcement points, and identity and access management are the principal components of the ZTA model.

i. Policy Engine (PE): is the core decision-maker responsible for approving, denying or restricting the access

requests according to the organizational security policies and identity and contextual factors such as the health of the device being used or location (Bradatsch et al., 2023). The policy administrator and policy enforcement points work with the policy engine.

ii. Policy Administrator (PA): This is where the implementation policy engine's decision is actualized. It applies the needed configuration to network components such as firewalls, proxies, or software-defined perimeters, meaning traffic flow or access requests are granted, denied, or partitioned accordingly.

iii. Policy Enforcement Points (PEP): are distributed in various locations on the network and serve as the gatekeepers of access (Azad et al., 2024). They also ensure the policy security decisions made by the policy engine block or pass traffic according to a set security policy. PEPs can exist anywhere along the network spectrum, whether in firewalls, proxies, or even an endpoint security solution.

iv. Identity and Access Management (IAM): One of Zero Trust's core elements is identity verification, which ensures that only verified and trusted identities have access to some of its resources or network (Indu et al., 2018). This is commonly guarded by multi-factor authentication (MFA) and role-based access control (RBAC).

The flow of operation in ZTA is depicted in Figure 1, where a device or user sends a request to access a resource, which the policy engine will evaluate based on the identity of the user, location, device posture, and other important context. After that, the policy administration will configure the system in line with the routing traffic or decision appropriate, and the policy enforcement point will ensure that the access and traffic conform to these decisions. Continuous monitoring is performed in real-time to gain insights into the behavior of the devices or network users, enabling automated responses in case of potential threats.

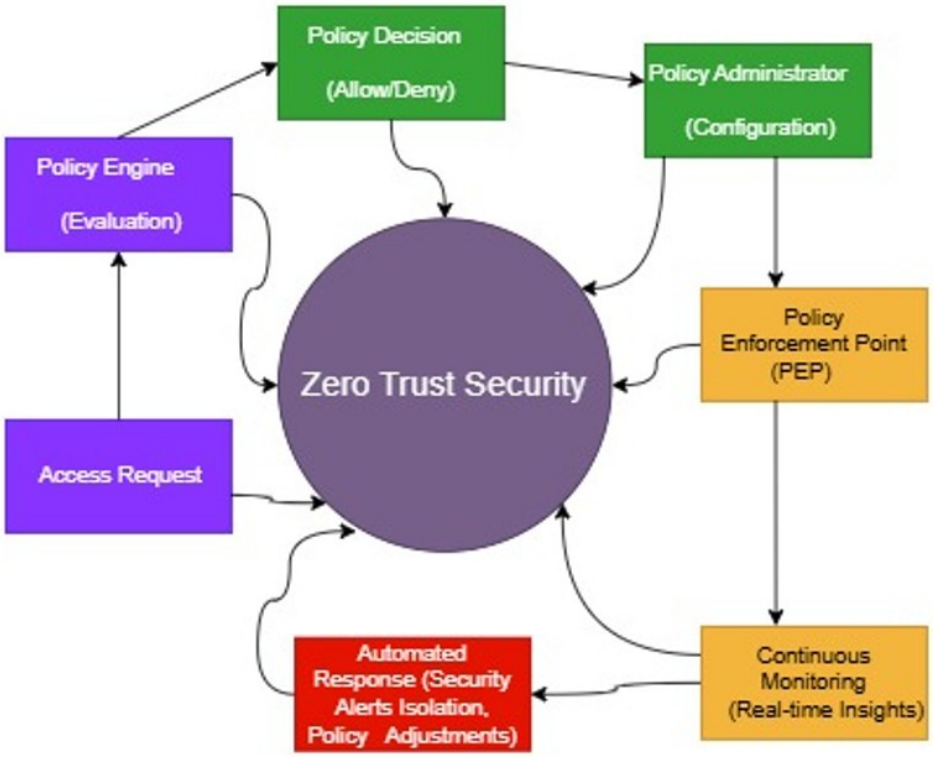

Figure 1: The flow of operation in Zero Trust Architecture (Author created)

2.4. Zero Trust Architecture Versus Traditional Network Security Models

Traditional network security techniques use several components, such as firewalls, intrusion detection systems, virtual private networks, and endpoint protection with perimeter defense. However, this technique has its demerits such that once the user or device is inside the network, it automatically earns trust, which can lead to inside threats and lateral movement vulnerabilities. Zero trust architectures use different components such as identity and access management, endpoint security and device posture, least privilege and role-based access control, micro-segmentation, and identity-based security, and still do not trust existing devices or users. Given this, continuous monitoring and analytics are done consistently for devices inside and outside the network to quickly track and respond to likely threats.

Table 1 compares perimeter defense, micro-segmentation, and identity-based security in this discourse. Each technique has its advantages but performs much better when combined. For example, perimeter defense would perform better against external threats, micro-segmentation would mitigate the impact of a breach, and identity-based security would give continuous monitoring of devices and users' access.

Table 1: Comparison between Traditional Network Security and Zero Trust Architecture (Author created)

S/N	Aspect	Perimeter Defense	Micro-segmentation	Identity-based security
1	Main goal	It creates a robust and powerful boundary in the network.	It isolates segments within a network.	It verifies and regulates access based on the device's identity.
2	Trust model	Automatic trust of users/devices within the network once access is gained.	Trust is limited to particular segments.	Trust depends on the consistent verification of identity.
3	Major technique	Intrusion detection/prevention, firewalls, VPNs.	Partition network into small, secured zones.	Least privilege, authentication, identity, and access management.
4	Security priority	Perimeter-based access.	Segregate workloads and curtail lateral movement.	Identity verification determines access and permissions.
5	Response to threats	It only blocks outside threats	Confine the reach of breaches within a network.	Reduces threat by managing identity access.
6	Limitation	Susceptible to inside threats and lateral movement.	It needs monitoring and comprehensive configuration.	Intricate implementation needs IAM maintenance.
7	Resilience to insider threats	Low	Moderate	High

2.5. Trends in Zero Trust Architecture

Due to a rising number of more complex cyber threats, the concept of traditional perimeter-based security models has given way to the zero-trust technique, which believes that no one can be trusted. ZTA enables us to continuously confirm the identity and limit access adopted across different sectors based on their security requirements, risk exposure, and compliance. The trends have evolved into various sectors and are categorized into industry adoption, technological innovation driving ZTA, and regulatory and compliance trends. The industry adoption of zero trust architecture is discussed in Table 2.

i. Technological Innovations Driving Zero Trust Architecture (ZTA)

Zero Trust Architecture is an emerging strategy in cybersecurity that is known for its technological advances that assist organizations in addressing, overcoming challenges, and improving their security (Stafford, 2020, Ahmadi, 2024). This evolution is made possible through innovations in DevSecOps incorporation, Artificial intelligence, machine learning, and cloud computing (Sanders et al., 2021, Sandu, 2021). All these technologies improved ZTA, making it more flexible and robust in a contemporary distributed environment.

The adoption of Zero Trust Architecture (ZTA) has accelerated in response to the shift toward cloud computing and distributed environments, especially since COVID-19. Unlike traditional security models that trust internal network entities, ZTA is founded on a "never trust, always verify" model, where users must authenticate and authorize regardless of their location or device (Bendale and Prasad, 2020, Joshi, 2024). In cloud computing, ZTA applies strict constraints, vigilance, and encryption mechanisms to secure applications and data, (Yadav et al., 2023, Röttinger and Wenning, 2024) with significant providers like AWS and Microsoft Azure offering Zero Trust solutions to manage hybrid and multi-cloud security (Sarkar et al., 2022, Lakhani, 2024). Integrating DevSecOps and automation tools with ZTA brings security at every phase of the software development lifecycle (Vemula, 2022, Tanque and Foxwell, 2023). DevSecOps uses agile development methodology to build secured applications from the outset (Sharma, 2024). Automation tools in DevSecOps environments align with ZTA by continuously monitoring access points to detect vulnerabilities, enforce security protocols automatically and ensure that every code update is tested for security compliance before deployment (Marandi et al., 2023). This

approach reduces human error and maintains ZTA principles throughout development.

Table 2: Zero Trust Architecture Industry Adoption (Author created)

S/N	Sector	Description	Examples of organisations that have adopted ZTA	ZTA Methodology Applied	References
1	Healthcare	Need to safeguard patient information, and ensure strict adherence with regulations such as HIPAA and GDPR.	Mayo Clinic, Cleveland Clinic	IoT security, cloud security, data encryption.	(34)
2	Financial Services	There is a need for a secured transaction, as well as protection of sensitive customer data.	JPMorgan Chase, Goldman Sachs	Encryption, Access Control, MFA, AI-based detection.	(35)
3	Government	National security is the top priority, and protecting citizens' data has encouraged the adoption of ZTA.	Cybersecurity and Infrastructure Security Agency (CISA)	Continuous monitoring, network segmentation, multi-factor authentication (MFA). .	(36)
4	Technology	Having a secured remote work environment and protecting critical details such as IP addresses, etc., drive the early adoption of ZTA.	Google (BeyondCorp), Microsoft		(37, 38).

Similarly, the adoption of AI/ML has greatly enhanced ZTA as they offer techniques of real-time threat identification and response procedures (Ajish, 2024)These technologies process large amounts of data to identify unusual patterns that can deduce potential threats. Once a threat is detected, AI-integrated automation tools will

automatically counteract it by restraining access, quarantining the systems, or notifying the security teams. This strengthens an organization's defense against advanced cyberattacks and mitigates damage through rapid automated responses.

ii. Regulatory and Compliance Trends in Zero Trust Architecture (ZTA)

The increasing demand for regulatory and compliance standards drives the adoption of ZTA. Globally recognized data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), emphasize security models like ZTA to ensure organizations comply with privacy standards, manage cyber risks, and protect personal data (Mendoza and Herrera, 2023, Chaturvedi et al., 2024, Roy et al., 2024).

Similarly, government policies in some nations, including the U.S. Executive Order 14028 and guidelines from the National Institute of Standards and Technology (NIST), mandate that federal agencies should incorporate Zero Trust principles, such as multi-factor authentication and network segmentation, to improve their data security and resilience across sectors (Sarkar et al., 2022, Nivarthi and Gatla, 2022, Carroll, 2024). These initiatives set ZTA as a benchmark for protecting sensitive data, boosting sector resilience and reducing breach risks.

3. Impact of Zero Trust on Information Security

The ZTA approach in information security has significantly improved the identification of threats, reduced internal threats and strengthened control over networks (Muhammad et al., 2022). As much as it has notable benefits, it has drawbacks when implemented in organizations with complex structures or processes. A few benefits of ZTA in information security are early detection of threats and automated alerts and responses when threats are identified. This is achieved by increasing the visibility and control of users' access to some sensitive information in the applications and networks using Least Privilege access and compulsory user verification at the access point. This technique minimizes unauthorized movement and attacks on the networks.

In addition, Zero Trust leverages on machine learning and artificial intelligence to search for anomalies and detect threats in real time (Gudala et al., 2021, Ajish, 2024). ZTA automatically triggers feedback, such as imposing MFA or restricting access before significant damage is caused. Similarly, it alerts the security team when unusual patterns or unexpected access is attempted from a new location. Also, the enforcement of the least privilege and continuous monitoring technique has significantly reduced inside and outside threats in the network because there is real-time detection, quick response to suspicious actions and access is only granted to the specific resources needed (Nyamasvisva and Arabi, 2022).

4. Challenges and Future of Zero Trust Architecture in Information Security

Zero Trust is a notable improvement over the traditional approach as its main focus is reducing the attack surface, sustaining performance, balancing compliance and privacy as well as the time to improve threat detection (Buck et al., 2021). However, full implementation of a Zero Trust environment might not be a realistic goal for many organizations to implement effectively because of some challenges, such as difficulty for older and legacy systems to adopt Zero trust due to old infrastructures that often lack identity management, contemporary security measures, and integration capabilities, which are important in effectively implementing Zero trust (Teerakanok et al., 2021). Introducing ZTA into such systems may require extensive configuration and expensive upgrades, which will be time-consuming and require intensive resources.

Furthermore, numerous organizations perform their operations via hybrid and multi-cloud platforms, sometimes using different cloud providers that implement various protocols and security configurations, causing discrepancies that complicate policy enforcement. Sustaining Zero Trust across these platforms can be challenging (Chimakurthi, 2020, Kanungo, 2023). Similarly, establishing and sustaining ZTA requires that an organization should have experts and advanced security equipment; this might put pressure on such organization's finances and resources (Buck et al., 2021, Daley, 2022). Unfortunately, numerous organizations lack experts who can continuously monitor the adaptive response needed by ZTA and real-time detection of threats, which is not cost-effective, particularly for small to medium-scale organizations. In addition, the basis of Zero Trust is based on the principle of continuous authentication and access validation that slows response time and interrupts user experiences and workflows (Gellert et al., 2023). For instance, receiving multiple MFA prompts or access checks can be frustrating and thus reduce user productivity.

The future of Zero Trust Architecture (ZTA) is expected to grow rapidly because of its suitability in handling emerging cybersecurity threats. The market forecast indicates that the growth is stimulated by the increase in

cyber threats, adoption of remote work, and cloud-based infrastructures in different sectors such as finance, healthcare, and government. These industries, susceptible to data breaches, are specifically suited to the Zero Trust model, which provides the identity-centric security they need for robust data protection.

Emerging technologies, such as 5G, quantum computing, and blockchain, are important for the evolution of ZTA. 5 G's low latency and high-speed connectivity will improve the implementation of ZTA across cloud and mobile networks. At the same time, blockchain provides enhanced security with decentralized and tamper-resistant data verification features. In the future, quantum computing may introduce advanced encryption techniques, further bolstering ZTA's capability to counter sophisticated cyber threats and ensure real-time detection.

5. Conclusion

This article reviewed the concept and evolution of Zero-Trust architecture and the trends and technological advancements in information security, adopting systematic literature review from 2022 to 2025 and qualitative research method. The study investigates the fundamental principles of ZTA and compared the conventional security model to Zero Trust Architecture. Through the adoption of systematical analysis of the literature, we have identified how continuous monitoring and identity-based access controls can be a good option in ZTA in addressing complex threats in contrast to the conventional perimeter security models.

The findings of the study emphasized that to successfully implement ZTA in information security, the following must be considered: least privileged access, encryption techniques, continuous verification and robust identity access management across on-premises and cloud environments. As technology keeps evolving, the insight from this study provides a valuable contribution to how a robust security strategy can be developed to protect data and assets in the digital sphere.

Acknowledgement

We would like to thank the Department of Information System and Management, Stanton University, California, USA, for giving us access to materials from the library. Similarly, we would like to thank Mr Yusuf Olatunde from the Department of Cyber Security, Osun State University, Osogbo, Nigeria, for his invaluable support and guidance throughout this research endeavor.

References

ABRERA, J. 2024. Data Privacy and Security in Cloud Computing: A Comprehensive Review. *Journal of Computer Science and Information Technology,* 1**,** 01-09.

AHMADI, S. 2024. Zero trust architecture in cloud networks: application, challenges and future opportunities. *Ahmadi, S.(2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports,* 26**,** 215-228.

AJISH, D. 2024. The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology,* 11**,** 30.

ALEVIZOS, L., TA, V. T. & HASHEM EIZA, M. 2022. Augmenting zero trust architecture to endpoints using blockchain: A state‐of‐the‐art review. *Security and privacy,* 5**,** e191.

AMEER, S., PRAHARAJ, L., SANDHU, R., BHATT, S. & GUPTA, M. 2024. ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model. *ACM Transactions on Privacy and Security*.

ASLAN, Ö., AKTUĞ, S. S., OZKAN-OKAY, M., YILMAZ, A. A. & AKIN, E. 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics,* 12**,** 1333.

AZAD, M. A., ABDULLAH, S., ARSHAD, J., LALLIE, H. & AHMED, Y. H. 2024. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things,* 27**,** 101227.

BELL, C., BROKLYN, P. & EGON, A. 2024. Zero-Trust Security Model for Enhanced Cloud Security and Data Privacy. *Available at SSRN 4904958*.

BENDALE, S. & PRASAD, J. 2020. Preliminary study of Software Defined Network on COVID-19 pandemic use cases. *Available at SSRN 3612815*.

BISPHAM, M., CREESE, S., DUTTON, W. H., ESTEVE-GONZALEZ, P. & GOLDSMITH, M. Cybersecurity in working from home: An exploratory study. TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, 2021.

BRADATSCH, L., MIROSHKIN, O., TRKULJA, N. & KARGL, F. Zero Trust Score-based Network-level Access Control in Enterprise Networks. 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2023. IEEE, 1422-1429.

BUCK, C., OLENBERGER, C., SCHWEIZER, A., VÖLTER, F. & EYMANN, T. 2021. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security,* 110**,** 102436.

BUSH, M. & MASHATAN, A. 2022. From zero to one hundred: Demystifying zero trust and its implications on enterprise people, process, and technology. *Queue,* 20**,** 80-106.

CARROLL, J. The US National Cybersecurity Strategy: A Vehicle with an International Journey. European Conference on Cyber Warfare and Security, 2024. 107-115.

CHATURVEDI, I., PAWAR, P. M., MUTHALAGU, R. & TAMIZHARASAN, P. 2024. Zero Trust Security Architecture for Digital Privacy in Healthcare. *Information Technology Security: Modern Trends and Challenges.* Springer.

CHAUDHRY, U. B. & HYDROS, A. K. 2023. Zero‐trust‐based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET blockchain,* 3**,** 98-115.

CHIMAKURTHI, V. N. S. S. 2020. The challenge of achieving zero trust remote access in multi-cloud environment. *ABC Journal of Advanced Research,* 9**,** 89-102.

DALEY, S. 2022. Evaluation of Zero Trust framework for remote working environments. Dept of Science and Technology, Bournemouth University.

DAVIS, P., COFFEY, S., BESHAJ, L. & BASTIAN, N. D. 2024. Emerging Technologies for Data Security in Zero Trust Environments. *The Cyber Defense Review,* 9**,** 49-72.

DIMITRAKOS, T., DILSHENER, T., KRAVTSOV, A., LA MARRA, A., MARTINELLI, F., RIZOS, A., ROSETTI, A. & SARACINO, A. Trust aware continuous authorization for zero trust in consumer internet of things. 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), 2020. IEEE, 1801-1812.

DONGIOVANNI, A. 2024. *Zero Trust Network Security Model in Containerized Environments.* Politecnico di Torino.

EDO, O. C., TENEBE, T., ETU, E.-E., AYUWU, A., EMAKHU, J. & ADEBIYI, S. 2022. Zero Trust Architecture: Trend and Impacton Information Security. *International Journal of Emerging Technology and Advanced Engineering,* 12**,** 140.

EL-AMIR, S. 2023. Comprehensive Cybersecurity Review: Modern Threats and Innovative Defense Approaches. *International Journal of Computers and Informatics,* 1**,** 30-37.

FERNANDEZ, E. B. & BRAZHUK, A. 2024. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces,* 89**,** 103832.

FERRETTI, L., MAGNANINI, F., ANDREOLINI, M. & COLAJANNI, M. 2021. Survivable zero trust for cloud computing environments. *Computers & Security,* 110**,** 102419.

GELLERT, G. A., KELLY, S. P., WRIGHT, E. W. & KEIL, L. C. 2023. Zero Trust and the future of cybersecurity in healthcare delivery organizations. *J. Hosp. Adm,* 12.

GUDALA, L., SHAIK, M. & VENKATARAMANAN, S. 2021. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. *Journal of Artificial Intelligence Research,* 1**,** 19-45.

INDU, I., ANAND, P. R. & BHASKAR, V. 2018. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal,* 21**,** 574-588.

ITODO, C. A. 2024. *A Novel Framework for the Adoption of Zero Trust Security for Small, Medium and Large-Scale Organizations.* University of Cincinnati.

JEBBAR, W. A. & AL-ZUBAIDIE, M. 2024. Transaction-Based Blockchain Systems Security Improvement Employing Micro-Segmentation Controlled by Smart Contracts and Detection of Saddle Goatfish. *SN Computer Science,* 5**,** 1-23.

JIMMY, F. 2024. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023,* 2**,** 129-171.

JOSHI, H. 2024. Emerging Technologies Driving Zero Trust Maturity Across Industries.

KANUNGO, S. 2023. Security Challenges and Solutions in Multi-Cloud Environments. *Stochastic Modelling and Computational Sciences,* 3**,** 139-146.

KERMAN, A., BORCHERT, O., ROSE, S. & TAN, A. 2020. Implementing a zero trust architecture. *National Institute of Standards and Technology,* 2020**,** 17-17.

LAKHANI, R. 2024. Zero Trust Security Models: Redefining Network Security in Cloud Computing Environments. *International Journal of Innovative Research in Computer and Communication Engineering,* 12**,** 141 - 156.

MAKHDOOM, I., ABOLHASAN, M., LIPMAN, J., LIU, R. P. & NI, W. 2018. Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials,* 21**,** 1636-1675.

MARANDI, M., BERTIA, A. & SILAS, S. Implementing and Automating Security Scanning to a DevSecOps CI/CD Pipeline. 2023 World Conference on Communication & Computing (WCONF), 2023. IEEE, 1-6.

MENDOZA, C. & HERRERA, J. 2023. Enhancing Security and Privacy in Advanced Computing Systems: A Comprehensive Analysis. *Journal of Advanced Computing Systems,* 3**,** 1-9.

MUHAMMAD, T., MUNIR, M. T., MUNIR, M. Z. & ZAFAR, M. W. 2022. Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology,* 6**,** 99-135.

NIVARTHI, K. S. P. & GATLA, G. 2022. Fighting Cybercrime with Zero Trust. *American Academic Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS),* 90**,** 371-381.

NYAMASVISVA, T. E. & ARABI, A. A. M. 2022. A Comprehensive SWOT Analysis For Zero Trust Network Security Model. *International Journal of Infrastructure Research and Management Vol. 10 (1), June 2022*.

PAKMEHR, M., KHAMVILAI, T., BEHBAHANI, A. R., COSTELLO, J., SKERTIC, R. & ADEMOLA, A. P. Applying Zero Trust Principles to Distributed Embedded Engine Control Systems. AIAA AVIATION 2022 Forum, 2022. 3480.

PÓSA, T. & GROSSKLAGS, J. 2022. Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy,* 2**,** 490-515.

PUAT, H. A. M. & ABD RAHMAN, N. A. IoMT: a review of pacemaker vulnerabilities and security strategy. Journal of Physics: Conference Series, 2020. IOP Publishing, 012009.

RAH, A. 2023. *Device Management in the Security of "Bring Your Own Device"(BYOD) for the Post-pandemic, Remote Workplace*, University of Fairfax.

RÖTTINGER, R. & WENNING, S. 2024. ZERO TRUST ARCHITECTURES IN THE ENERGY SECTOR: APPLICATIONS AND BENEFITS. *European Journal of Engineering and Technology,* 12.

ROY, A., DHAR, A. & TINNY, S. S. 2024. Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. *Journal of Computer Science and Information Technology,* 1**,** 25-50.

ROY, S. & PHADKE, A. C. 2023. A Review on Zero Trust—Balancing Security and Usability Needs.

SANDERS, G., MORROW, T., RICHMOND, N. & WOODY, C. 2021. Integrating zero trust and devsecops. Carnegie-Mellon Univ Pittsburgh Pa.

SANDU, A. K. 2021. DevSecOps: Integrating Security into the DevOps Lifecycle for Enhanced Resilience. *Technology & Management Review,* 6**,** 1-19.

SARKAR, S., CHOUDHARY, G., SHANDILYA, S. K., HUSSAIN, A. & KIM, H. 2022. Security of zero trust networks in cloud computing: A comparative review. *Sustainability,* 14**,** 11213.

SEYMOUR, N. L. 2023. Zero Trust Architectures: A Comprehensive Analysis and Implementation Guide.

SHARMA, P. 2024. DevSecOps Integration-Security in the Software Delivery Pipeline: Exploring the integration of security practices into the software delivery pipeline to ensure secure software development practices. *Australian Journal of Machine Learning Research & Applications,* 4**,** 46-54.

STAFFORD, V. 2020. Zero trust architecture. *NIST special publication,* 800**,** 207.

SYED, N. F., SHAH, S. W., SHAGHAGHI, A., ANWAR, A., BAIG, Z. & DOSS, R. 2022. Zero trust architecture (zta): A comprehensive survey. *IEEE access,* 10**,** 57143-57179.

TANQUE, M. & FOXWELL, H. J. 2023. Cyber risks on IoT platforms and zero trust solutions. *Advances in Computers.* Elsevier.

TEERAKANOK, S., UEHARA, T. & INOMATA, A. 2021. Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks,* 2021**,** 9947347.

TYLER, D. & VIANA, T. 2021. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Applied Sciences,* 11**,** 7499.

VEERAMACHANENI, V. 2025. Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. *Recent Trends in Cloud Computing and Web Engineering,* 7**,** 78-92.

VEMULA, V. R. 2022. Integrating Zero Trust Architecture in DevOps Pipeline: Enhancing Security in Continuous Delivery Environments. *Transactions on Latest Trends in IoT,* 5**,** 1-18.

YADAV, V., SONI, M. K. & PRATAP, A. Secured Identity and Access Management for Cloud Computing Using Zero Trust Architecture. International Conference on Cryptology & Network Security with Machine Learning, 2023. Springer, 687-698.