Conceptual Model for Remote Access Security Using Zero-Trust Network Access (ZTNA)

Abstract

The rise of remote work and cloud-based environments has revealed significant vulnerabilities in traditional security models like Virtual Private Networks (VPNs). These models, relying on perimeter-based security, often grant excessive trust after initial authentication, exposing systems to lateral movement and unauthorized access. Zero-Trust Network Access (ZTNA) addresses these gaps through a model of continuous verification and strict application-level controls. This study explores ZTNA's efficacy as a robust alternative to traditional VPNs, focusing on its principles, implementation challenges, and security benefits. Through comprehensive analysis and case study evaluation, it was found that ZTNA not only mitigates risks associated with lateral movement but also enhances compliance with regulatory frameworks and scalability in remote and distributed environments. The findings confirm ZTNA as an adaptable solution for securing remote access in diverse modern contexts.

Keywords**:** Zero-Trust Network Access (ZTNA), remote access security, cybersecurity framework, identity-based access, application-specific controls, lateral movement prevention, regulatory compliance, scalable security solutions.

1. Introduction

The growing adoption of remote work and cloud services has exposed critical flaws in traditional security models. Virtual Private Networks (VPNs), designed for encrypted remote connections, operate on a perimeter-based approach that assumes implicit trust after initial authentication. This model grants extensive network access, increasing the risk of unauthorized actions, lateral movement, and insider threats. These vulnerabilities have led organizations to seek more robust alternatives, particularly as remote work becomes a permanent aspect of modern work environments.

Zero-Trust Network Access (ZTNA) has emerged as a viable solution to address these challenges. Unlike VPNs, ZTNA operates on a principle of "never trust, always verify," requiring continuous authentication and context-aware access controls. ZTNA limits access to specific applications and enforces strict identity and device-based permissions, enhancing security and aligning with modern regulatory requirements.

This study aims to evaluate ZTNA's effectiveness in addressing the limitations of traditional VPNs. It explores the principles underpinning ZTNA, its key components, and the challenges organizations face during its implementation. By analyzing theoretical foundations and real-world applications, this study provides insights into how ZTNA supports secure, scalable, and compliant remote access.

The paper begins with an overview of ZTNA's background and principles, followed by a literature review that traces the evolution of remote access security. The methodology section outlines the approach used for data collection and analysis. Case studies and findings are then presented, highlighting ZTNA's benefits and challenges. Finally, the paper concludes with recommendations for successful adoption and future research directions.

2. Literature Review

Remote access security has evolved significantly in response to the rise of cloud computing and decentralized work environments. Historically, perimeter-based security models dominated, relying heavily on Virtual Private Networks (VPNs) to create encrypted tunnels for remote connections. VPNs operate on an implicit trust model, granting users broad network access once authenticated. This approach sufficed for centralized, on-premise systems but proved inadequate formodern, distributed networks. The rapid expansion of remote work has exposed these vulnerabilities, particularly issues of scalability, insider threats, and credential-based attacks.

The limitations of VPNs are well-documented. Research highlights that implicit trust models introduce a single point of failure, making them susceptible to unauthorized access, as Deshpande (2021) emphasized. VPNs lack granular access controls, often permitting lateral movement across networks in case of a breach. Performance bottlenecks are also common when supporting large, distributed workforces, reducing efficiency in modern cloud environments. Traditional VPN models, while effective in their time, have become increasingly inadequate in addressing the demands of decentralized networks. Mandal, Khan, and Jain (2021) argued that the perimeter-based approach of VPNs assumes inherent trust, a model poorly suited to environments where insider threats and credential-based attacks are prevalent. Additionally, the reliance on encrypted tunnels for data transmission, while secure, offers limited control over user permissions. Peterson (2021) further noted that organizations adopting these traditional models often struggle with visibility into user activity, leaving critical gaps in their security frameworks.

The Zero-Trust Security model emerged in response to these challenges, promoting continuous verification and adaptive access controls. Wu, Yan, and Wang (2021) expanded on this concept by introducing real-identity-based controls, which align permissions with dynamic contextual factors such as user behavior and device health. These features directly address the limitations identified by Mandal et al., bridging the gap between user access and resource protection. Studies further demonstrate ZTNA's capacity to mitigate risks inherent in VPN-based systems. For example, identity-based access control within ZTNA ensures that permissions align strictly with user roles, thereby limiting unauthorized access (Bashir, 2024). Micro-segmentation further enhances security by isolating network resources and restricting the movement of

potential attackers. Continuous monitoring enables real-time threat detection, supporting proactive responses to emerging risks (Chen et al., 2023)

ZTNA also provides distinct advantages in adapting to future challenges, such as securing emerging technologies like 6G and IoT networks. Kim et al. (2024) identified that ZTNA's dynamic policy enforcement and micro-segmentation principles could address the latency and interoperability challenges posed by these decentralized environments. Similarly, Indran and Alwi (2024) highlighted the importance of integrating Secure Access Service Edge (SASE) principles into ZTNA, enabling consistent and scalable security in multi-cloud infrastructures.

Despite these benefits, challenges persist, such as integration complexity and high initial costs, which may hinder adoption, particularly for small to medium enterprises. The integration of advanced analytics and AI-based systems into ZTNA frameworks, as proposed by Daley (2022), could enhance its adaptability by enabling predictive threat detection and dynamic policy adjustments. These capabilities, when combined with user-centric strategies like real-identity-based controls, could further improve compliance and reduce operational friction during adoption.

By addressing VPN limitations and aligning with the demands of modern networks, ZTNA has positioned itself as a superior framework for secure remote access. Table 1 summarizes key studies on ZTNA's effectiveness, presenting the advantages identified, methodologies, and challenges. For instance, while Fang et al. (2022) noted improved access control, they identified high implementation costs as a primary obstacle. Similarly, Tuyishime et al. (2024) found scalability benefits but noted integration challenges with diverse cloud platforms. These findings reinforce ZTNA's critical role in overcoming the security vulnerabilities inherent in traditional VPNs.

Table 1: Summary of Existing Research on ZTNA Effectiveness

Author(s) & Year	Focus Area	Methodology	Key Findings	Identified Challenges
Fang et al. (2022)	iOS Remote Security via ZTNA	Case Study	ZTNA improved remote access control by reducing attack exposure by 30% compared to VPNs.	High implementation costs; integration issues with legacy systems.
Anderson et al. (2022)	BYOD Security Enhancement	Experimental Design	Enhanced security and user experience in	Complexity in policy management;

			BYOD scenarios using ZTNA.	user resistance to stricter controls.
Brazhuk & Fernandez (2022)	Abstract Security Pattern for ZTNA	Theoretical Framework	ZTNA minimizes unauthorized access and supports compliance with security policies.	Need for complex architecture redesign; lack of standardized practices.
Tuyishime et al. (2024)	Cloud-Based Remote Lab Access	Case Study	Improved scalability and flexibility in remote access to cloud-based labs using ZTNA principles.	Integration challenges with diverse cloud platforms; high operational costs.
Qazi (2022)	ZTNA for Network Security	Empirical Analysis	Demonstrated enhanced network security through adaptive access control in ZTNA frameworks.	Requires continuous monitoring and analytics; high resource demand.
Federici et al. (2023)	ZTNA in Industrial IoT Infrastructure	Simulation-Based Evaluation	Improved security and access control in industrial IoT networks using ZTNA.	Initial setup complexity; potential latency in large-scale deployments.
Chen et al. (2023)	ZTNA for 6G Security	Simulation & Model Development	ZTNA can enhance 6G network security by enforcing strict identity-based access controls.	Implementation complexity; interoperability issues with evolving technologies.

3. Methodology

This study employed a mixed-methods approach to evaluate the effectiveness of Zero-Trust Network Access (ZTNA) as a secure alternative to Virtual Private Networks (VPNs) for remote access. The combination of qualitative and quantitative methods allowed for a comprehensive analysis of theoretical frameworks, case studies, and empirical data.

The research design comprised two phases. The exploratory phase focused on reviewing existing literature and analyzing case studies to establish foundational knowledge about ZTNA. Studies on identity-based access control and continuous verification, such as those by Federici et al. (2023), provided insights into ZTNA's core principles and components. This phase also identified specific challenges in VPN-based security models, including limited scalability and vulnerability to lateral movement. The analytical phase involved evaluating quantitative data from case studies and surveys, which measured ZTNA's performance in areas such as access control efficiency and breach reduction rates.

Data collection combined literature review and secondary data analysis. The literature review relied on peer-reviewed articles, conference papers, and industry reports obtained from credible sources, such as IEEE Xplore and SpringerLink. These resources offered detailed perspectives on ZTNA's implementation, highlighting both benefits and obstacles. For example, Brazhuk and Fernandez (2022) provided valuable information on ZTNA's ability to enhance compliance with regulatory standards. Secondary data analysis supported these findings by examining breach statistics, user adoption rates, and integration challenges reported in recent case studies.

Data analysis utilized thematic and comparative techniques. Thematic analysis identified recurring patterns in ZTNA implementation, such as the emphasis on micro-segmentation and real-time monitoring. By categorizing themes like scalability and compliance, the analysis structured qualitative data into actionable insights. Comparative analysis quantified the advantages of ZTNA over VPNs, using metrics like breach reduction percentages and user satisfaction scores. For instance, Anderson et al. (2022) highlighted the improved security outcomes in Bring Your Own Device (BYOD) environments, a critical consideration in flexible working scenarios.

The chosen methodology, by integrating exploratory and analytical approaches, ensured a balanced evaluation of ZTNA. The combination of literature-driven insights and empirical evidence allowed the study to address theoretical principles while validating practical applications. This approach provides a robust foundation for assessing ZTNA's potential to transform remote access security frameworks.

4. Case Studies

The practical application of Zero-Trust Network Access (ZTNA) has been demonstrated across various industries, highlighting its effectiveness in securing remote access while addressing unique organizational challenges. This section examines key scenarios

involving corporate remote access and cloud-based services, showcasing ZTNA's role in enhancing security, scalability, and operational efficiency.

In corporate environments, ZTNA has proven instrumental in mitigating the risks associated with broad network access granted by VPNs. A study on ZTNA deployment within a remote laboratory setting, conducted by Tuyishime et al. (2024), illustrated how identity-based access controls restricted unauthorized entry to sensitive resources. By enforcing role-specific permissions and context-aware authentication, ZTNA facilitated secure, granular access, which enhanced overall compliance with organizational security policies. These findings are critical as they demonstrate ZTNA's adaptability to complex infrastructures where remote employees frequently access diverse applications.

Moreover, the same deployment highlighted ZTNA's scalability, as organizations were able to support increasing numbers of remote users without significant performance degradation. This scalability is particularly valuable in dynamic work environments, where employee counts and access requirements fluctuate rapidly. Tuyishime et al. observed that despite these benefits, integration challenges emerged during implementation, particularly in environments reliant on legacy systems. These challenges underscored the importance of robust infrastructure planning and technical expertise, as noted by Iță et al. (2023), who highlighted the role of segmentation controls in optimizing implementation efficiency.

ZTNA has also demonstrated its utility in securing cloud-based operations, which are central to modern remote work strategies. Brazhuk and Fernandez (2022), in their analysis of ZTNA applied to multi-cloud environments, emphasized the framework's ability to enforce consistent security policies across disparate cloud platforms. Through centralized policy management, ZTNA ensured compliance with security standards and maintained uniform protection against threats, even when organizations operated across multiple cloud service providers. Indran and Alwi (2024) expanded on these findings, noting that integrating Secure Access Service Edge (SASE) principles into ZTNA frameworks can further enhance multi-cloud environments by simplifying policy enforcement and increasing scalability.

In addition to centralized management, ZTNA's micro-segmentation features played a pivotal role in limiting lateral movement during potential breaches. By isolating resources into distinct zones, ZTNA minimized the scope of access for both users and attackers. Although Brazhuk and Fernandez noted that establishing this segmentation required extensive customization due to varying cloud provider protocols, the resulting security enhancements outweighed these initial complexities. This case study demonstrates how ZTNA can be tailored to meet the diverse needs of cloud-dependent organizations while mitigating risks associated with platform variability. Similarly, Abuhasel (2023) observed that ZTNA's segmentation capabilities were particularly

valuable in industrial environments, where they effectively restricted attackers from accessing sensitive IoT systems.

Across both case studies, ZTNA consistently delivered a stronger security posture by employing continuous monitoring and adaptive security policies. The integration of advanced analytics, as suggested by Daley (2022), further strengthens ZTNA frameworks by enabling real-time anomaly detection and dynamic policy enforcement. The enforcement of multi-factor authentication (MFA), combined with context-aware access controls, significantly reduced the risk of unauthorized access. For example, Anderson et al. (2022) identified that user-centric design elements, including seamless integration with existing authentication systems, improved user compliance and minimized resistance during adoption.

However, challenges such as high implementation costs and integration difficulties persisted. Organizations deploying ZTNA often encountered obstacles when aligning new security protocols with pre-existing systems. These challenges, as noted by Fang and Guan (2022), frequently required significant investments in infrastructure upgrades and technical training, which could strain resources, especially for small to medium enterprises. Addressing these challenges necessitates strategic planning, phased implementation, and ongoing support. Furthermore, Kim et al. (2024) argued that addressing compatibility issues with evolving technologies, such as IoT and 6G, requires continuous innovation within ZTNA frameworks to maintain their effectiveness.

These case studies illustrate ZTNA's transformative potential for remote access security. By enhancing identity-based controls, limiting lateral movement, and improving compliance, ZTNA effectively addresses the vulnerabilities inherent in traditional VPN models. Despite implementation hurdles, the demonstrated benefits position ZTNA as a vital framework for organizations navigating modern security challenges.

5. Findings and Discussion

The findings from this study underscore the significant advantages of Zero-Trust Network Access (ZTNA) compared to traditional VPN-based models. By addressing inherent vulnerabilities in perimeter-based security, ZTNA demonstrates its ability to enhance remote access security through principles of continuous verification and identity-based controls. These findings are consistent across literature, empirical studies, and case analyses.

ZTNA's adoption has resulted in a marked improvement in organizational security, particularly by reducing unauthorized access risks. For instance, Fang and Guan (2022) observed a 30% reduction in breach attempts following the implementation of ZTNA in corporate environments, where identity-based access controls mitigated risks associated with credential theft. Additionally, ZTNA's use of micro-segmentation

confined access to application-specific zones, limiting lateral movement, which is a significant vulnerability in traditional VPN frameworks. By segmenting networks into smaller, secure zones, as highlighted by Federici et al. (2023) and reinforced by Abuhasel (2023), ZTNA effectively prevents attackers from escalating privileges or compromising multiple resources.

Furthermore, ZTNA enhances compliance with regulatory standards such as GDPR and HIPAA by enforcing strict access controls and maintaining detailed activity logs. These logs provide organizations with an audit trail, simplifying regulatory audits and strengthening accountability. Research by Qazi (2022) noted that ZTNA's structured policies facilitate alignment with stringent compliance requirements, which are particularly relevant in data-sensitive sectors like healthcare and finance. Daley (2022) added that integrating advanced analytics into ZTNA frameworks can further streamline compliance processes, enhancing real-time threat detection and reporting capabilities.

ZTNA's scalability, a critical factor for organizations with distributed workforces, was another key finding. Unlike VPNs, which often face performance bottlenecks under heavy user loads, ZTNA maintains high performance by leveraging cloud-based architecture and adaptive security policies. Chen et al. (2023) demonstrated how ZTNA's dynamic access management scales effectively in hybrid and multi-cloud environments, ensuring consistent security without compromising user experience. Indran and Alwi (2024) suggested that integrating Secure Access Service Edge (SASE) principles into ZTNA frameworks could further improve scalability, particularly in environments relying on multiple cloud service providers.

In terms of usability, ZTNA supports seamless integration with modern IT infrastructure, including Bring Your Own Device (BYOD) policies. Anderson et al. (2022) identified that ZTNA's minimal latency during access authentication, coupled with its ability to dynamically adjust permissions based on context, improved user satisfaction. This balance between security and user experience is critical for organizations prioritizing both efficiency and robust access control. Moreover, as Kim et al. (2024) observed, ZTNA's adaptability positions it well for emerging technologies like IoT and 6G networks, where decentralized systems and real-time access management are vital.

Despite its benefits, ZTNA implementation poses several challenges. One major barrier, identified by Tuyishime et al. (2024), is the high initial investment required for advanced Identity and Access Management (IAM) systems, secure access gateways, and analytics tools. This financial burden can be prohibitive, especially for small to medium enterprises. Furthermore, integrating ZTNA with legacy systems requires extensive customization and infrastructure upgrades, which can delay deployment and inflate costs. As highlighted by Iță et al. (2023), overcoming these challenges often necessitates phased implementation and strategic resource allocation.

Another notable challenge lies in user adaptation. Transitioning to ZTNA often involves changes in authentication protocols, such as the adoption of multi-factor authentication (MFA), which may encounter resistance from employees. Qazi (2022), in their examination of ZTNA adoption, found that organizations with insufficient user education programs experienced slower transitions and lower compliance rates. Comprehensive training and engagement strategies, as suggested by García-Teodoro et al. (2022), are essential for overcoming this resistance, particularly in environments with a large and diverse user base.

ZTNA offers significant advantages over traditional VPNs in terms of security, scalability, and compliance, making it a superior choice for modern remote access requirements. While VPNs rely on implicit trust and grant broad network access, ZTNA enforces strict, identity-based access controls and continuous verification, which reduces risks associated with lateral movement and insider threats. Additionally, ZTNA is designed to integrate with cloud and hybrid environments, ensuring consistent performance and security even under heavy user loads. In contrast, VPNs often struggle with scalability, leading to bottlenecks in distributed workforces. Moreover, ZTNA provides enhanced compliance support through detailed logging and adaptive policies, aligning with modern regulatory standards like GDPR. These distinctions are summarized in Table 2 below.

Table 2: Comparative Analysis of ZTNA and Traditional VPNs

Aspect	**Traditional VPN**	**Zero-Trust Network Access (ZTNA)**
Trust Model	Implicit trust after authentication	Continuous verification, no implicit trust
Access Level	Broad network-level access	Application-specific access
Security Principle	Perimeter-based security	Identity-based, least-privilege access
Scalability	Limited scalability; prone to performance bottlenecks	High scalability; integrates with cloud environments
Granular Control	Limited; lacks role-specific access restrictions	High granularity; enforces context-aware permissions
Monitoring	Basic traffic monitoring	Continuous monitoring with real-time analytics
Compliance	Limited regulatory support	Enhanced compliance through detailed logging and policies

The table illustrates that ZTNA surpasses VPNs by addressing the limitations inherent in perimeter-based models. While VPNs grant excessive trust once a user is authenticated, ZTNA restricts access dynamically, adapting to real-time context and user roles. The added capabilities of continuous monitoring and identity-driven controls position ZTNA as a more robust solution for securing modern remote access environments. Federici et al. (2023) and Qazi (2022) have demonstrated the tangible benefits of these distinctions in practical applications, reinforcing ZTNA's growing adoption across industries.

6. Conclusions

This study evaluated the effectiveness of Zero-Trust Network Access (ZTNA) as a modern alternative to traditional VPN-based models for securing remote access. The findings confirm that ZTNA, through its identity-based and application-specific access controls, addresses significant vulnerabilities inherent in perimeter-based security frameworks. Unlike VPNs, which grant broad network-level access, ZTNA operates on the principles of "never trust, always verify," requiring continuous authentication and minimizing risks associated with lateral movement and insider threats. These advantages align with research by Federici et al. (2023), who emphasized ZTNA's capability to limit unauthorized access while enhancing operational security.

Moreover, ZTNA has demonstrated exceptional scalability and adaptability in cloud and hybrid environments, ensuring consistent performance for distributed workforces. Chen et al. (2023) highlighted ZTNA's role in maintaining secure access across multi-cloud architectures, showcasing its potential for large-scale deployments. Additionally, the implementation of micro-segmentation and real-time monitoring strengthens its security posture by limiting attack surfaces and providing timely breach detection. These features collectively position ZTNA as a critical framework for modern cybersecurity needs.

However, the adoption of ZTNA is not without challenges. High initial implementation costs and integration complexities, especially with legacy systems, remain significant barriers, as noted by Tuyishime et al. (2024). Organizations must also address user adaptation issues, as employees often resist transitioning to new authentication protocols. Addressing these hurdles requires strategic planning, phased deployment, and comprehensive training programs, which can facilitate smoother transitions and enhance adoption rates.

In summary, ZTNA provides a transformative solution for remote access security by overcoming the limitations of VPNs and aligning with the demands of modern, distributed networks. Its effectiveness in reducing breach risks, ensuring regulatory compliance, and supporting scalability makes it an ideal choice for organizations navigating increasingly complex cybersecurity landscapes. While challenges persist,

proactive measures can mitigate these obstacles, enabling organizations to fully leverage ZTNA's potential in securing their digital infrastructures.

Acknowledgments

The authors thank all members of the School of Computing who participated in this study. This study was carried out as part of the System and Network Security Project. This work was supported by Universiti Utara Malaysia.

References

Abuhasel, K. A. (2023). A zero-trust network-based access control scheme for sustainable and resilient industry 5.0. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10287925/

Anderson, J., Huang, Q., Cheng, L., & Hu, H. (2022, October). BYOZ: Protecting BYOD through zero trust network security. In 2022 IEEE International Conference on Networking, Architecture and Storage (NAS) (pp. 1-8). IEEE. https://ieeexplore.ieee.org/abstract/document/9925513/

Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. Journal of Computer Science and Technology Studies, 6(4), 54-59. https://al-kindipublisher.com/index.php/jcsts/article/view/7962

Brazhuk, A., & Fernandez, E. B. (2022, October). An abstract security pattern for zero trust access control. In Proceedings of the 29th Conference on Pattern Languages of Programs (pp. 1-5). https://dl.acm.org/doi/abs/10.5555/3631672.3631675

Chen, X., Feng, W., Ge, N., & Zhang, Y. (2023). Zero trust architecture for 6G security. IEEE Network. https://ieeexplore.ieee.org/abstract/document/10288499/

Daley, S. (2022). Evaluation of zero trust framework for remote working environments. Cybersecurity Journal, 12(3), 234-248. https://www.researchgate.net/profile/Sam-Daley/publication/357779759_Evaluation_of_Zero_Trust_framework_for_remote_working_environments/links/61df178a5c0a257a6fe34c29/Evaluation-of-Zero-Trust-framework-for-remote-working-environments.pdf

Deshpande, A. (2021). Relevance of zero trust network architecture amidst its rapid adoption driven by work-from-home scenarios. Psychology and Education Journal, 58(1), 5672-5677. https://pdfs.semanticscholar.org/f9d1/2dc64c5f8aa91492f0172a1827e7180d94ae.pdf

Fang, W., & Guan, X. (2022). Research on iOS remote security access technology based on zero trust. In 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC) (Vol. 6, pp. 123-130). IEEE. https://ieeexplore.ieee.org/abstract/document/9734455/

Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. Electronics, 12(3), 566. https://www.mdpi.com/2079-9292/12/3/566

García-Teodoro, P., Camacho, J., Maciá-Fernández, G., Gómez-Hernández, J. A., & López-Marín, V. J. (2022). A novel zero-trust network access control scheme based on the security profile of devices and users. Computer Networks, 212, 109068. https://www.sciencedirect.com/science/article/pii/S1389128622002109

Indran, S., & Alwi, N. H. M. (2024). Systematic literature review on secure access service edge (SASE) and zero trust network access (ZTNA) implementation to ensure secure access. Journal of Advanced Research in Applied Sciences and Engineering Technology, 182-195. http://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/article/view/6563

Iță, C. R., Constantinescu, R. C., Vlădescu, A., & Alexandrescu, B. (2023, March). Security in remote access, based on zero trust model concepts and SSH authentication with signed certificates. In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI (Vol. 12493, pp. 684-691). SPIE. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12493/124932T/Security-in-remote-access-based-on-zero-trust-model-concepts/10.1117/12.2643058.short

Kim, H., Kim, Y., & Kim, S. (2024). A study on the security requirements analysis to build a zero-trust-based remote work environment. arXiv preprint, arXiv:2401.03675. https://arxiv.org/abs/2401.03675

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: An approach to support work-from-home driven by the COVID-19 pandemic. New Generation Computing, 39(3), 599-622. https://link.springer.com/article/10.1007/s00354-021-00130-6

Peterson, E. (n.d.). Achieving visibility and control in OT systems: Remote maintenance, securing remote access, and the zero-trust approach. Cybercore Integration Center, Idaho National Laboratory. Retrieved from https://www.cisa.gov/sites/default/files/2023-05/Achieving%20Visibility%20and%20Control%20in%20OT%20Systems%20Remote%20Maintenace%2C%20Securing%20Remote%20Access%2C%20and%20the%20Zero-Trust%20Approach_508c.pdf

Qazi, F. A. (2022, December). Study of zero trust architecture for applications and network security. In 2022 IEEE 19th International Conference on Smart Communities:

Improving Quality of Life Using ICT, IoT, and AI (HONET) (pp. 111-116). IEEE. https://ieeexplore.ieee.org/abstract/document/10019186/

Tuyishime, E., Radu, F., Cotfas, P., Cotfas, D., Balan, T., & Rekeraho, A. (2024, June). Online laboratory access control with zero trust approach: Twingate use case. In 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/10607562/

Wu, Y. G., Yan, W. H., & Wang, J. Z. (2021, August). Real identity-based access control technology under zero trust architecture. In 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG) (pp. 18-22). IEEE. https://ieeexplore.ieee.org/abstract/document/9616576/

Yiliyaer, S., & Kim, Y. (2022, January). Secure access service edge: A zero-trust-based framework for accessing data securely. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 586-591). IEEE. https://ieeexplore.ieee.org/abstract/document/9720872/

Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero trust VPN (ZT-VPN): A cybersecurity framework for modern enterprises to enhance IT security and privacy in remote work environments. Cybersecurity Research Review, 14(1), 23-40. https://www.preprints.org/manuscript/202410.0301