**Borneo International Journal eISSN 2636-9826**; Vol. 7 (4); 2024; 28-34
Published by *Majmuah Enterprise*
www.majmuah.com

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

HON JUN.YOON, MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 UUM Sintok
*Kedah Darul Aman, MALAYSIA*
Email: hon_jun_yoon@soc.uum.edu.my, m.fadli.zolkipli@uum.edu.my | Tel: +60173216633,

Received: November 18, 2024
Accepted: November 22, 2024
Online Published: December 01, 2024

**Abstract**

The surge in remote work and reliance on cloud environments has exposed major weaknesses in traditional security methods like Virtual Private Networks (VPNs). These methods, which use perimeter-based security, often provide excessive trust after the initial authentication step, leaving systems vulnerable to lateral movement and unauthorized access. Zero-Trust Network Access (ZTNA) provides a better alternative by emphasizing continuous verification and stringent controls at the application level. This study explores how ZTNA can effectively replace traditional VPNs, focusing on its key principles, challenges in implementation, and security benefits. By conducting detailed analysis and evaluating real-world case studies, the research finds that ZTNA not only minimises risks associated with lateral movement but also improves compliance with regulatory standards and supports scalability in distributed and remote settings. The findings highlight ZTNA's versatility in securing remote access for modern use cases.

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 surge in remote work and the increasing adoption of cloud services has exposed critical weaknesses in traditional security models. Virtual Private Networks (VPNs), which were originally designed to provide encrypted remote connections, operate on a perimeter-based model that assumes implicit trust once a user has been authenticated. This approach grants broad access to the network, increasing the risks of unauthorized actions, lateral movement, and insider threats. As remote work becomes a permanent feature of modern work environments, these vulnerabilities have pushed organisations to search for more robust alternatives. Zero-Trust Network Access (ZTNA) has emerged as a practical solution to address these issues. Unlike VPNs, ZTNA operates on the principle of "never trust, always verify," requiring constant authentication and using context-aware access controls. It restricts access to specific applications and enforces stringent identity and device-based permissions, improving security and meeting the requirements of modern regulations. This study aims to evaluate how effective ZTNA is in overcoming the limitations of traditional VPNs. It examines the fundamental principles of ZTNA, its key components, and the challenges faced by organisations when implementing it. By analysing theoretical concepts and real-world applications, this paper provides insights into how ZTNA supports secure, scalable, and compliant remote access.

The paper begins with a background overview and the principles of ZTNA, followed by a review of literature that tracks the evolution of remote access security. The methodology section outlines the approach used for data collection and analysis. This is followed by case studies and findings, which showcase the advantages and challenges of ZTNA. Lastly, the paper concludes with recommendations for successful adoption.

## 2. Literature Review

The evolution of remote access security has been significantly influenced by the rise of cloud computing and decentralised work environments. Traditionally, perimeter-based security models dominated the field, relying heavily on Virtual Private Networks (VPNs) to establish encrypted tunnels for remote connections. VPNs operate on an implicit trust model, granting users wide access to the network once authenticated. While this model worked well for centralised, on-premises systems, it has proven inadequate for today's distributed networks. The rapid growth of remote work has exposed these shortcomings, especially when it comes to scalability, insider threats, and credential-based attacks. Research has shown that VPNs have inherent vulnerabilities due to their implicit trust model, which creates a single point of failure. Deshpande (2021) highlighted how this can lead to unauthorised access. VPNs also lack

granular access controls, often allowing lateral movement across networks if a breach occurs. Performance bottlenecks are another common issue when supporting large and distributed workforces, reducing efficiency in cloud-driven environments. Traditional VPNs, while suitable in the past, are no longer able to meet the needs of decentralised networks. Mandal, Khan, and Jain (2021) argued that the perimeter-based security approach assumes inherent trust, making it ill-suited for environments vulnerable to insider threats and credential-based attacks. Additionally, VPNs rely on encrypted tunnels for data transmission, which, while secure, provide limited control over user permissions. Peterson (2021) observed that organisations using traditional models often lack visibility into user activity, leaving significant gaps in their security systems. In response to these challenges, the Zero-Trust Security model was introduced, promoting continuous verification and adaptive access controls. Wu, Yan, and Wang (2021) expanded on this by introducing real-identity-based controls, aligning permissions with dynamic contextual factors like user behaviour and device health. These features address the limitations of VPNs, bridging the gap between user access and resource protection.

ZTNA has proven to be effective in addressing VPN-related risks. For instance, identity-based access controls in ZTNA ensure permissions are aligned strictly with user roles, limiting unauthorised access (Bashir, 2024). Additionally, micro-segmentation enhances security by isolating network resources and restricting the movement of potential attackers. Continuous monitoring further enables real-time detection of threats, allowing for initiative-taking responses to emerging risks (Chen et al., 2023). ZTNA also offers advantages in adapting to future challenges, such as securing technologies like 6G and Internet of Things (IoT) networks. Kim et al. (2024) noted that ZTNA's dynamic policy enforcement and micro-segmentation principles can address latency and interoperability challenges in these decentralised environments. Similarly, Indran and Alwi (2024) emphasised that integrating Secure Access Service Edge (SASE) principles into ZTNA enables consistent and scalable security across multi-cloud infrastructures. Despite its strengths, ZTNA faces challenges, such as integration complexities and high initial costs, which can limit adoption—particularly for small and medium enterprises. Daley (2022) suggested that incorporating advanced analytics and AI systems into ZTNA frameworks could improve its adaptability by enabling predictive threat detection and dynamic policy adjustments. These capabilities, combined with user-centric strategies like real-identity-based controls, could enhance compliance and reduce operational difficulties during implementation.

By addressing the limitations of VPNs and meeting the demands of modern networks, ZTNA has established itself as a superior framework for secure remote access. Table 1 below provides a summary of key studies, highlighting ZTNA's advantages, methodologies, and the challenges identified.

**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 BYOD scenarios using ZTNA. | Complexity in policy management; user resistance to stricter controls. |
| Brazhuk & Fernandez (2022) | Abstract Security Pattern for ZTNA | Theoretical Framework | ZTNA minimises 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 assess the effectiveness of Zero-Trust Network Access (ZTNA) as a secure alternative to Virtual Private Networks (VPNs) for remote access. By combining qualitative and quantitative methods, the research offers a thorough analysis of theoretical framework and case studies The research design was divided into two phases. The exploratory phase focused on reviewing existing literature and analysing 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 valuable insights into ZTNA's principles and key components. This phase also identified specific challenges in VPN-based security models, such as scalability issues and vulnerability to lateral movement. The second phase, the analytical phase, involved evaluating quantitative data from case studies and surveys to measure ZTNA's performance in areas like access control efficiency and breach reduction rates. For example, the breach reduction percentages from Anderson et al. (2022) provided quantifiable evidence of ZTNA's superior security outcomes in various environments. Literature reviews is used as the main method of data collection. The literature review utilised peer-reviewed articles, conference papers, and industry reports from reliable sources like IEEE Xplore and SpringerLink. These resources offered detailed perspectives on ZTNA implementation, highlighting both benefits and challenges.

Thematic and comparative analysis methods were employed for data interpretation. Thematic analysis identified recurring patterns in ZTNA implementation, such as the emphasis on micro-segmentation and real-time monitoring. By grouping themes like scalability and compliance, qualitative data was structured into actionable insights. Comparative analysis was used to quantify the advantages of ZTNA over VPNs. Metrics like breach reduction percentages and user satisfaction scores provided a measurable understanding of ZTNA's effectiveness. The chosen methodology, integrating exploratory and analytical approaches, ensured a balanced evaluation of ZTNA. This comprehensive approach provides a robust foundation for assessing ZTNA's potential to revolutionise remote access security frameworks.

## 4. Case Studies

The practical implementation of Zero-Trust Network Access (ZTNA) across various industries highlights its effectiveness in enhancing remote access security while addressing unique organisational challenges. This section highlights key use cases involving corporate remote access and cloud-based services, demonstrating how ZTNA improves security, scalability, and operational efficiency. In corporate settings, ZTNA has been instrumental in addressing risks associated with the broad network access granted by VPNs. For instance, a study by Tuyishime et al. (2024) on ZTNA deployment in a remote laboratory environment revealed how identity-based access controls restricted unauthorised entry to sensitive resources. By enforcing role-specific permissions and context-aware authentication, ZTNA facilitated secure and granular access while improving compliance with organisational security policies. These findings are particularly significant for infrastructures where remote employees regularly access diverse applications. The same study also demonstrated ZTNA's scalability. Organisations successfully supported increasing numbers of remote users without experiencing major performance issues. This scalability is crucial in dynamic work environments, where workforce size and access requirements often change rapidly. Tuyishime et al. noted, however, that integration challenges, especially in systems relying on legacy infrastructure, emerged during the implementation process. These challenges underline the importance of strategic infrastructure planning and technical expertise, as highlighted by Iță et al. (2023), who stressed the role of segmentation controls in streamlining implementation efforts.

ZTNA has also proven valuable for securing cloud-based operations, which are now central to modern remote work strategies. Brazhuk and Fernandez (2022), in their analysis of ZTNA in multi-cloud environments, emphasised its ability to enforce consistent security policies across various cloud platforms. Centralised policy management ensured compliance with security standards and maintained protection against threats, even in organisations using multiple cloud service providers. Indran and Alwi (2024) further noted that integrating Secure Access Service Edge (SASE) principles into ZTNA frameworks can simplify policy enforcement and enhance scalability in multi-cloud setups. Another critical feature of ZTNA is micro-segmentation, which plays a pivotal role in limiting lateral movement during potential breaches. By isolating resources into distinct zones, ZTNA minimises access for both users and attackers. While Brazhuk and Fernandez acknowledged that micro-segmentation requires substantial customisation due to varying cloud provider protocols, the enhanced security outcomes outweigh these initial complexities. For example, ZTNA's segmentation capabilities were particularly beneficial in industrial environments, where they effectively restricted attackers' access to sensitive IoT systems (Abuhasel, 2023).

Across both case studies, ZTNA consistently demonstrated a stronger security posture by employing continuous monitoring and adaptive security policies. Advanced analytics, as proposed by Daley (2022), further enhance ZTNA

frameworks by enabling real-time anomaly detection and dynamic policy enforcement. For example, Anderson et al. (2022) found that integrating multi-factor authentication (MFA) with context-aware access controls significantly reduced unauthorised access risks. However, challenges such as high implementation costs and integration difficulties remain prevalent. Organisations deploying ZTNA often face obstacles in aligning new security protocols with pre-existing systems. Fang and Guan (2022) observed that these challenges often require significant investments in infrastructure upgrades and technical training, which can strain resources, particularly for small and medium enterprises. Addressing these barriers requires strategic planning, phased implementation, and ongoing support. Furthermore, Kim et al. (2024) highlighted that compatibility issues with evolving technologies, such as IoT and 6G, require 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 addresses the vulnerabilities inherent in traditional VPN models. Despite implementation hurdles, the demonstrated benefits establish ZTNA as an essential framework for organisations navigating modern security challenges.

## 5. Findings and Discussion

The findings of this study highlight the significant advantages of Zero-Trust Network Access (ZTNA) compared to traditional VPN-based security models. By addressing inherent vulnerabilities in perimeter-based security, ZTNA demonstrates its ability to enhance remote access security through continuous verification and identity-based access controls. These findings are consistent across literature and real-world case analyses. ZTNA adoption has led to noticeable improvements in organisational security, particularly by reducing the risk of unauthorised access. For instance, Fang and Guan (2022) reported a 30% reduction in breach attempts following ZTNA implementation in corporate settings. Identity-based access controls were key in mitigating risks associated with credential theft. Moreover, ZTNA's micro-segmentation confined access to specific application zones, effectively limiting lateral movement—one of the major weaknesses in traditional VPN frameworks. By segmenting networks into smaller, secure zones, as observed by Federici et al. (2023) and Abuhasel (2023), ZTNA prevents attackers from escalating privileges or compromising multiple resources. ZTNA also strengthens compliance with regulatory standards, such as GDPR and HIPAA, by enforcing strict access controls and maintaining detailed activity logs. These logs provide an audit trail that simplifies regulatory audits and improves accountability. Research by Qazi (2022) noted that ZTNA's structured policies align seamlessly with stringent compliance requirements, which is particularly relevant in industries like healthcare and finance. Daley (2022) added that integrating advanced analytics into ZTNA frameworks enhances compliance processes by enabling real-time threat detection and more efficient reporting.

Scalability is another critical advantage of ZTNA, particularly for organisations with distributed workforces. Unlike VPNs, which often encounter performance bottlenecks when managing large numbers of users, 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 further improves scalability, particularly for organisations relying on multiple cloud service providers. In terms of user experience, ZTNA provides seamless integration with modern IT infrastructures, including Bring Your Own Device (BYOD) policies. Anderson et al. (2022) found that ZTNA's minimal latency during access authentication and its ability to dynamically adjust permissions based on context improved user satisfaction. This balance between security and user convenience is crucial for organisations prioritising efficiency alongside robust access controls. Additionally, Kim et al. (2024) highlighted ZTNA's adaptability to emerging technologies like IoT and 6G networks, where real-time access management and decentralised systems are essential.

Despite its benefits, ZTNA implementation presents challenges. One major barrier is the high initial investment required for advanced Identity and Access Management (IAM) systems, secure access gateways, and analytics tools. As Tuyishime et al. (2024) observed, this financial burden can be prohibitive for small and medium enterprises. Furthermore, integrating ZTNA with legacy systems requires extensive customisation and infrastructure upgrades, leading to delays and inflated costs. Iță et al. (2023) suggested that phased implementation and strategic resource allocation can mitigate these challenges. Additionally, other significant challenge is user adaptation. Transitioning to ZTNA often involves new authentication protocols, such as multi-factor authentication (MFA), which may face resistance from employees. Qazi (2022) reported slower adoption rates and reduced compliance in organisations that lacked comprehensive user education programs. García-Teodoro et al. (2022) recommended training and engagement strategies to overcome this resistance, particularly in organisations with a large and diverse workforce.

In summary, ZTNA provides significant improvements over traditional VPNs in terms of security, scalability, and compliance. This makes it a superior choice for modern remote access requirements. While VPNs operate on implicit trust and grant broad network access, ZTNA enforces strict, identity-based controls and continuous verification. This reduces risks like lateral movement and insider threats. Additionally, ZTNA integrates seamlessly with cloud and hybrid environments, maintaining consistent performance under heavy user loads. In contrast, VPNs often struggle with scalability, leading to bottlenecks in distributed workforces. Enhanced compliance support through detailed logs and adaptive policies further aligns ZTNA with modern regulatory standards like GDPR. The comparison between ZTNA and traditional VPNs is summarised 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 |

Table 2 shows that ZTNA surpasses VPNs by addressing the inherent limitations of perimeter-based security models. It restricts access dynamically, adapting to real-time contexts and user roles, while providing advanced monitoring and identity-driven controls. These features position ZTNA as a robust solution for modern remote access challenges, as evidenced by practical applications highlighted in studies by Federici et al. (2023) and Qazi (2022).

## 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 effectively addresses significant vulnerabilities in perimeter-based security frameworks by leveraging identity-based and application-specific access controls. Unlike VPNs, which grant broad network access after authentication, ZTNA operates on the principles of "never trust, always verify." This approach ensures continuous authentication, minimising risks like lateral movement and insider threats. These advantages align with research by Federici et al. (2023), which highlighted ZTNA's ability to limit unauthorised access while improving operational security. Additionally, ZTNA has proven to be highly scalable and adaptable for cloud and hybrid environments, maintaining consistent performance even for distributed workforces. Chen et al. (2023) demonstrated how ZTNA supports secure access across multi-cloud architectures, highlighting its potential for large-scale deployments. Features like micro-segmentation and real-time monitoring further enhance ZTNA's security capabilities by reducing attack surfaces and providing timely breach detection. These factors collectively establish ZTNA as a critical framework for modern cybersecurity needs.

Despite its strengths, ZTNA implementation comes with challenges. High initial implementation costs and integration complexities, especially with legacy systems, remain significant barriers to adoption. Tuyishime et al. (2024) noted that these challenges often require substantial investments in infrastructure upgrades and technical training, which can strain resources, particularly for small and medium enterprises. Strategic planning, phased deployment, and targeted training programs are crucial to overcoming these hurdles. Another challenge lies in user adaptation. Changes in authentication protocols, such as the introduction of multi-factor authentication (MFA), often face resistance from employees. Organisations that fail to implement comprehensive user education programs experience slower adoption rates and reduced compliance. To address this, García-Teodoro et al. (2022) recommended user-centric strategies, including engagement and training, to ensure a smoother transition. In conclusion, ZTNA offers a transformative solution for remote access security by effectively overcoming the limitations of traditional VPNs. Its ability to reduce breach risks, ensure regulatory compliance, and support scalability makes it an ideal choice for organisations navigating the increasingly complex cybersecurity landscape. While implementation challenges persist, initiative-taking measures can mitigate these issues, allowing organisations to fully leverage ZTNA's potential to secure their digital infrastructures.

**Acknowledgments**

The authors thank all members of the School of Computing who participated in this study. This study was conducted 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