*International Journal of Infrastructure Research and Management*
*Vol. 10 (1), June 2022, pp. 44 - 53*

# A COMPREHENSIVE SWOT ANALYSIS FOR ZERO TRUST NETWORK SECURITY MODEL

Tadiwa Elisha Nyamasvisva and Atiff Abdalla Mahmoud Arabi
*Infrastructure University Kuala Lumpur, MALAYSIA*

## ABSTRACT

The Zero Trust approach is a cybersecurity preventive measure based on the notion that nothing should be trusted within or near, or outside your network unless their identities are validated. Identities are regularly verified using authentication and authorization mechanisms in this framework. Security does not end once a user enters the network; identities are continually confirmed as they travel across the network. Instead of relying on network perimeters, Zero Trust's approach to security focuses on your identity infrastructure. Systems and networks can no longer rely on a user's affiliation with an organization or the password they supply. Users' traits and activity patterns must be examined by systems and networks to determine who is attempting to access resources, how they might get access, and what they might do with that access. This is a case of Zero Trust. Zero Trust has pros and limitations when compared to other security systems. It is also seen as the final answer to decentralized usage of resources over the internet. This paper's prescription focuses on Zero Trust's strengths, shortcomings, possibilities, and threats.

**Keywords:**
*Virtual Private Networks (VPNs), Multi-Factor Authentication (MFA), Bring Your Own Device (BYOD), Network segmentation, Software Defined Perimeter (SDN)*

## INTRODUCTION

Security in networks is an evolving challenge that needs to be scrutinized (Andrade, Ortiz-Garces, & Cazares, 2020). Some approaches to network security have worked for extended periods of time with minor alterations to the entire framework of security (Uctu, Alkan, Dogru, & Dorterler, 2019). Significant changes are always required when there are major shakeups at the technology forefront. The introduction of new modern technologies brings about new challenges and always opens once patched loopholes for exploitation (D'Silva & Ambawade, 2021). In traditional network security (Sreeja, Saleem, & Sravya, 2020), security was about protecting the boundaries of the environment; with time more ubiquitous methods started to be introduced.

The recent cybersecurity breaches have had a massive impact. Traditional security measures are ineffective in the face of billions of compromised identities and sensitive data. According to recent data breaches, three out of every five businesses anticipate being hacked. Finding and containing a malicious actor takes an average of 74 days, and privileged credentials are used in 80 percent of breaches. Furthermore, within a 24-hour period, 67 percent of firms penetrated were unable to submit a report indicating who has access to essential systems and accounts (Alkhalil, Hewage, Nawaf, & Khan, 2021). What this demonstrates is that the perimeter as we know it is no longer functional, and the once-defensible perimeter has become the new network attack route (Alkhalil et al., 2021).

Internal and external attacks exploiting current access and compromising the perimeter continue to progress the attack lifecycle (Andrade et al., 2020). Once inside, bad actors can use elevated access to conduct reconnaissance and move laterally through the network, disrupting operations and stealing data (Sreeja et al., 2020).

The infrastructure of a typical business has become increasingly sophisticated. Several internal networks, remote offices with their own local infrastructure, remote and/or mobile personnel, and cloud services may all be run by a single company. Because there is no one readily identifiable border for the company, old perimeter-based network security approaches have been outperformed.

Boundary-based network security has also been proved to be insufficient because once attackers break the perimeter, they have unrestricted access to the whole of the network (Rose, Borchert, Mitchell, & Connelly, 2020).

As a result of this complicated operation, a new cybersecurity paradigm is known as "zero trust" has been developed (ZT). The primary focus of a ZT strategy is data and service security, but it may and should be broadened to encompass all corporate assets and subjects. The term "zero trust" refers to a security reaction to corporate network developments such as remote users, bring your own device (BYOD), and cloud-based assets that are not within an enterprise-owned network perimeter. This is a common practice in industry and education as the focus centered more on cloud and cloud-related activities (Abu-Asba, Azman, Mustaffa, & Ali, n.d.; Hasan, Ibrahim, Mustapha, Islam, & Al Younus, 2018).

## BACKGROUND

From the network perimeters, a typical model for network security oversees access to an organization's networks and related assets, resources, and apps (Sreeja et al., 2020). This is known as the castle and trench paradigm, and it involves the deployment of security protocols such as firewalls, Virtual Private Networks (VPNs), access controls, email security, online security, and Security Information and Event Management (SIEM), including self-defined algorithms for tracking users (Sibghatullah H M, Elisha Tadiwa, Atiff Abdalla Mahmoud, Abudhahir, & Fares Anwar Salem, 2021)to name a few. Table 1 below outlines some of the classic network security techniques over time.

Table 1: Timeline of Security Approaches

| Period | Security Approaches |
|---|---|
| Before 2000 | Firewall with MDS and Bastion Host |
| | VLAN infrastructure |
| | QoS |
| 2000 to 2010 | The extension of VM |
| | VL and virtual network environments, |
| | Multiple DMZ with VPN concentrators |
| | Multi-factor for remote access. |
| | IDS |
| | IPS |
| | 802.1x |
| | Comprehensive QoS and PoS across both LAN and WAN |
| 2010 till 2020 | Network Segmentation |
| | Next generation firewalls |
| | Identity and Access management |

However, as more businesses migrate from on-site to hybrid settings and cloud environments, and as several employees work remotely and with their own devices, it is becoming more challenging to safeguard network perimeters and keep track of who goes laterally within the network (Sreeja et al., 2020). As a result, businesses are taking a broader approach to network security.

## ZERO TRUST AS A COMPLETE SOLUTION

VPNs and SDNs complement each other when it comes to network security (Van Der Pol, Gijsen, Zuraniewski, Romão, & Kaat, 2016). These approaches are ok to some extent, but they are not comprehensive enough to completely secure network-based resources. There are several issues related to traditional networks, including but not limited to;

i. Lack of principle of least privilege (PoLP).
ii. Noncompliance to multi-factor authentication (MFA)
iii. No use of micro-segmentation.
iv. Lack of audit to the network.

The growing complexity of dynamic workloads moving across the data center and multi-cloud environments, remote users, and endpoints, combined with a flood of new vulnerabilities and risks from hackers and targeted threats such as ransomware and malware outbreaks, have exposed the inadequacy of traditional security models (Greenwood, 2021). Zero Trust addresses the four shortcomings as part of its offering (Simpson & Foltz, 2021). Adopting Zero Trust architecture is more important than ever since most businesses operate in a multi-cloud environment with distributed and remote workforces. An identity-centric approach to your Zero Trust model should be at the centre of your organization's security architecture. (Atiff, David, & Elisha, 2021).

The Zero Trust Security idea adopts a new access model in which all users are seen as untrustworthy (Chen et al., 2020; Xiaojian, Liandong, Jie, Xiangqun, & Qi, 2021). It represents a paradigm change away from traditional perimeter-based access and toward a user-centric strategy (Redondi, Chirico, Borsani, Cesana, & Tagliasacchi, 2013; Vanickis, Jacob, Dehghanzadeh, & Lee, 2018). Zero Trust is an all-encompassing security approach for people, apps, data, and networks that combines strong authentication principles, multi-factor authentication, step-up authentication, and the use of contextual access limitations and interrogation (Mehraj & Banday, 2020).

"Never trust, always verify." This Zero Trust philosophy-turned-strategy fundamentally changes the way security is approached since trust is a vulnerability that can be exploited (Wylde, 2021). Cloud applications and security are treated equally to on-premises systems and apps under the Zero Trust approach (Rodigari, O'Shea, McCarthy, McCarry, & McSweeney, 2021). For improved identification of risks and breaches, the model supports the use of sophisticated analytics, artificial intelligence, and machine learning. To implement Zero Trust successfully, these three stages are proposed for a holistic and highly effective security strategy for Zero Trust. The three stages are the discovery stage, the definition stage, and the enforcement stage. Table 2 below describes these three stages.

Table 2: ZT Implementation Guidelines

| Stage | Process | Description |
|---|---|---|
| 1 | Discovery | - Determine how users, devices, and apps are connected.<br>- Real-time mapping across endpoints and applications<br>- Mapping of sensitive data across users, devices, networks, workloads, and applications<br>- Enabling a single source of truth |
| 2 | Definition | - Micro-segmentation controls<br>- Automated policy creation.<br>- Compensation of control when it cannot be patched.<br>- Visualize and test policies |
| 3 | Enforcement | - Enable a default-deny policy<br>- Secure data in transit |

| | | |
|---|---|---|
| | | - Continuous monitoring<br>- Dynamic Zero Trust policies<br>- Seamless integration with third-party IT tools |

The discovery process is used to determine what should be permitted to communicate based on the principle of least privilege. The discovery approach also encourages cooperation by including business and IT stakeholders in the creation of Zero Trust micro perimeters and security regulations. Understanding what is communicating and what should not be communicating is crucial in the discovery process as a vital initial step. By defining and automating the appropriate amount of Zero Trust segmentation rules across endpoints, the described process assures risk reduction and reduces deployment complexity. The second phase is likewise in charge of enforcement, ensuring that when offering security at birth in cloud-native apps, no applications are broken. Using an allow list, enforcement enables a decoupled default-deny policy to implement effective Zero Trust rules wherever your endpoints and workloads are located. Without needing any adjustments or upgrades to the existing network, data in transit is safeguarded.

## ZT STRENGTHS

Many of the pillars upon which IT and security are based may be strengthened by incorporating Zero Trust into the core of an organization's infrastructure. Zero Trust can help companies enhance their security posture and restrict their attack surface by introducing some fundamental barriers to entry and enabling access on an as-needed basis, whether it's in fortifying identity and access controls or segmenting data. Table **3** below describes the strengths of Zero trust.

Table 3: The strengths of Zero Trust

| No | Strength | Explanation |
|---|---|---|
| 1 | Less vulnerability | – The Zero Trust paradigm improves the company's security, particularly against in-network lateral attacks that may appear under a different security model. |
| 2 | Strong policies for user identification and access. | – Zero Trust necessitates tight user control within the network, resulting in more secure accounts.<br>– Using multi-factor authentication, which goes beyond passwords and includes biometrics, as an effective technique to keep accounts secure.<br>– Categorization of users for the purpose of allowing them access to data and accounts as needed for their job duties. |
| 3 | Smart segmentation of data. | – Dividing a company's network into compartments, protecting critical intellectual property from illegal users<br>– Lowering the attack surface by keeping susceptible systems well-protected<br>– Threats should not be allowed to migrate laterally across the network.<br>– Reducing the effects of insider threats, particularly those that may endanger employees physically. |
| 4 | Increased data protection. | – Keeping data secure in both storage and transit.<br>– Backups that are automated are encrypted and hashed, and the message transmission is encrypted and hashed. |

| | | |
|---|---|---|
| | | – Restricting data access<br>– By segmenting the assault surface, we may reduce the attack surface.<br>– Edge encryption, scrambled data, automatic backups, and leaky bucket security |
| 5 | Good security orchestration | – Make sure that all of your security features function together efficiently and effectively, with no gaps left unfilled and the integrated elements complementing one another rather than showing inconsistencies between them.<br>– Zero Trust guarantees that security solutions integrate smoothly and cover all potential attack routes.<br>– Finding the optimal settings to enhance productivity while minimizing disputes. |

In a Zero Trust paradigm, there would be no one large pool of data that all users could access. (Ahmed, Nahar, Urmi, & Taher, 2020). Data may be segmented by kind, sensitivity, and purpose for a more secure arrangement. This protects essential or sensitive data while reducing potential attack surfaces. Without adequate data and resource segregation, robust access controls won't make sense with Zero Trust. The necessity of security orchestration runs across all of these pillars. Organizations employing Zero Trust would need to guarantee that security solutions function effectively together and cover all potential attack vectors even if they didn't have a security management system (Mehraj & Banday, 2020). Overlap isn't an issue in and of itself, but finding the optimal settings to enhance efficiency while minimizing conflicts may be difficult.

## ZT WEAKNESSES

With all of these added security benefits, the Zero Trust approach complicates security policies. Here are some of the extra obstacles that such a thorough plan entails. (See table 4):

Table 4: The Weaknesses of Zero Trust

| No | Weakness | Explanation |
|---|---|---|
| 1 | Time and effort to set up. | - Challenging in reorganizing policies within an established network.<br>- Maintaining functionality during the shift.<br>- Better to design a new network from scratch and then shift over.<br>- Incompatible Legacy networks with the Zero Trust architecture require starting from scratch. |
| 2 | Increased management of varied users. | - It may be challenging to reorganize policies inside the existing network while they continue to function during the transition.<br>- Preferable to design a new network from scratch and then shift over.<br>- If legacy systems are incompatible with the Zero Trust architecture, the process must be restarted. |
| 3 | More devices to manage. | - Current work environments comprise not only diverse sorts of workers but also varied types of equipment. |

| | | |
|---|---|---|
| | | - Different devices with unique attributes and connection methods must be monitored and protected always. |
| 4 | More complicated application management. | - A more comprehensive range of varying applications.<br>- Cloud-based apps are frequently used across various platforms. They may be disclosed to third parties.<br>- App use should be planned, monitored, and designed in accordance with a Zero Trust attitude. |
| 5 | More careful data security. | - Data is being housed in several locations, which means there are more places to defend.<br>- Data configuration must be done responsibly and in accordance with the highest security requirements. |

**ZT OPPORTUNITIES**

The Zero Trust approach does not explicitly call for achieving complete effectiveness. Zero Trust emphasizes that businesses must start with the user's identification. A solid identity governance and management plan must be in place. As the name implies, Zero Trust offers a surplus of possibilities. See table 5 below.

Table 5: The Opportunities of Zero Trust

| No | Opportunity | Explanation |
|---|---|---|
| 1 | Principle of least privilege (PoLP) | The Zero Trust principle is based on the Principle of Least Privilege (PoLP) (DelBene, Medin, & Murray, 2019; Mehraj & Banday, 2020). The concept of least privilege, often known as least privilege access, is a security protocol that assumes that everyone is a potential danger and that; as a result, they should only be provided the rights necessary to accomplish their job function. The notion of least privilege may be extended to programmes, apps, systems, and gadgets in addition to human users (Christ, 2021; Gómez, Alonso-Zárate, Verikoukis, Pérez-Neira, & Alonso, 2007). By restricting user access from within the network, least privilege access helps to protect and secure privileged credentials, data, and assets. As a result, if an attacker gains access to your IT environment, PoLP minimizes their chances of acquiring access to a privileged account, lowering the risk of a data breach. |
| 2 | Multi-factor authentication (MFA) | Authentication should be at the heart of every cybersecurity strategy, especially in the case of Zero Trust (Stafford, 2020). There are several authentication techniques available, but multi-factor authentication provides an extra degree of protection by requiring a user to give various pieces of proof (factors) in order to validate their identity and obtain access to a network or multi-cloud environment (Uttecht, 2020). Methods of multi-factor authentication for verification include:<br>i. "Something you know: username, password, or pin number."<br>ii. "Something you have: mobile device or app."<br>iii. "Something you are: biometrics such as a fingerprint, face, or voice recognition software" |

| | | |
|---|---|---|
| 3 | Micro-segmentation. | Micro-segmentation divides a data centre or cloud environment into different segments, limiting user access to specific regions based on their organizational position (Mujib & Sari, 2020). As a result, the user and their workload are protected and isolated to a single network segment until they have the authorization to travel elsewhere.<br>It provides insight into all network activity, allowing administrators to create exact segmentation based on what they see and prevent any risks from spreading laterally across the network. (Sheikh, Pawar, & Lawrence, 2021). |
| 4 | Network Audit. | Your Zero Trust solution must be implemented for all users and systems in your IT ecosystem in order to be effective (Li, Zhang, Lei, & Song, 2022). Begin by auditing the identities, access limitations, and access policies on your network. Understanding where your data and applications live, as well as access policies and access controls such as who has access and how they use that access, are vital stages of considering as you begin to develop the security and access protocols for your network. |
| 5 | Assured Security | Adoption of an identity and access management system capable of validating these users' identities before granting them access to your network and apps, provisioning access based on user roles, and using policy management to automate, regulate, and monitor how their access is used within the network. A firm Zero Trust policy ensures the safety of all users, apps, and data. |

Opportunities from Zero Trust largely present themselves within the versatile identity strategies, which vary according to the application domain and are never similar in many instances. These should include but are not limited to:

- Identity governance controls for roles, entitlements, appropriateness, and SOD policies, as well as risk
- Lifecycle automation for all identities, including workers, contractors, business partners, and machines
- Strong/multi-factor authentication and credential management
- Privileged account and entitlement management
- Centralized application access and self-service fulfillment
- Certification, auditing, and reporting of access

## ZT THREATS

There will always be some dangers when a novel solution to a complex problem evolves and appears over time. It takes more than a shift in thinking to implement a Zero Trust security strategy in a business. It will necessitate a thorough understanding of the company's departments' functions, present software, access levels, and devices, as well as what each of those requirements will look like in the future. This is the most severe danger. Because the existing network must stay operational during the transition time, constructing a Zero Trust network from the bottom up is often easier than reconfiguring an existing network into Zero Trust. In all circumstances, IT and security teams should develop a strategy that includes the ideal ultimate infrastructure as well as a step-by-step plan for getting there.

## CONCLUSION

Zero Trust as a concept is not a specific product or solution. It is a paradigm shift in the way we think about security. People are the new security perimeter, according to Zero Trust. The new firewall is identity, and it should be at the heart of every Zero Trust plan. Analytics provide an extensive context for access control choices, policy enforcement, and abnormal activity identification. An identification strategy makes access simple and safe while also ensuring that it is the correct access at the right time. To reduce the danger of entitlement creep, orphaned accounts, and separation of duties and appropriateness policies, the strategy should define and regulate access permissions. When properly deployed, the solution will reveal who has access to what and when. Who should have access to the information? What are they going to do with it now that they have it?

Access control is critical in the Zero Trust strategy. During the authentication and authorization process, identity context is reviewed to ensure that a user is who they say they are, that they are using the correct device and that they are accessing the network from an authorized location. This is to control premeditated unauthorized dishonest activities (Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, 2020; Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Buhari, & Wong, 2020). Identity identifies and grants the access they should have while also eliminating any access that is inappropriate, unneeded, or no longer required. An identification approach should comprise high-value assets (HVA), sensitive and critical data, structured applications, unstructured data, hosts, and networks. Cloud and on-premises apps should be considered similar and regulated centrally by the Identity platform. Advanced analytics, artificial intelligence, and machine learning benefit all identification data and occurrences. Continuous review and oversight of assignments, rules, and risk, as well as identifying orphaned, potentially toxic, overexposed, or unauthorized access, and revealing behavioral and historical events that may indicate hazardous behavior or malicious intent, are all strengths of Zero Trust. Table 6 summarizes the benefits, drawbacks, opportunities, and dangers of adopting Zero Trust as the final solution to existing security concerns.

Table 6: SWOT analysis of the Zero Trust Model

| **Strengths** | **Weaknesses** |
|---|---|
| • Less vulnerability<br>• Strong user identity policies<br>• Smart data segmentation<br>• Enhanced data protection<br>• Great security instrumentation | • Increased setup time<br>• Increased management of varied users<br>• Additional devices to deal with<br>• Additional complex application administration<br>• More careful data security |
| **Opportunities** | **Threats** |
| • Principle of least privilege (PoLP)<br>• Multi-factor authentication (MFA)<br>• Micro-segmentation<br>• Network Audit<br>• Assured Security | • Implementation<br>• Different environmental challenges<br>• Imported risks from third-party software<br>• Evolving technologies that need constant monitoring |

## AUTHOR BIOGRAPHY

**Tadiwa Elisha Nyamasvisva**, **PhD** is a member at the Faculty of Engineering and Science Technology in IUKL. His research interests are in Computer Algorithm Development, Data Analysis, Networking and Network Security, and IT in Education. Email: tadiwa.elisha@iukl.edu.my

**Atiff Abdalla Mahmoud Arabi** is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. He obtained his BIT and Masters in IT in Networking from IUKL. His research interests include Zero Trust, Biometrics Authentication, and Prevention of Network-Based Academic Dishonesty. Email: atiff2009@gmail.com

## REFERENCES

Abu-Asba, A., Azman, H., Mustaffa, R., & Ali, F. (n.d.). TEACHING STYLES OF YEMENI SCIENCE TEACHERS. *RESEARCH JOURNAL (IUKLRJ)*, 53.

Ahmed, I., Nahar, T., Urmi, S. S., & Taher, K. A. (2020). Protection of sensitive data in zero trust model. *Proceedings of the International Conference on Computing Advancements*, 1–5.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Andrade, R. O., Ortiz-Garces, I., & Cazares, M. (2020). Cybersecurity attacks on smart home during Covid-19 pandemic. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, (October 2020), 398–404. https://doi.org/10.1109/WorldS450073.2020.9210363

Atiff, A., David, A., & Elisha, T. (2021). *A Zero-Trust Model-Based Framework For Managing Of Academic Dishonesty In Institutes Of Higher Learning*. *12*(6), 5381–5389.

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., … Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248–10263.

Christ, B. (2021). Maturing operational security with an automation-first approach to IAM. *Cyber Security: A Peer-Reviewed Journal*, *5*(2), 126–134.

D'Silva, D., & Ambawade, D. D. (2021). Building A Zero Trust Architecture Using Kubernetes. *2021 6th International Conference for Convergence in Technology (I2CT)*, 1–8. https://doi.org/10.1109/I2CT51068.2021.9418203

DelBene, K., Medin, M., & Murray, R. (2019). The Road to Zero Trust (Security). *DIB Zero Trust White Paper*, *9*.

Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, J. R. (2020). Prevalence of Premeditated Academic Dishonesty at University Level. A Case Study. *JOURNAL OF CRITICAL REVIEWS*, *7*(15), 4494–4501. https://doi.org/10.31838/jcr.07.15.598

Gómez, J., Alonso-Zárate, J., Verikoukis, C., Pérez-Neira, A. I., & Alonso, L. (2007). Cooperation on demand protocols for wireless networks. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*. https://doi.org/10.1109/PIMRC.2007.4394100

Greenwood, D. (2021). Applying the principles of zero-trust architecture to protect sensitive and critical data. *Network Security*, *2021*(6), 7–9.

Hasan, M. M., Ibrahim, F., Mustapha, S. M., Islam, M. M., & Al Younus, M. A. (2018). The use of YouTube videos in learning English language skills at tertiary level in Bangladesh. *IUKL Res. J*, *6*, 27–36.

Li, D., Zhang, E., Lei, M., & Song, C. (2022). Zero trust in edge computing environment: a blockchain

based practical scheme. *Mathematical Biosciences and Engineering*, *19*(4), 4196–4216.

Mehraj, S., & Banday, M. T. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6. https://doi.org/10.1109/ICCCI48352.2020.9104214

Mujib, M., & Sari, R. F. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 27–32. https://doi.org/10.1109/ICITEE49829.2020.9271749

Nyamasvisva, T. E., Atiff Abdalla Mahmoud Arabi, Buhari, A., & Wong, F. (2020). *Premeditated Academic Dishonesty : An IoT Based Preventive Solution*. (January 2021).

Redondi, A., Chirico, M., Borsani, L., Cesana, M., & Tagliasacchi, M. (2013). An integrated system based on wireless sensor networks for patient monitoring, localization and tracking. *Ad Hoc Networks*, *11*(1), 39–53.

Rodigari, S., O'Shea, D., McCarthy, P., McCarry, M., & McSweeney, S. (2021). Performance Analysis of Zero-Trust multi-cloud. *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, 730–732. https://doi.org/10.1109/CLOUD53861.2021.00097

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (2nd Draft)*. National Institute of Standards and Technology.

Sheikh, N., Pawar, M., & Lawrence, V. (2021). *Zero trust using Network Micro Segmentation*. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

Sibghatullah H M, S., Elisha Tadiwa, N., Atiff Abdalla Mahmoud, A., Abudhahir, B., & Fares Anwar Salem, H. (2021). An Ad Hoc Movement Monitoring Algorithm for Indoor Tracking During Examinations. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(3), 3840–3846. https://doi.org/10.17762/turcomat.v12i3.1672

Simpson, W. R., & Foltz, K. E. (2021). Maintaining zero trust with federation. *International Journal of Emerging Technology and Advanced Engineering*, *11*(5), 17–32. https://doi.org/10.46338/IJETAE0521_03

Sreeja, B., Saleem, M. B., & Sravya, V. (2020). Issues With Perimeter Based Network Security and a Better Model To Resolve Them. *European Journal of Molecular & Clinical Medicine*, *07*(09), 2020. Retrieved from https://ejmcm.com/article_6830.html

Stafford, V. A. (2020). Zero trust architecture. *NIST Special Publication*, *800*, 207.

Uctu, G., Alkan, M., Dogru, I. A., & Dorterler, M. (2019). Perimeter Network Security Solutions: A Survey. *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings*, (May 2020). https://doi.org/10.1109/ISMSIT.2019.8932821

Uttecht, K. D. (2020). *Zero Trust (ZT) concepts for federal government architectures*. MASSACHUSETTS INST OF TECH LEXINGTON.

Van Der Pol, R., Gijsen, B., Zuraniewski, P., Romão, D. F. C., & Kaat, M. (2016). Assessment of SDN technology for an easy-to-use VPN service. *Future Generation Computer Systems*, *56*, 295–302. https://doi.org/10.1016/j.future.2015.09.010

Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access Control Policy Enforcement for Zero-Trust-Networking. *2018 29th Irish Signals and Systems Conference (ISSC)*, 1–6. https://doi.org/10.1109/ISSC.2018.8585365

Wylde, A. (2021). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478244

Xiaojian, Z., Liandong, C., Jie, F., Xiangqun, W., & Qi, W. (2021). Power IoT security protection architecture based on zero trust framework. *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 166–170. IEEE.