International Journal of Infrastructure Research and Management
Vol. 10 (1), June 2022, pp. 79 - 90

ZERO TRUST SECURITY IMPLEMENTATION CONSIDERATIONS IN DECENTRALISED NETWORK RESOURCES FOR INSTITUTIONS OF HIGHER LEARNING

Atiff Abdalla Mahmoud Arabi, Tadiwa Elisha Nyamasvisva and Sangeetha Valloo
Infrastructure University Kuala Lumpur, Malaysia

ABSTRACT

Unlike conventional perimeter-based security, Zero Trust allows Institutions of Higher Learning (IHL) and related businesses to operate while also modifying security architecture to suit new user demographics, customer interaction models, cloud usage, and IoT devices. The COVID-19 epidemic has prompted widespread transformation, necessitating a quick shift to Zero Trust. Starting with identity and device security, IHLs and related businesses may reduce risk quickly by concentrating on identity management and device security. These two key elements of the Zero Trust ecosystem provide assurance and the institutes will immediately see security advantages from its Zero Trust programme. Implementing Zero Trust is a slow process, as large-scale projects are unlikely to succeed. Working with current security capabilities and progressively moving to a Zero Trust paradigm while implementing important, strategic changes over a set period of time is the core concept of Zero trust Implementation. This paper recommends practices for implementing the five core pillars of Zero Trust in IHLs and related businesses. The pillars discussed are people, workloads, devices, networks, and data.

Keywords:
Network segmentation (MFA), Multifactor authentication, workloads, software-defined networking (SDN), Zero Trust, Parameterised Networks

INTRODUCTION

Zero Trust is quickly becoming the preferred security strategy for both businesses and governments (Deshpande, 2021; Egerton et al., 2021; Mohammed, 2012). As an implementation domain, institutions of higher learning (IHL) are not exempt. However, security professionals in IHL and other application areas are often unsure where to start with Zero Trust implementation or are intimidated by the fundamental changes in strategy and design that Zero Trust necessitates (Jewell et al., 2022; von Faber, n.d.). However, implementing Zero Trust does not need removing all of your existing security measures and starting over, and with the correct methodology, you can start reaping the advantages right now. This study is for security executives who want to learn about the practical components of a successful Zero Trust implementation path (Atiff et al., 2021; Buck et al., 2021; D'Silva & Ambawade, 2021; Xiaojian et al., 2021).

PREREQUISITES FOR IMPLEMENTING ZERO TRUST IN INSTITUTIONS OF HIGHER LEARNING

Zero Trust is a conceptual and architectural framework for transitioning security from a network-oriented, perimeter-based security paradigm to one based on continuous verification of trust (Lowdermilk & Sethumadhavan, 2021). It is based on the original Zero Trust idea. While this may appear to be a straightforward task, it necessitates a mental shift as well as significant adjustments in the implementation and usage of security solutions. It is vital to create a thorough roadmap that specifies the primary workstreams and projects required to accomplish your Zero Trust approach.

Administrators can see the exact delivery schedule, how much money they'll need to invest, and what particular business and security benefits they will get from their investment in Zero Trust. Institutions should review the plan before formalisation:

i. Set their overall Zero Trust strategy.
ii. Define the seven core pillars, or components, of Zero Trust in the context of the institute.
iii. Detail the core institutional capabilities necessary to deliver all the requirements
iv. Recruit both Institute and IT stakeholders in the development of the roadmap
v. Identify interdependencies with other security, IT, and Institute projects

The data security component requires that the institute can inventory, classify, archive, or delete data according to policy (Garbis & Chapman, 2021b; Horne & Nair, 2021). Today, no single vendor or provider can deliver all the capabilities and components of zero trust, it will be necessary to partner with multiple providers. Building a practical and pragmatic roadmap will allow the institutes to identify and evaluate the appropriate providers and individual technologies. Recruiting both institute (business) and IT stakeholders in the development of the roadmap the Zero Trust implementation will require new investment or, at a minimum, shifting of investment, and it will also create an avalanche of technical and organizational change. Identifying the key players that are critical for the institute's Zero Trust strategy requires that the institution need to include at a minimum (Garbis & Chapman, 2021a; Lowdermilk & Sethumadhavan, 2021):

i. The institute's board members (who are often the ultimate decision-makers) and business and IT executives (who will grant you the budget).
ii. The institute's enterprise architects and application owners (who will ensure Zero Trust supports the broader IT strategy and other projects).
iii. The institute's IT operations team (who will manage the infrastructure that you are building). They must understand the concerns of each stakeholder and address them.

The institutions need to clarify their vision, listen to the feedback, and communicate in a manner that each stakeholder can comprehend. The institutions need to identify interdependencies with other security, IT, and business projects. A Zero Trust effort needs to include existing security, IT, and business projects (Greenwood, 2021; Wylde, 2021). Projects, including cloud migrations to engaging new business partners, can be the catalysts for Zero Trust transformation. As other stakeholders and participants are recruited, integrate the associated roadmaps into the Zero Trust effort. Institutions need to ensure that they properly map and clearly communicate project dependencies (DUO - CISCO, 2019; Haber, 2020; Horne & Nair, 2021). Care must be taken to consider existing requirements in the plan for example, micro segmentation that is too granular could disrupt existing network functions and hamper the overall schedule of IT operations (Sheikh et al., 2021).

Identifying the Starting Point for Institutions of Higher Learning Zero Trust Implementation

Understanding the institutes current maturity level and where the institute want to be in each period will help focus projects and initiatives. For instance, if an institute has a mature identity and access management capability and have already implemented many of the necessary technologies from multifactor authentication to privileged identity management, they may wish to start with an area such as cloud workload security that is less mature. To begin creating an institute detailed roadmap the following needs to be considered (DUO - CISCO, 2019; Lowdermilk & Sethumadhavan, 2021; Luchenko et al., 2021; Simpson & Foltz, 2021; Teerakanok et al., 2021b).

i. assessing the maturity of the institute current Zero Trust state
ii. understanding current business initiatives and security projects for the institute
iii. documenting where the institute can reuse existing capabilities
iv. setting goals for the institute’s future maturity state and period to achieve it

Establish your current baseline by assessing your Institution of Higher Learning current Zero Trust maturity and establish a baseline of capabilities. Identify current business initiatives and existing

security capabilities. Before starting a Zero Trust initiative, learn what other business initiatives are implementing. Security leaders should take advantage of these changes that the business has already sanctioned to deliver Zero Trust more effectively in their organization. Institutes of Higher Learning must set their desired maturity state and time frames to achieve them.

ROADMAP CONSIDERATION FOR ZERO TRUST IMPLEMENTATION IN INSTITUTES OF HIGHER LEARNING

To compliment the prerequisites for implementing zero trust in institutions of higher learning and the starting point recommendations put forward in the earlier sections, this paper outlines the roadmap considerations for implementing zero trust. In doing so the paper fucuses on people, workloads, devices, networks, and data as the main pillars to be considered by the Institutions of Higher Learning before, during, and after adopting zero trust.

Zero Trust Roadmap Considerations for People

Institutes of Higher Learning, anywhere around the world, require platforms that are secure but also intuitive enough to adopt without hurting students experience or staff/faculty experience (Abu-Asba et al., n.d.; Hasan et al., 2018). With students, employees, business partners, and network access equipment all using unique identities with differing access privileges, identity and access management requirements have grown increasingly complex (Ahmed et al., 2020; DelBene et al., 2019). Zero trust for people, as a component of a framework that focuses heavily on identity and access management, is often one of the least mature areas, and one of the top three vectors for external attacks. And being the least mature, it is often the easiest to quickly improve with some essential capabilities and supporting technologies. As the institutes of higher learning develop their roadmap for people as a pillar, the following should be considered. See table 1.

Table 1: IHL Zero Trust Considerations and Justifications for People

No	Consideration	Justification
1	Investment in identity and access management technologies that solve the most critical problems (DelBene et al., 2019)	– To justify the monetary costs and potential disruption caused by adopting Zero Trust IAM (Identity and Access Management), security professionals must show how these modern technologies solve the organization's most pressing people and access problems. – When developing IAM improvements as an expansion of an institute's larger digital evolution, the chances of project approval, funding, and completion skyrocket. – When implementing multifactor authentication (MFA) and single sign-on (SSO), the implementation helps fix other issues related to compliance, security, and productivity.
2	Application of least privilege (DelBene et al., 2019; Haber, 2020)	– Do not provide more access to data and apps than users need. This is one of the most important principles of solid zero trust identity and access management practices. – Institutes of higher learning need an annual proof/access review process whereby managers and applications and data owners review user entitlements and grant or revoke them in an identity management and governance platform.

		– Institutes of higher learning must ensure that privileged users do not have access to admin functions on systems they do not need to do their job. – As users move from job to job and project to project, institutes must be sure to retire their access to assets. – Overprivileged users, employees, contingent workers, business partners, and customers and dated access credentials lead to breaches.
3	Retire the password. (Mehraj & Banday, 2020)	– While deep-rooted in applications, passwords are snoopable, crackable, and stuffable, representing a significant weakness. – Ensure, at a minimum, that MFA protects critical applications and data assets. Using passwordless authentication methods such as biometrics, tokens, or keys, reduces the surface of man-in-the-middle attacks. – Vendors such as Google, Ivanti, Microsoft, Okta, Secret Double Octopus, Yubico, and others deliver solutions to help kill the password

Zero Trust Roadmap Considerations for Workloads

Upon initiating IHL's Identification and authentication management projects and initiatives, the IHL need to determine the next Zero Trust pillar on which to focus. The maturity model completed in phase one will help IHLs choose their next Zero Trust initiative. For many institutes of higher learning, devices or workloads will be the next initiative. "The rapid adoption of cloud and the new models of computing that support rapid application development have made workload security an urgent area to mature."(Ahmed et al., 2020). Table 2 below outlines the consideration for workloads for IHLs.

Table 2: IHL Zero Trust Considerations and Justifications for Workloads

No	Consideration	Justification
1	Robust cloud governance process and structure (Ali et al., 2021; DelBene et al., 2019)	– To ensure that governance is an ongoing benefit to security, build a repeatable process not a one-time checkbox compliance exercise. – To ensure proper coverage and scope, as your organization may have many different areas and infrastructure components that it wishes to cover, including on-premises, private, and public clouds, and – To ensure executive support. Cloud governance should also cover cost optimization, budgets, regulatory compliance, and threat detection
2	Inventory and monitor workload configurations (DelBene et al., 2019)	– Because of the ease of creation, cloud workloads proliferate very quickly, often without any oversight or formal governance of cloud platform credentials, configuration settings, and even instance creation. – Manual processes or IaaS-specific tools will not cut it institutes of higher learning need a true cross-cloud workload security solution.

		– Vendors like CloudPassage, Qualys, and Trend Micro can help
3	Cloud-native security and management solutions (DelBene et al., 2019; Mehraj & Banday, 2020)	– Cloud washing and dumb lift and-shift of data and workloads to the cloud without a proper governance structure and oversight lead to data sprawl, inadequate data protection, prohibitive costs, and audit findings. – The configurations and protection appropriate for an on-premises workload are rarely appropriate in a public cloud. – Cloud migrations are a terrific opportunity to re platform, reconfigure, or refactor applications to use cloud-native storage, databases, containerization, and logging

Zero Trust Roadmap Considerations for Devices

To fully adopt a ZT (Zero Trust) framework, institutes of higher learning must be able to monitor, isolate, secure, control, and remove every device that is connected to the network at any given moment (Atiff et al., 2021; Sibghatullah et al., 2021). Most security teams still find securing laptops and mobile devices to be a challenge (Teerakanok, Uehara, & Inomata, 2021). IoT devices will make it exponentially more difficult. In the past few years, numerous compromises against a wide range of connected devices have emerged (Kimani et al., 2019). These threats rely on a range of known and unknown vulnerabilities ranging from botnets to insecure software, weak or non-existent encryption, default plain-text passwords, and insecure communication protocols. Security professionals must create a flexible architecture that can adapt to the evolving threat landscape quickly and effectively. As the development an IHL roadmap gathers momentum, the following should be considered for all kinds of devices as in table 3**.**

Table 3: IHL Zero Trust Considerations and Justifications for Devices

No	Consideration	Justification
1	Apply network segmentation to manage devices. (Kimani et al., 2019; Sheikh et al., 2021)	– IoT network segmentation solutions take an existing network of IoT devices and create zones or micro perimeters to help isolate IoT devices from other IT devices or networks, including the ability to quarantine potentially infected or compromised devices from propagating malware. – Segmenting user and device traffic away from the rest of the network can significantly reduce the risk of cybersecurity incidents.
2	Harden IoT devices. (Kimani et al., 2019)	– IoT device hardening solutions enable IoT devices and data integrity through capabilities such as secure firmware, trusted execution environments obscuring, or binary modification to help minimize the risk of device/data tampering and unauthorized access and use of the IoT device and its data. – Device hardening can support secure communications, signed software delivery, and secure patches and application updates.

		– Allows for device-based lockdown and application sandboxing. – Vendors in this space include Cisco, Infineon, Intel, and Thales.
3	Reduce user risk created by BYOD (Bring Your Own Device) policies. (Morolong et al., 2020; Stafford, 2020)	– BYOD and the increasingly mobile workforce have eliminated the control IT used to have over endpoints that connect to enterprise networks and access data. – Must minimize issues by negating the obviously plain threats that endpoints present such as malicious software infections, ransomware events, and malware. – Must conduct health checks on endpoints before allowing them (eg backdoor and virus programs and software updates especially those related to security) to connect to the network or access systems. – Allow to shut down all the non-used and threat-riddled apps your users want to run on their BYOD devices. – Act prescriptively to gain some control by using software-defined networking (SDN) solutions that push the focus of your enterprise security out to the endpoint. – It may not be "your" endpoint, but it is your network, and you can enforce your security policies on those endpoints if you do it right.

Zero Trust Roadmap Considerations for Networks

The perimeter does not disappear, as it remains. But the perception of the network perimeter has evolved. The perimeter is now "the edge" of your network, whereby users touch or connect to the enterprise. Consider a core principle of Zero Trust by redrawing logical segmentation boundaries around network assets and increasing isolation between segmentations. Authorize and log all access at segmentation boundaries and inspect and log all activity within each network segmentation (Sheikh et al., 2021). The following should be considered as you develop your roadmap:

Table 4: IHL Zero Trust Considerations and Justifications for Networks

No	Consideration	Justification
1	Redraw the boundaries. Draw boundaries to protect resources, not networks. (Rose et al., 2020)	– Segment around an application and its associated hosts, peers, and services. – The segmentation policy defines the access that each group has with another group. – The baseline, if generated by sensors, will often include the suggested segmentation policy. – Review it for anomalies before enforcement, of which enforcement of the segmentation policy can be done at each host (via an agent) or via virtual network routing. – Host-based agents are the most common, but some users shy away from them for fear of having to deploy those agents on tens of thousands of endpoints.

		– In fully virtualized environments like VMware, use a hypervisor component to enforce the policy.
2	Push controls to the "edge" of the enterprise. (Chen et al., 2020; Guide et al., n.d.)	– There are multiple approaches to leveraging the existing north-south perimeter as an inspection zone for all human-generated traffic. – Web gateways operating in explicit-proxy and transparent modes can detect and block risky clicks and stop malware. – Use DNS-based solutions to achieve most of the border security goals while being incredibly simple to deploy.
3	Use modern enterprise firewalls to augment cloud security controls. (Mehraj & Banday, 2020)	– The next-generation firewall (NGFW) was the backbone for Zero Trust, and it is even better today. – Today, NGFW are stuffed with crypto chips to decrypt and inspect all traffic transiting a boundary, but virtualized use cases are finally becoming common, too. – Insert a layer of autoscaling virtualized firewalls or IDS/IPS behind a gateway load balancer to inspect your application traffic. – Integrate the management of container security policies and cloud firewalls into their cloud-delivered or cloud-connected security dashboards, signalling a path forward where third parties manage cloud objects on your behalf.

Zero Trust Roadmap Considerations for Data

ZT is a much more data- and identity-centric approach to security than a network-focused one or rather the historical approach. This involves building capabilities for visibility into the interaction between users, apps, and data across a multitude of devices and the ability to set and enforce one set of policies irrespective of whether the user is connected to the corporate network. This is not easy and is compounded by the challenge of understanding what is sensitive and valuable data for the organization today. Typically, basic data security controls are already established due to compliance requirements (Ahmed et al., 2020; Mehraj & Banday, 2020); Institutions of higher learning feel they have stopped the bleeding, buying themselves a bit more time yet everything is premeditated by the perpetrators (Nyamasvisva et al., 2020)(Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, 2020). However, there is need to evaluate all the Zero Trust pillars together in the context of your critical applications, data, and assets. While building your roadmap:

Table 5: IHL Zero Trust Considerations and Justifications for Data

No	Consideration	Justification
1	Define your data to understand what you must protect, where, and how. (Ahmed et al., 2020)	This includes building capabilities for data discovery and classification to help identify where data is located, and what is sensitive data. These capabilities are readily available today as a feature of other technology offerings as well as from specialized offerings. Work with the risk and privacy Institutions of higher learning to help define the policies around this.
2	Dissect your data to understand its value and lifecycle, and threats to it. (Embrey, 2020)	This data intelligence provides business and contextual insights about data to help guide policies and controls. It requires processes and technologies to help answer questions about your data, such as: • How does this data flow to produce a business outcome? • Who is using this data, how often, and for what purpose? • Why does the business have this data, how is it collected, and what is its useful lifecycle? • What are the consequences if data integrity is compromised? In addition, understand the threats to the data collected from other security tools in your environment, such as DLP and EDR, to help guide decision-making.
3	Defend your data through four core measures and enabling technologies. (Assunção, 2019; Shore et al., 2021)	These include controlling access, inspecting data usage patterns, defensible disposal of data, and obfuscation. There are many key technologies to support data security and privacy. Encryption alone encompasses a variety of separate offerings from email encryption to database encryption, to support protecting data in its various states (at rest, in transit, and in use), as well as innovations like homomorphic encryption and quantum-safe offerings

RECOMMENDATIONS

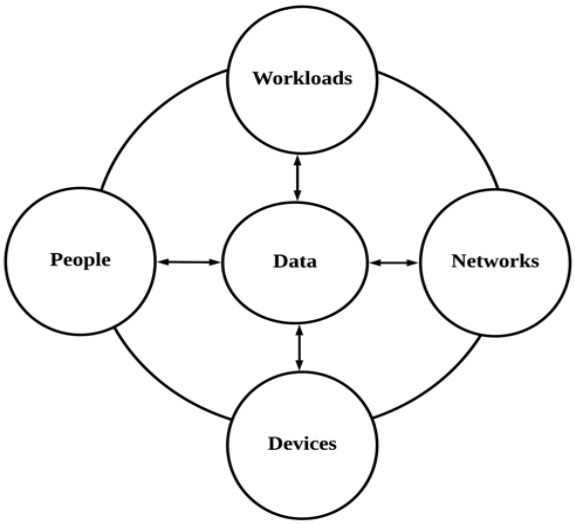

Figure 1: The Recommended Mapping of Zero Trust for Institutions of Higher Learning (IHLs)

The thesis of this paper is summarised in the diagram above which shows the relationships between the pillars of Zero trust.

Bring your ZT (Zero Trust) strategy and roadmap right to the institutions board (DelBene et al., 2019). Chief Information Security Officers (CISOs) have become common fixtures in boardrooms, communicating complex issues and engaging board members' and executives' hearts and minds on the topic of security(DUO - CISCO, 2019). This is shifting the boards from having a vague awareness that security threats are real to having an actual understanding of what these threats are and how to tackle them. They are asking tough questions that increasingly demonstrate they understand that the old way of doing security is no longer sufficient. Courageous CISOs are taking Zero Trust to the boardroom (DUO - CISCO, 2019).

To be successful the organization must be clear that ZT is what will get you customer trust. To some, the concept of Zero Trust seems at odds with engendering trust. Build engaging ZT content to meet your board's expectations. The security team must manage cybersecurity like any other risk. Translate technology needs to business benefits. Do not focus on validating more technology just to acquire more technology. The goal of security is to make business better and better to protect your customers' data. Not having more cool security tools. If done right, there should be culling of technologies that do not align with business needs and removing solutions that are not optimal for your strategy.

AUTHOR BIOGRAPHY

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*

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*

Sangeetha Valloo, is a faculty member at the Faculty of Engineering and Science Technology in IUKL. Her research interests are in Data Communication and Networking as well as Network Security. She was a former Dean at the Faculty of Creative Media and Information Technology in IUKL. Currently, she manages and coordinates all final year projects for the Department of Information Technology at the Faculty. *Email: sangeetha@iukl.edu.my*

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.

Ali, B., Gregory, M. A., & Li, S. (2021). Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security Model. *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, 192–197.

Assunção, P. (2019). A zero trust approach to network security. *Proceedings of the Digital Privacy and Security Conference 2019*.

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

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436.

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & 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.

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.

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

Deshpande, A. (2021). A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic. *New Visions in Science and Technology Vol. 1*, 26–33.

DUO - CISCO. (2019). *Zero Trust Evaluation Guide For the Workforce*. 29.

Egerton, H., Hammoudeh, M., Unal, D., & Adebisi, B. (2021). Applying Zero Trust Security Principles to Defence Mechanisms Against Data Exfiltration Attacks. *Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications*, 57–89.

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. http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=144463015&lang=es&site=ehost-live

Embrey, B. (2020). The top three factors driving zero trust adoption. *Computer Fraud & Security*, *2020*(9), 13–15.

Garbis, J., & Chapman, J. (2021a). *Zero Trust Security: An Enterprise Guide*.

https://doi.org/10.1007/978-1-4842-6702-8

Garbis, J., & Chapman, J. (2021b). *A Zero Trust Policy Model* (pp. 211–238). https://doi.org/10.1007/978-1-4842-6702-8_17

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

Guide, A. E., Garbis, J., & Chapman, J. W. (n.d.). *Zero Trust Security*.

Haber, M. (2020). *Zero Trust* (pp. 295–304). https://doi.org/10.1007/978-1-4842-5914-6_22

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.

Horne, D., & Nair, S. (2021). *Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype*. *April*.

Jewell, D. O., Jewell, S. F., & Kaufman, B. E. (2022). Designing and implementing high-performance work systems: Insights from consulting practice for academic researchers. *Human Resource Management Review*, *32*(1), 100749.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49.

Lowdermilk, J., & Sethumadhavan, S. (2021). *Towards Zero Trust: An Experience Report*. https://doi.org/10.1109/SecDev51306.2021.00027

Luchenko, Y., Semenova, V., & Kravets, N. (2021). Zero Trust Technology Application for Ai Medical Research. *Грааль Науки*, *10*, 264–267. https://doi.org/10.36074/grail-of-science.19.11.2021.049

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

Mohammed, I. A. (2012). Analysis of Identity and Access Management alternatives for a multinational information-sharing environment. *INTERNATIONAL JOURNAL OF ADVANCED AND INNOVATIVE RESEARCH*, *1*(8), 1–7.

Morolong, M. P., Shava, F. B., & Gamundani, A. M. (2020). Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho. *International Conference on Cyber Warfare and Security*, 346–XVI.

Nyamasvisva, E. T., Arabi, A. A. M., Buhari, A., Wong, F., & Valloo, S. (2020). Premeditated Academic Dishonesty: An IoT Based Preventive Solution. *Solid State Technology*, *63*(6), 19369–19379.

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

Shore, M., Zeadally, S., & Keshariya, A. (2021). Zero Trust: The What, How, Why, and When. *Computer*, *54*(11), 26–35.

Sibghatullah, H. M. S., Nyamasvisva, T. E., Arabi, A. A. M., & Buhari, A. (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

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

Teerakanok, S., Uehara, T., & Inomata, A. (2021a). Migrating to zero trust architecture: reviews and challenges. *Security and Communication Networks*, *2021*.

Teerakanok, S., Uehara, T., & Inomata, A. (2021b). Migrating to Zero Trust Architecture: Reviews and Challenges. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9947347

Von Faber, E. (n.d.). *On the future of IT security management in the face of changes in technology and service delivery*.

Wylde, A. (2021). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*. 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.