Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.14, No.1, 2024

Integrating Zero Trust and Human Elements for Enhanced Cloud Security

Mohamed Rajraji[1*] Steve Simske[2] Anass Rabii[3]

1. Walter Scott, Jr. College of Engineering, Colorado State University, 6029 Campus Delivery, Fort Collins, CO, USA
2. Walter Scott, Jr. College of Engineering, Colorado State University, 6029 Campus Delivery, Fort Collins, CO, USA
3. School of Engineering, Ecole Mohammadia d'Ingénieurs, BP: 765, Avenue Ibn Sina, Agdal, Rabat, Morocco

* E-mail of the corresponding author: Mohamed.rajraji@colostate.edu

Abstract

This study investigates increasingly complex cyber threats that are challenging cloud environments as traditional protocols reach limitations. The rapid increase in cloud computing has exposed organizations to advanced cyber threats. This exposure has left them vulnerable to attacks that are large-scaled and complex. Conventional security models, which focus primarily on defending the perimeter, are not sufficient to meet the challenges posed by these changing threats. This situation requires a significant shift in cybersecurity strategies to ensure effective protection of cloud environments and to keep sensitive data safe. In response to these threats, we present an innovative methodology integrating Zero Trust principles with understanding of human factors for a versatile defense system closely aligned to nuances of conduct and culture.

Our approach offers comprehensive solutions designed to address the dynamic and sophisticated nature of cloud protection requirements. As cyber risks continue to intensify, our methodology stands out by providing adaptive and human-centric security solutions. It represents a step forward in addressing the evolving challenges in cloud computing security, ensuring that defenses remain robust and responsive to both technological and human dynamics.

Keywords: Human Factors, Zero Trust, Cloud Security, Cyber Threats, Adaptive Security Solutions, Vulnerability Exploitation, User-Centered Design, Behavioral Sciences, Cybersecurity Enhancements

DOI: 10.7176/ISDE/14-1-05
Publication date: April 30th 2024

1. Introduction

In the rapidly evolving digital landscape, cloud computing faces escalating cyber threats. Current control frameworks, as noted by Koskenkorva (Koskenkorva, 2021), are increasingly challenged to effectively tackle these threats, particularly in light of the surge in remote access and cloud connectivity. This paper seeks to address these emerging challenges by exploring advanced security strategies that are adaptable and resilient.

As the sophistication of cyber threats grows, revealing major weaknesses in traditional security methods, there is a clear need for reimagining security approaches (Loukaka & S. M. Rahman, 2017). Zero Trust, as highlighted by Kindervag (2010) and Kudrati & Pillai (2022), offers a promising alternative with its emphasis on identity verification, encryption, and limited access rights. However, this shift also brings to light the often-overlooked human element – the interplay between technology, people, and organizational culture.

This research advocates a significant shift in cybersecurity strategy, integrating the Zero Trust architecture with a human-centered design. This approach aims to balance strict security requirements with user-friendliness and efficiency. It also considers the influence of human factors such as motivational triggers and cognitive capacities, essential for effective cybersecurity in contemporary cloud environments.

The paper extends beyond the conceptual exploration of Zero Trust's impact on organizational behavior by Astakhova (2022), integrating insights from Pollini et al. (2022) on human factors. By doing so, it proposes an integrated framework that not only addresses technical vulnerabilities but also enhances the security posture of cloud environments by considering the human aspects of cybersecurity.

2. Cloud Security Landscape and Key Challenges

The landscape of cloud computing is increasingly concerned with a range of security challenges that extend beyond technical factors to encompass human dimensions. This complexity is highlighted in the work of Liginlal et al. (2009) and Tabrizchi & Kuchaki Rafsanjani (2020), emphasizing the need for security approaches that address user behaviors, cognitive biases, and cultural factors. These approaches aim to create a security paradigm that synergizes technology with human actions, recognizing the interconnected nature of these elements.

The pivotal role of identity access management in cloud security, as observed by Alenezi (2021) and Mthunzi et al. (2020), further stresses integrating governance spanning people and systems. Moreover, declining cloud trust despite surging adoption levels highlights the fact that substitution needs are transcending purely technical fixes - instead necessitating holistic strategies fusing tools and culture for trust restoration as Ramachandra et al. (2017) and Faizi & Rahman (2019) discuss.

Recent research has also explored innovative approaches to enhance cloud security and optimize data storage. For example, Thottipalayam Andavan et al. (2024) proposed a secure cloud data deduplication approach that combines proxy re-encryption, refraction learning-based chimp optimization for optimal key generation, and an optimal verified fuzzy keyword search to eliminate duplicate files. While their primary focus is on data deduplication and storage optimization, their work highlights the importance of addressing security concerns alongside performance improvements in cloud environments.

In response, this paper proposes an adaptation of the Zero Trust architecture with a focus on human-centered design. This approach, which emphasizes usability and adoption, is grounded in exposure models and risk assessments. It seeks to strike a balance between security and efficiency, integrating psychological insights and considerations for user acceptance. This integrated methodology aligns with Astakhova's (2022) exploration of Zero Trust's impact on organizational behavior and incorporates insights on human factors in security contexts from Pollini et al. (2022). Additionally, it builds upon Nobles & Mcandrew's (2023) approach, aiming to strengthen cloud security postures through a socio-technical synthesis.

3. Traditional Cybersecurity Models and Their Cloud Limitations

Evaluating the inadequacies of traditional, perimeter-based security models in the context of cloud computing highlights a stark contrast with the Zero Trust framework. As explained by DeCusatis et al. (2016), conventional cybersecurity has historically relied on robust network perimeters, operating under an inherent trust in resources within these boundaries. However, the inherent nature of cloud computing challenges this concept of fixed security perimeters. The shift towards externally managed, variable resources undermines the notion of static digital boundaries, rendering traditional models, premised on set divisions, ineffectual against contemporary threats (Abdulazeez, 2017).

In stark contrast, the Zero Trust model introduces a security architecture tailored for the cloud era. This model diverges from previous trust-based approaches by mandating continuous verification for all access attempts, irrespective of their origin within or outside the organizational network. This notion of comprehensive authentication and authorization, before permitting any user or workload connection, aligns seamlessly with the fluid boundaries characteristic of cloud computing. The emphasis on identity within the Zero Trust model aptly addresses the gaps left by the transient nature of cloud infrastructure, which static perimeter defenses struggle to manage effectively (Chimakurthi, 2020).

The transition from an implicit trust in resources within traditional digital perimeters to the adoption of Zero Trust frameworks signifies a fundamental shift in cybersecurity philosophy, warranting further exploration. Emphasizing universal identity validation as the cornerstone for securing dynamic cloud resources underscores the necessity to re-examine the foundational concepts shaping modern access environment protection.

The ensuing section delves deeper into the core tenets of the Zero Trust framework and its adaptations for the cloud era, reshaping traditional security boundaries.

4. Zero Trust Security Framework

Responding to the deficiencies of traditional security models, the Zero Trust framework has emerged as a pivotal approach in addressing the intricacies of cloud security challenges. This shift in cybersecurity, moving away from a reliance on assumed trust within predefined business perimeters to a focus on ongoing and explicit verification, is well-articulated by Campbell, (2020) and Rose et al. (2020). This transition is visually encapsulated in Figure 1, which illustrates the Core Principles of the Zero Trust Security Model, offering a graphical depiction of these foundational concepts.

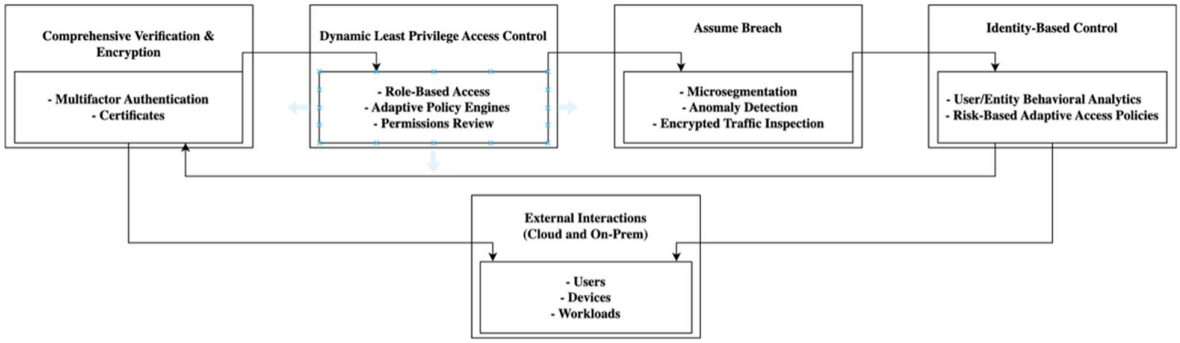

Figure 1. Core Principles of the Zero Trust Security Model. Adapted from Kudrati & Pillai (2022)

The Zero Trust approach depends on key principles designed specifically to handle today's digital environments challenges:

1. Comprehensive Verification and Encryption: Zero Trust revolves around multifactor authentication (MFA), a process where both users and devices must prove their legitimacy. It also includes strong encryption to protect data and communications, as noted by Hosney et al. (2022). Additional security checks, such as device verification, are employed to fortify defenses.
2. Dynamic Least Privilege Access: In Zero Trust, access rights are carefully managed and adjusted based on the specific role of a user and the context of their access request. This method, highlighted by Chimakurthi (2020) and Collier & Sarkis (2021), involves constantly reassessing permissions to minimize unnecessary access and reduce internal threats. This is also known as the *Principle of Least Privilege*.
3. Assume Breach: Operating under the assumption that breaches can occur, Zero Trust adopts an approach that makes data-driven decisions on access. This includes segmenting (or *partitioning*) the network into smaller, secure parts and using encryption to limit potential threats, a strategy emphasized by Collier & Sarkis (2021) and Wylde (2021).
4. Identity-based Control: Central to Zero Trust is the principle that security depends on confirming the identities of users and the status of their devices, rather than their location within a network. This focus on identity, as detailed by Collier & Sarkis (2021) and Kudrati & Pillai (2022), allows for more precise control based on real-time risk assessments.

These principles of the Zero Trust model articulate a significant shift from traditional security paradigms, focusing on rigorous verification and continuous adaptation to emerging security challenges. This is particularly relevant for cloud environments, where older security models fall short, as underscored by Madsen (2024) and Sheikh et al. (2021). By embedding these principles, Zero Trust offers a proactive, resilient framework poised to meet the diverse and evolving threats of the digital age.

5. The Role of Human Factors in Advancing Cybersecurity

Integrating human factors into cybersecurity represents a pivotal research arena attracting extensive focus. A substantial body of findings, including insights by (Verizon, 2022) implicates human errors rather than technical gaps alone behind a dominant proportion of breaches, exceeding 82% per some estimates. This exposes an underappreciated vulnerability in prevailing strategies that concentrate disproportionately on infrastructure upgrades rather than addressing the pivotal influence of behaviors, psychology and social interactions.

Incorporating perspectives highlighted by scholars like Nobles (2018), the immense value of embedding cross-disciplinary expertise spanning psychology, cognitive sciences and human factors becomes apparent. Nobles advocates comprehensive integration of human-centric considerations to enhance cybersecurity outcomes. This encompasses analyzing and appraising end-user actions in system environments - given technological controls alone remain insufficient for ensuring information security.

Numerous case studies consistently demonstrate exploitations arising from mismatched alignments between user activities and security designs - whether from social engineering manipulating trust or convoluted tools confusing operators (Chowdhury et al., 2020; Moallem, 2018). Nobles further spotlights behavioral specialists providing invaluable inputs to harden cyber operations against risks introduced by cognitive biases or emotional stressors.

Essentially, strategically assimilating insights across technology and culture promises more holistic cloud security solutions that sustain productivity alongside protection for contemporary boundary-less environments.

6. Combining Human Factors and Zero Trust for Enhanced Cloud Security

In the realm of cybersecurity, the fusion of Zero Trust principles with insights into human behavior stands as a crucial strategic foundation. This integration brings about significant improvements, including a 65% reduction in misconfigurations, typically due to human errors, and a 99% decrease in the chances of exploitation, as detailed by Basta et al. (2022). Hence, the adoption of user-centered design principles in cloud security is essential, not just for enhancing user adoption but also for maintaining productivity. It bridges technical security advancements with human interaction's subtleties, as demonstrated by Figure 2 in our document, which showcases a model of Holistic Cloud Security Centered on People, blending human factors with Zero Trust principles effectively.

The role of behavioral sciences in this strategy is pivotal, as evidenced by Zimmermann & Renaud, (2019). Employing clear language in security alerts and promoting safe practices are crucial to encourage secure user behaviors. Additionally, training programs tailored to diverse learning styles and knowledge levels are vital. Russo et al. (2021) highlight how such programs can significantly increase user engagement and comprehension of security protocols.

Behavior monitoring forms an integral component of the Zero Trust framework. It entails the analysis of user behaviors to identify patterns that might signal potential security threats, crucial for uncovering anomalies that could lead to breaches or highlight areas needing further training. Russo et al. (2021) also stress the benefits of gamification and simulations in training, making complex security concepts more accessible and engaging. This approach not only aids in achieving better compliance with security protocols but also strengthens the overall security stance. By integrating gamification, we enhance this methodology, turning routine security tasks into intriguing challenges, thus fostering a more intuitive understanding of complex protocols and encouraging users to willingly adopt secure practices, including multifactor authentication (MFA).

Central to this strategy is motivational incentive design. Understanding the motivations behind user behavior enables organizations to devise rewards systems that promote adherence to security policies, thereby aligning security measures with the organization's human elements.

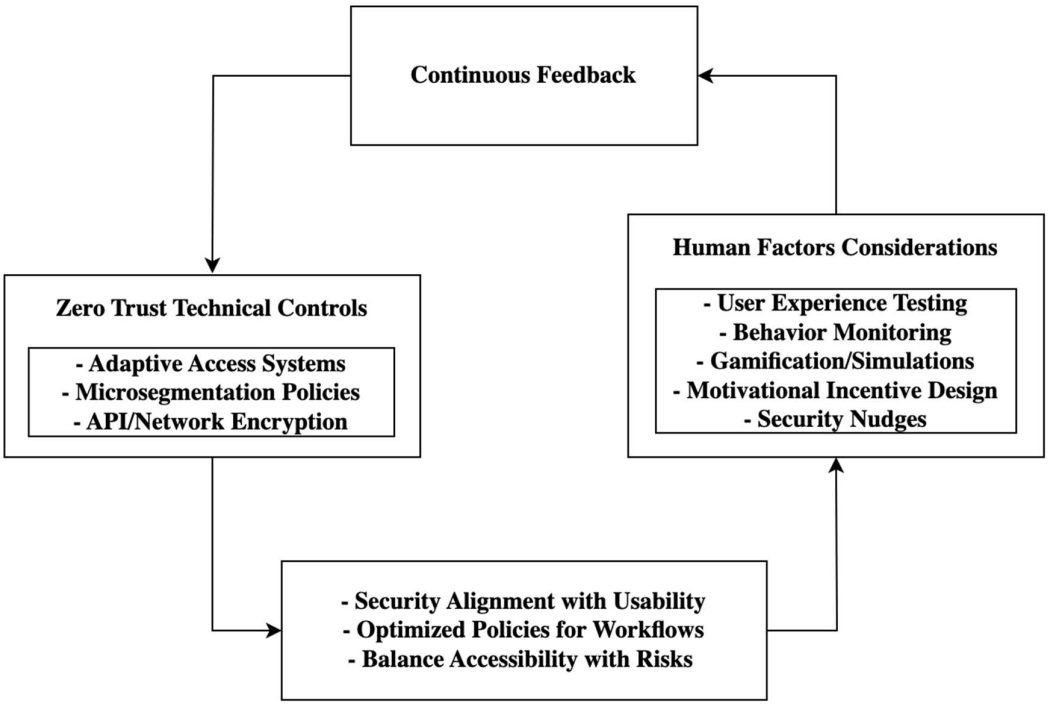

Figure 2. Holistic Cloud Security Centered on People

The strategic implementation of security nudges within the system serves as a user-friendly method to steer user behavior towards safer security decisions. These nudges, intentionally designed to be discreet and non-intrusive, motivate users towards more secure actions without burdening them with technical complexity.

This holistic approach is further enhanced by continuous feedback loops, allowing the system to adapt and evolve based on user behaviors, thereby proactively adjusting the security landscape to anticipate and mitigate emerging risks.

In conclusion, the amalgamation of technological advancements with a nuanced understanding of cultural and behavioral aspects furnishes more comprehensive cloud security solutions. These solutions adeptly balance productivity and protection in today's limitless cloud computing environments. Illustrated in Figure 2, this segment of the paper underscores the critical need to consider both technical and human factors in formulating effective security strategies for cloud environments.

7. Case Studies of Zero Trust in Action

In the realm Real-world examples are instrumental in showcasing the effective integration of human aspects with Zero Trust principles in enhancing cloud security. These case studies offer crucial insights into how this integrated approach can be successfully implemented in diverse settings.

Google's BeyondCorp Initiative: Google's transition from traditional perimeter-based security to a Zero Trust model, as detailed by Das (2023), stands as a landmark example of this framework in action. This strategy, eliminating the need for VPNs for remote access (Assunção, 2019; Garbis & Chapman, 2021) reflects our paper's focus on adaptable, context-sensitive security. BeyondCorp's method expertly merges technical strategies with user-centric policies, demonstrating how Zero Trust can be applied in a way that is responsive to human behavior and organizational dynamics.

PagerDuty's Zero Trust Model: PagerDuty's implementation of Zero Trust, especially in server-to-server interactions within cloud environments (Garbis & Chapman, 2021), underscores the framework's adaptability. Their use of a central policy engine and distributed enforcement points, along with automated configuration management, illustrates how Zero Trust can be tailored to specific infrastructure needs. This case study aligns with

the paper's viewpoint on personalizing Zero Trust to address both human and system-based vulnerabilities.

Securing a Logistics Platform: The application of Zero Trust in a logistics platform, incorporating commercial encryption and software-defined boundaries (Wang et al., 2022), exemplifies the framework's flexibility. The addition of blockchain for enhanced trustworthiness underlines innovative methods addressing both human and technical factors. This example resonates with the paper's emphasis on blending human factors with Zero Trust to manage risks effectively.

In summary, these case studies reinforce the paper's central theme: the integration of human factors with Zero Trust principles is vital for devising flexible and robust cloud security strategies. They exemplify how a people-centric approach, combined with advanced technology, can create security solutions that are not only technically effective but also align with the needs and behaviors of users, thereby strengthening the overall security posture of cloud environments.

8. Discussion and Implications of Integrating Human Factors in Cloud Security

In the realm Integrating human factors into cloud security is not just theoretical but also pragmatically essential. Our research shows how combining Zero Trust and understanding human behavior can majorly strengthen cloud security strategies. This goes past technical fixes by addressing how technology and people come together.

Key points from our discussion:

Adaptive Security in Context-Sensitive Environments: As shown in Google's BeyondCorp project, blending human factors into access and identity management proves security should be flexible and adaptive. This meshes technical steps with policies centered on users, aligning with our paper's focus on making security systems effective but also helpful for user needs.

Customized Solutions for Complex Environments: The implementation of Zero Trust in diverse settings, like that of PagerDuty's server-to-server interactions, showcases the framework's versatility. It illustrates how technical safeguards can be tailored to specific infrastructural needs, addressing both human and system-based vulnerabilities.

Innovative Approaches in Varied Sectors: The application of Zero Trust in different sectors, such as in a logistics platform, demonstrates the adaptability of the framework. Incorporating advanced technologies like blockchain for added trust signifies the importance of innovative solutions that cater to both human and technical factors.

In conclusion, these case studies and our discussion emphasize the essential role of integrating human factors with Zero Trust principles in developing cloud security strategies. This integration not only enhances technical security measures but also ensures that they are in tune with human behaviors and organizational culture. By doing so, cloud security becomes not only more robust and flexible but also more aligned with the needs and behaviors of users, thereby strengthening the overall security posture and user engagement in cloud environments.

9. Challenges and Future Directions

As we navigate the integration of Zero Trust and human factors in cloud security, several key challenges emerge, necessitating future research directions:

Organizational Culture and Workforce Motivation: Examining the evolving patterns of employee behavior and the drivers of their motivation, especially for crucial security-enhancing approaches like MFA, is essential for understanding their influence on the adoption of Zero Trust across various organizational contexts. Such an inquiry provides valuable insights, which are instrumental in guiding the adaptation of security frameworks to align with the nuances of contemporary workplace environments (Astakhova, 2022; Buck et al., 2021).

Sector-Specific Strategies: Different sectors, particularly those like healthcare, finance, and telecommunications, face unique challenges due to distinct data sensitivities and regulatory environments. Tailoring Zero Trust strategies to these specific needs requires further investigation (Sarkar et al., 2022).

Technological Evolution and Policy Support: As technological advancements continue, particularly in areas like automation and contextual analytics, there is a growing need for decision-support systems that can efficiently manage access policies in cloud environments (Yan & Wang, 2020).

Human Factors Perspective: Addressing security awareness beyond standard training methods and understanding the emotional strain on analysts in high-pressure environments are vital challenges from a human factors perspective (Nobles, 2018). Further, exploring ways to quantify human vulnerabilities and integrating these

assessments into risk models is an emerging field crucial for a comprehensive view of security threats (Nobles, 2019).

By tackling these challenges and pursuing these research directions, we aim to deepen our understanding of Zero Trust integrated with human factors in cloud security. This comprehensive approach is key to developing more adaptable, resilient, and effective cybersecurity frameworks that can respond to the dynamic threats of the digital landscape.

Future research could explore the application of this integrated zero trust and human factors approach across different industries and organizational contexts. Additionally, investigating the long-term effectiveness of these strategies in mitigating evolving cyber threats and maintaining user engagement will provide valuable insights. Further studies to examine the potential of integrating advanced technologies, such as artificial intelligence and machine learning, to enhance the adaptability and responsiveness of these human-centric security solutions in cloud environments, are also warranted.

10. Conclusion

As we conclude our examination of integrating Zero Trust and human factors in cloud security, we recognize several crucial insights. This paper illustrates that the fusion of Zero Trust principles with an in-depth understanding of human dynamics is vital for crafting resilient cloud security solutions. Emphasizing human behavior and psychology is key for the successful implementation and effectiveness of Zero Trust across various environments.

The blend of cutting-edge technology with insights into human subtleties is essential for advancing cybersecurity practices. Our research highlights the necessity of continual exploration into the interplay between technical and human domains. Future research should focus on:

1. Harnessing behavioral analytics to enhance identity and access management.
2. Exploring the potential of AI and ML in predicting and mitigating human errors in security systems.
3. Assessing the effectiveness of targeted training programs in fostering a security-conscious culture.

Moreover, evaluating the long-term impact of these integrated strategies on organizational resilience against cyber threats is a crucial next step. In summary, this paper advocates for a multi-faceted approach in cloud security, balancing technical advancements with a deep understanding of human behavior. This approach is key to developing more effective, adaptable, and comprehensive security strategies, ready to confront the challenges of the rapidly evolving digital landscape.

References

Abdulazeez, M. B. (2017). *Intrusion detection and prevention systems in the cloud environment*. The University of Liverpool (United Kingdom).

Alenezi, M. (2021). *Safeguarding Cloud Computing Infrastructure: A Security Analysis*. 9.

Assunção, P. (2019). *A Zero Trust Approach to Network Security*. 8.

Astakhova, L. V. (2022). Zero Trust Model as a Factor of Influence on the Information Behavior of Organization Employees. *Scientific and Technical Information Processing*, *49*(1), 60–64. https://doi.org/10.3103/S0147688222010105

Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 1–7. https://doi.org/10.1109/NOMS54207.2022.9789888

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. https://doi.org/10.1016/j.cose.2021.102436

Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. *Computer*, *53*(10), 110–113. https://doi.org/10.1109/MC.2020.3011081

Chimakurthi, V. N. S. S. (2020). The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment. *ABC Journal of Advanced Research*, *9*(2), 89–102. https://doi.org/10.18034/abcjar.v9i2.608

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101931.

Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust.

International Journal of Production Research, *59*(11), 3430–3445. https://doi.org/10.1080/00207543.2021.1884311

Das, R. (2023). *The zero trust framework: Threat hunting & quantum mechanics*. CRC Press.

DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 5–10. https://doi.org/10.1109/SmartCloud.2016.22

Faizi, S., & Rahman, S. (2019). Secured cloud for enterprise computing. *CATA*, 356–367.

Garbis, J., & Chapman, J. W. (2021). *Zero trust security: An enterprise guide*. Springer.

Hosney, E. S., Halim, I. T. A., & Yousef, A. H. (2022). An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA). *2022 5th International Conference on Computing and Informatics (ICCI)*, 343–350. https://doi.org/10.1109/ICCI54321.2022.9756117

Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*.

Koskenkorva, H. (2021). *The role of security patch management in vulnerability management*.

Kudrati, A., & Pillai, B. A. (2022). *Zero trust journey across the digital estate*. CRC Press.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3–4), 215–228. https://doi.org/10.1016/j.cose.2008.11.003

Loukaka, A., & S. M. Rahman, S. (2017). Discovering New Cyber Protection Approaches from a Security Professional Prospective. *International Journal of Computer Networks & Communications*, *9*(4), 13–25. https://doi.org/10.5121/ijcnc.2017.9402

Madsen, T. (2024). *Zero-trust–An introduction*. CRC Press.

Moallem, A. (2018). *Human-computer interaction and cybersecurity handbook*. CRC Press.

Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, *107*, 620–644. https://doi.org/10.1016/j.future.2019.11.013

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Nobles, C. (2019). *Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity*.

Nobles, C., & Mcandrew, I. (2023). The Intersectionality of Offensive Cybersecurity and Human Factors: A Position Paper. *Scientific Bulletin*, *28*(2), 215–233. https://doi.org/10.2478/bsaft-2023-0022

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science*, *110*, 465–472. https://doi.org/10.1016/j.procs.2017.06.124

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Russo, D., Ahram, T., Karwowski, W., Di Bucchianico, G., & Taiar, R. (2021). *Advances in intelligent systems and computing*. Springer: Cham, Switzerland.

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability*, *14*(18), Article 18. https://doi.org/10.3390/su141811213

Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Thottipalayam Andavan, M., Parameswari, M., Subramanian, N., & Vairaperumal, N. (2024). A novel model for enhancing cloud security and data deduplication using fuzzy and refraction learning based chimp optimization. *International Journal of Machine Learning and Cybernetics*, *15*(3), 1025–1038.

Verizon. (2022). *2022. Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Wang, H., Ou, W., & Han, W. (2022). A Novel Logistics Scheme Based on Zero-Trust Model. In J. Lin & Q. Tang (Eds.), *Applied Cryptography in Computer and Communications* (pp. 203–215). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-17081-2_13

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

Yan, X., & Wang, H. (2020). Survey on Zero-Trust Network Security. In X. Sun, J. Wang, & E. Bertino (Eds.), *Artificial Intelligence and Security* (Vol. 1252, pp. 50–60). Springer Singapore. https://doi.org/10.1007/978-981-15-8083-3_5

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005