SUSTAINABLE MACHINE INTELLIGENCE JOURNAL

Revisiting Zero-Trust Security for Internet of Things

Mahmoud Ismail[1,*], Amal F.Abd El-Gawad[2]

[1] Decision support department, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Sharqiyah, Egypt; mmsabe@zu.edu.eg
[2] Decision support department, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Sharqiyah, Egypt; amgawad2001@yahoo.com.
* Correspondence: mmsabe@zu.edu.eg

Event	Date
Received	04-03-2023
Revised	15-05-2023
Accepted	11-06-2023
Published	24-06-2023

Abstract: The proliferation of Internet of Things (IoT) devices has revolutionized various industries, yet concurrently introduced unprecedented security challenges. Zero-Trust security emerges as a promising paradigm to mitigate the escalating risks associated with IoT ecosystems. This mini review provides a comprehensive analysis of Zero-Trust principles and their application within IoT environments. Beginning with an elucidation of the Zero-Trust framework's foundational tenets, this paper explores its relevance in the context of IoT, emphasizing the necessity for continuous authentication, strict access controls, micro-segmentation, and encryption strategies. Furthermore, it delves into the evolving threat landscape faced by IoT systems and evaluates how Zero-Trust principles effectively counteract these threats, safeguarding sensitive data, ensuring device integrity, and bolstering overall system resilience. Additionally, the review highlights notable challenges and implementation considerations in integrating Zero-Trust security within diverse IoT infrastructures.

Keywords: Zero-Trust Security, Internet of Things (IoT), Cybersecurity, Dynamic Risk Management, Governance Frameworks, Regulatory Compliance.

1. Introduction

The advent of the Internet of Things (IoT) has ushered in an era of unprecedented connectivity, enabling seamless communication between a myriad of devices. However, this interconnected landscape has also given rise to complex security challenges. Traditional security paradigms are often inadequate to protect the vast and diverse ecosystem of IoT devices. As we navigate this evolving digital landscape, a reevaluation of security strategies becomes imperative to address the distinct vulnerabilities inherent in IoT systems [1-2].

Zero-Trust Security, a paradigm gaining prominence in the realm of cybersecurity, offers a compelling alternative to conventional approaches. Unlike traditional security models that rely on perimeter defenses, Zero Trust operates on the fundamental premise that no entity, internal or external, should be inherently trusted [3]. Every interaction, irrespective of the source, is subjected to scrutiny, demanding continuous verification and authentication. This approach challenges the traditional notions of assumed trust within a network, calling for a comprehensive reassessment of security strategies [4].

Contrasting the Classic Security Approach with the Zero-Trust paradigm underscores the necessity of the latter in the context of IoT. Classic security models typically hinge on perimeter defenses, assuming safety within the network boundaries [5].

However, in the dynamic landscape of IoT, with diverse and distributed devices, the perimeter becomes porous, rendering conventional defenses less effective. Zero Trust, by adopting a holistic and adaptive security stance, accommodates the fluidity and complexity of IoT ecosystems [6-7].

The significance of revisiting Zero-Trust Security for IoT lies in its potential to provide a comprehensive and adaptable solution to the intricate security challenges posed by the proliferation of connected devices. The motivation behind this exploration stems from the escalating frequency and sophistication of cyber threats targeting IoT infrastructure [8]. By adopting a Zero-Trust approach, organizations can fortify their defenses, mitigating the risks associated with unauthorized access, data breaches, and malicious activities. This mini-review seeks to delve into the evolving landscape of Zero Trust in the context of IoT, shedding light on its practical applications, benefits, and the path forward in securing the increasingly interconnected digital realm.

2. The Imperative for Zero Trust in IoT

This section explores the compelling reasons behind the adoption of Zero Trust in the IoT landscape, delving into key drivers such as evolving business models, emerging partnerships, rapidly changing technology, regulatory dynamics, disruptive events, and the paradigm shift to remote work.

2.1. Evolving Business Models

The dynamic landscape of evolving business models in the IoT era necessitates a shift in security strategies. Traditional models, centered on perimeter defenses, struggle to adapt to the fluidity of modern business structures. As organizations embrace interconnected ecosystems, incorporating devices from various vendors and engaging in diverse collaborations, the need for a security paradigm like Zero Trust becomes paramount. Zero Trust's adaptive approach ensures that security measures align with the agile nature of evolving business models, safeguarding sensitive data and critical assets within an ever-expanding IoT ecosystem [9].

2.2. Emerging Partnerships

The rise of collaborative ventures and emerging partnerships in the IoT space introduces a complex network of interactions. These collaborations extend beyond organizational boundaries, involving multiple stakeholders and devices. Zero Trust provides a foundation for secure collaboration by treating every device and user as untrusted until proven otherwise. This approach becomes instrumental in mitigating the risks associated with sharing sensitive information across diverse networks, fostering a secure environment for the seamless integration of devices in emerging IoT partnerships [10].

2.3. Rapidly Changing Technology

In the realm of IoT, technology evolves at an unprecedented pace. The rapid adoption of new technologies, such as edge computing and 5G connectivity, introduces both opportunities and vulnerabilities. Traditional security models struggle to keep pace with these advancements, often leaving IoT devices exposed to emerging threats. Zero Trust, characterized by its agility and adaptability, becomes indispensable in this context, providing a proactive security framework that evolves with the technological landscape, ensuring robust protection against evolving cyber threats in the ever-changing IoT environment.

2.4. Regulatory, Geopolitical, and Cultural Forces

Regulatory frameworks, geopolitical shifts, and cultural nuances play a significant role in shaping the security landscape for IoT. Compliance requirements vary across regions, and geopolitical tensions can impact the threat landscape. Additionally, cultural factors influence user behavior and the perception of security. Zero Trust, with its decentralized and context-aware security model, accommodates the diversity of regulatory environments, geopolitical influences, and cultural nuances. This adaptability makes Zero Trust a crucial component for organizations navigating the complex interplay of regulatory, geopolitical, and cultural forces in the IoT space [11].

2.5. Disruptive Events

The inevitability of disruptive events, ranging from cyber-attacks to natural disasters, underscores the importance of resilient security measures in IoT deployments. Zero Trust, by assuming a continuous verification and validation stance, enhances an organization's ability to withstand and recover from disruptive events. Whether it's a malicious cyber-attack or an unforeseen natural calamity, Zero Trust ensures that access privileges are granted based on real-time assessments, minimizing the impact of disruptive events on the integrity and confidentiality of IoT systems.

2.6. Paradigm Shift to Remote Work

The paradigm shift towards remote work amplifies the complexity of securing IoT environments. With an increasing number of devices operating outside traditional corporate networks, the attack surface expands, exposing organizations to new vulnerabilities. Zero Trust, by eliminating the concept of implicit trust, aligns seamlessly with the distributed nature of remote work. It provides a robust security framework that authenticates and authorizes devices and users regardless of their location, ensuring that remote work does not compromise the security posture of IoT ecosystems [9-12].

3. **Principles of Zero-Trust In IoT**

As the complexity of IoT ecosystems continues to burgeon, the application of Zero-Trust Security emerges as a foundational pillar in safeguarding interconnected devices and data. In this section, we delve into the core principles that constitute the bedrock of Zero Trust within the IoT. Zero Trust, as a paradigm, revolutionizes traditional security notions by scrutinizing every interaction, device, and user, fostering a continuous verification and validation process.

3.1. IoT-based Work Enablement

In the rapidly evolving landscape of the IoT, the imperative for modern work enablement within organizational ecosystems cannot be overstated. Users must seamlessly traverse diverse networks and locations, demanding a paradigm that ensures consistent security assurances across all scenarios. Zero-Trust Security, aligned with organizational goals, becomes pivotal in providing a dynamic and adaptive security framework. By enabling users to work securely on any network, in any location, organizations not only enhance productivity but also align security measures with the evolving nature of modern work within the IoT ecosystem.

3.2. Goal Alignment:

In the intricate tapestry of IoT deployments, security must transcend its role as a mere safeguard; it must align seamlessly with organizational goals. A cohesive integration of security measures within the organizational framework, considering risk tolerance and thresholds, becomes paramount. Zero Trust, as a principle, ensures that security is not an impediment but a facilitator, enabling organizations to achieve their objectives while operating within acceptable risk parameters. This alignment ensures that security is not a hindrance but a catalyst for organizational success in the dynamic landscape of IoT [14].

3.3. Risk Alignment

Security in IoT is not a one-size-fits-all solution; instead, it necessitates a nuanced and consistent approach to risk management. The principles of Zero Trust align security risk management with the organization's risk framework, meticulously considering tolerance and thresholds. By consistently measuring and managing security risks, organizations can make informed decisions that resonate with their unique risk appetite. This approach ensures that security measures within the IoT ecosystem are tailored, adaptive, and harmonized with the overarching organizational risk landscape.

3.4. People Guidance and Stimulus

In the dynamic environment of IoT, organizational governance frameworks serve as guiding beacons, steering people, processes, and technology decisions. These frameworks, imbued with clear ownership structures, delineate decisions, policies, and aspirational visions. By providing guidance and inspiration, these frameworks become instrumental in fostering a security-conscious culture within the organization, ensuring that every stakeholder is aligned with the overarching security objectives in the ever-expanding realm of IoT [15].

3.5. Risk and Complexity Reduction

Governance in the context of IoT must act as a stabilizing force amidst the complexity and dynamic nature of interconnected systems. Zero Trust principles advocate for governance frameworks that not only simplify but also reduce the threat surface area. By streamlining processes and policies, governance becomes an enabler, minimizing complexities associated with IoT deployments while concurrently reducing the attack vectors, thus fortifying the security posture in the face of evolving threats.

3.6. Alignment and Automation

Aligning security policies and metrics with organizational missions and risk requirements is pivotal in the IoT landscape. Zero Trust emphasizes a proactive approach, favoring automated execution and reporting to ensure real-time adherence to security measures. This alignment not only streamlines processes within the organization but also positions security as an integral part of the organizational mission. Automation, guided by clear policies, becomes the linchpin for effective security governance in the IoT ecosystem.

3.7. Security for the Full Lifecycle:

The IoT lifecycle demands a sustained commitment to security, from the inception of data, transactions, or relationships to their eventual conclusion. Zero Trust principles advocate for a comprehensive approach, ensuring risk analysis and confidentiality, integrity, and availability assurances throughout the entire lifecycle. Asset sensitivity is reduced where possible, and assurances are provided for data in use, in-flight, and at rest. This approach ensures that security measures evolve with the evolving nature of data interactions within the dynamic and expansive IoT ecosystem [13-16].

3.8. Asset-Centric Security

In the IoT landscape, where a myriad of devices and applications coalesce, asset-centric security becomes imperative. Zero Trust advocates for a data-centric and application-centric approach, ensuring that security measures are as close to the assets as possible. This tailored approach minimizes productivity disruptions while offering a nuanced and effective security strategy that aligns with the diverse nature of assets within the IoT environment [17].

3.9. Least Privilege

Access control is a cornerstone of security in IoT, and the principle of least privilege takes center stage. Zero Trust emphasizes that access to systems and data should be granted only as required and promptly removed when no longer needed. This approach not only minimizes the potential for unauthorized access but also ensures that the IoT ecosystem operates with the least possible risk, aligning security measures with the dynamic access requirements in interconnected environments [18].

3.10. Simple and Pervasive

Security mechanisms within the IoT ecosystem must be characterized by simplicity, scalability, and ease of implementation. Zero Trust principles advocate for controls that are not only effective but also practical throughout the organizational ecosystem. By emphasizing simplicity and pervasiveness, security controls become an integral and seamless part of the IoT infrastructure, ensuring that they are readily implemented and managed, whether within internal or external organizational domains [19].

3.11. Explicit Trust in IoT

In the IoT paradigm, assumptions of integrity and trust level must be explicitly validated against organizational risk thresholds and tolerances. Zero Trust principles underscore the need for explicit validation of assets and/or data systems before allowing interactions. This approach ensures that trust is not assumed but verified, aligning security controls with the organizational risk landscape and fostering a secure and resilient IoT environment where every interaction is subject to scrutiny and validation [20].

4. Future Directions

In this section, we explore the evolving trajectory of Zero Trust within the context of IoT, delving into anticipated advancements, emerging trends, and crucial challenges that are set to shape the security paradigm in the years to come.

4.1. Integration with Emerging Technologies

As IoT continues to evolve, the integration of Zero-Trust Security with emerging technologies stands as a promising avenue. Future developments might see the amalgamation of artificial intelligence, machine learning, and blockchain to enhance the adaptability and efficiency of Zero Trust in safeguarding IoT ecosystems. These technologies can contribute to more intelligent threat detection, real-time risk assessment, and decentralized security architectures.

4.2. Continuous Authentication and Behavioral Analytics

The future of Zero Trust in IoT may witness a deeper emphasis on continuous authentication and behavioral analytics. Advancements in biometric authentication, user behavior analysis, and anomaly detection could fortify the Zero-Trust model. This ensures that the security posture adapts dynamically to the behavior patterns of users and devices, enhancing the overall resilience against evolving cyber threats.

4.3. Edge Computing and Zero Trust

With the proliferation of edge computing in IoT, the future direction of Zero Trust may involve tailored security strategies for edge devices. Implementing Zero Trust principles at the edge allows organizations to secure decentralized processing while maintaining a consistent security posture. The fusion of Zero Trust and edge computing ensures that security measures are applied closer to the data source, reducing latency and enhancing overall system efficiency.

4.4. Regulatory Compliance and Standardization

The future landscape of Zero-Trust Security in IoT is likely to witness an increased focus on regulatory compliance and standardization. As IoT deployments span across industries, adhering to specific regulations and standards becomes imperative. Future directions may involve the development of industry-specific standards for implementing Zero Trust in IoT, providing organizations with a clear framework to ensure compliance and mitigate regulatory risks.

4.5. Zero Trust for Supply Chain Security

As IoT ecosystems become more interconnected, securing the supply chain is emerging as a critical consideration. Future directions for Zero Trust may extend its application to supply chain security, ensuring that the entire lifecycle of IoT devices, from manufacturing to deployment, is protected. This involves establishing trustworthiness not only within an organization's network but also across the broader supply chain network.

4.6. Human-Centric Security Awareness

Future directions in Zero Trust for IoT should include a stronger emphasis on human-centric security awareness. Educating users and stakeholders about the principles of Zero Trust becomes essential in fostering a security-conscious culture. This may involve the development of training programs, awareness campaigns, and user-friendly interfaces that empower individuals to make security-conscious decisions in the IoT environment.

4.7. Resilience Against Quantum Threats

Anticipating the future threat landscape, Zero-Trust Security in IoT may need to address the potential challenges posed by quantum computing. Future developments might involve integrating post-quantum cryptography and quantum-resistant algorithms to ensure the continued efficacy of Zero Trust in the face of evolving cryptographic threats.

4.8. Collaboration and Information Sharing

The collaborative nature of IoT ecosystems suggests a future direction that encourages enhanced information sharing and collaboration among organizations. Establishing industry-wide threat intelligence sharing platforms and collaborative initiatives can fortify the collective defense against sophisticated cyber threats, aligning with the principles of Zero Trust.

4.9. User-Centric Privacy Controls

Considering the increasing concerns surrounding privacy in the IoT space, future directions for Zero Trust may include the development of more robust user-centric privacy controls. Organizations may need to adopt transparent and customizable privacy settings, empowering users to have greater control over the sharing and usage of their personal data within the Zero-Trust framework.

4.10. Automated Incident Response and Remediation

In the future, Zero Trust for IoT could see advancements in automated incident response and remediation. Implementing artificial intelligence and machine learning algorithms for rapid threat detection and automated response can significantly reduce the dwell time of cyber threats, enhancing the overall security posture of IoT environments.

5. Conclusions

This work has delved into the multifaceted realm of Zero-Trust Security within the IoT, offering a comprehensive overview of its principles, current applications, and future directions. As the IoT landscape continues to burgeon, the imperative for a security paradigm that challenges traditional assumptions becomes evident. Zero Trust's adaptability and holistic approach align seamlessly with the complexities of interconnected devices, providing a robust framework for mitigating evolving cyber threats. Through an exploration of the principles of Zero Trust, its application in diverse IoT scenarios, and a glimpse into the potential future developments, this review underscores the pivotal role that Zero Trust Security plays in fortifying the security posture of IoT ecosystems. As organizations navigate the intricate tapestry of IoT, the principles of continuous verification, least privilege, and dynamic risk management inherent in Zero Trust offer a beacon for resilient and adaptive security measures.

Funding

This research was conducted without external funding support.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Informed Consent Statement

Not applicable.

Data Availability Statement

Not applicable.

References

[1]. Samaniego, M., & Deters, R. (2018, July). Zero-trust hierarchical management in IoT. In *2018 IEEE international congress on Internet of Things (ICIOT)* (pp. 88-95). IEEE.

[2]. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing, 2022*.

[3]. Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1), 18-34.

[4]. Li, S., Iqbal, M., & Saxena, N. (2022). Future industry internet of things with zero-trust security. *Information Systems Frontiers*, 1-14.

[5]. Dimitrakos, T., Dilshener, T., Kravtsov, A., La Marra, A., Martinelli, F., Rizos, A., ... & Saracino, A. (2020, December). Trust aware continuous authorization for zero trust in consumer internet of things. In *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 1801-1812). IEEE.

[6]. 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.

[7]. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE Access*, *10*, 57143-57179.

[8]. Ameer, S., Gupta, M., Bhatt, S., & Sandhu, R. (2022, June). Bluesky: Towards convergence of zero trust principles and score-based authorization for iot enabled smart systems. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies* (pp. 235-244).

[9]. Colombo, P., Ferrari, E., & Tümer, E. D. (2021, December). Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era. In *2021 third ieee international conference on trust, privacy and security in intelligent systems and applications (tps-isa)* (pp. 159-166). IEEE.

[10]. Wang, J., Chen, J., Xiong, N., Alfarraj, O., Tolba, A., & Ren, Y. (2023). S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT. *ACM Transactions on Internet Technology*, *23*(3), 1-23.

[11]. Meng, L., Huang, D., An, J., Zhou, X., & Lin, F. (2022). A continuous authentication protocol without trust authority for zero trust architecture. *China Communications*, *19*(8), 198-213.

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

[13]. Stafford, V. A. (2020). Zero trust architecture. *NIST special publication*, *800*, 207.

[14]. Uttecht, K. D. (2020). Zero Trust (ZT) concepts for federal government architectures. *Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Lexington, Massachusetts*.

[15]. Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part I 6* (pp. 50-60). Springer Singapore.

[16]. Shah, S. W., Syed, N. F., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2021). LCDA: lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Computers & Security*, *108*, 102351.

[17]. Bertino, E. (2021). Zero trust architecture: does it help?. *IEEE Security & Privacy*, *19*(05), 95-96.

[18]. Federici, F., Martintoni, D., & Senni, V. (2023). A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics*, *12*(3), 566.

[19]. Chen, Z., Yan, L., Lü, Z., Zhang, Y., Guo, Y., Liu, W., & Xuan, J. (2021). Research on zero-trust security protection technology of power IoT based on blockchain. In *Journal of Physics: Conference Series* (Vol. 1769, No. 1, p. 012039). IOP Publishing.

[20]. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, *2021*, 1-10.