Adoption of Zero Trust Architecture (ZTA) in the Protection of Critical Infrastructure

Abraham Olasunkanmi Ojo

DOI: 10.22178/pos.113-2

JEL Classification: K39

Received 02.01.2025
Accepted 28.01.2025
Published online 31.01.2025

Corresponding Author:
abraham.cyberdefender@gmail.com

Abstract. Securing critical infrastructure (CI), including energy, healthcare, transportation, and financial systems, has become a pressing concern in the face of increasingly sophisticated cyber threats. These essential systems underpin modern society, and disruptions to their operations can have severe economic, social, and safety consequences. Traditional perimeter-based cybersecurity approaches have proven insufficient against evolving attack vectors, highlighting the need for more resilient strategies such as Zero Trust Architecture (ZTA). Zero Trust Architecture represents a paradigm shift in cybersecurity, advocating "never trust, always verify." Unlike legacy models, ZTA emphasises continuous authentication, least privilege access, and network micro-segmentation to mitigate external and internal threats. By assuming that breaches are inevitable, ZTA enforces stringent access controls and real-time monitoring to safeguard critical systems. This review examines the adoption of ZTA in the protection of critical infrastructure.

Key findings showed the benefits of ZTA, including enhanced resilience against cyberattacks and improved regulatory compliance. The paper also discusses challenges such as integration with legacy systems, resource constraints, and organisational resistance. Recommendations are provided to guide the phased implementation of ZTA and promote cross-sector collaboration to secure critical infrastructure effectively.

Keywords: critical infrastructure; cyberattacks; legacy model; Zero Trust Architecture.

INTRODUCTION

Critical Infrastructure (CI) encompasses the essential systems, assets, and networks that are vital to the functioning of modern society, which include sectors such as energy (power grid), transportation, healthcare, finance, water supply, and communication systems [1]. The disruption or compromise of these systems can lead to significant economic losses, public safety hazards, and national security concerns [2]. CI is the backbone of societal well-being, ensuring the continuity of services critical for daily life and economic stability. Sophistic cyberattacks increasingly target crucial infrastructure due to its high-value nature and interdependence across sectors [1]. Threat actors, including nation-states, organised crime groups, and hacktivists, exploit vulnerabilities in these systems to disrupt operations, extort ransom, or gain strategic advantage, and common vulnerabilities include legacy systems where many CI sectors rely on outdated technologies with limited or no built-in cybersecurity features [3]. Another vital aspect is insider threats, where employees with access to sensitive systems can inadvertently or maliciously compromise security. In addition, increased attack surface exists, where integrating IoT devices, remote access systems, and digital transformation efforts has expanded the avenues for exploitation [4]. Prominent examples of attacks include the Colonial Pipeline ransomware incident and the Stuxnet malware targeting industrial control systems. Such cases and incidents highlight the urgent need for robust security measures to protect CI [5, 6].

Therefore, this review aims to evaluate the adoption of Zero Trust Architecture in protecting critical infrastructure. It explores the principles and benefits of ZTA, analyses the challenges and limitations of its implementation, and identifies best practices for integrating ZTA with existing systems. By focusing on real-world case studies and

emerging trends, the paper seeks to provide actionable insights for policymakers, organisations, and stakeholders working to secure critical infrastructure against a rapidly changing threat landscape.

RESULTS AND DISCUSSION

Principles and Significance of Zero Trust Architecture: Zero Trust Architecture is a cybersecurity framework designed to address the limitations of traditional perimeter-based security models in a world where the boundaries of networks have become increasingly blurred [4, 7]. ZTA represents a modern approach to cybersecurity, fundamentally shifting from the traditional perimeter-based model, and the core principle of ZTA is "never trust, always verify," which assumes that no entity, whether inside or outside the network, should be inherently trusted [4, 7]. Integrating these principles allows Zero Trust Architecture to create a dynamic and proactive cybersecurity posture, enabling organisations to protect their most critical assets in an increasingly hostile digital landscape [3]. Its adoption is especially crucial for essential infrastructure sectors, where the stakes of a successful cyberattack are exceptionally high.

The significance of ZTA lies in its adaptability to modern, complex environments characterised by cloud computing, mobile workforces, and interconnected systems. ZTA's adoption is particularly significant for critical infrastructure, providing a proactive and adaptive defence against evolving cyber threats. Through its implementation, organisations can enhance resilience, minimise risks, and ensure the secure delivery of essential services [4, 8]. According to [3, 9], the main principles and components of ZTA are:

Identity Verification: This is where ZTA mandates rigorous identity verification for every access request, regardless of the user's location within or outside the network; this includes employing strong Identity and Access Management (IAM) systems with features such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), and dynamic risk-based assessments.

Least Privilege Access: This is where users and devices are granted access strictly on a need-to-know basis; this minimises the potential damage from compromised accounts by ensuring that entities only interact with the resources necessary for their tasks.

Micro-Segmentation: This is where networks are divided into smaller, isolated zones. Each segment operates independently, reducing an attacker's ability to move laterally across the network if one segment is breached.

Continuous Monitoring and Assessment: ZTA constantly evaluates users, devices, and applications to detect anomalies and unauthorised activities. This approach leverages real-time analytics, machine learning, and automated response mechanisms to maintain a secure environment.

Device Security Posture: This is where devices must meet predefined security standards before gaining access to network resources; this ensures that endpoints, including laptops, smartphones, and IoT devices, do not become entry points for attackers.

Encryption and Secure Communication: This is where all data, whether in transit or at rest, is encrypted to prevent unauthorised access; this ensures the confidentiality and integrity of sensitive information.

Assume Breach: This is where ZTA operates under the assumption that breaches are inevitable or may have already occurred. This principle shifts the focus from merely preventing breaches to minimising their impact and ensuring rapid detection and containment.

On the other hand, the significance of Zero Trust Architecture is all-encompassing. First, because of its enhanced protection against advanced threats, it addresses sophisticated threats, such as ransomware, insider attacks, and supply chain vulnerabilities, by limiting exposure and enforcing strict controls [1, 10]. In terms of its adaptability to modern environments, and given the rise of cloud services, remote work, and IoT, ZTA provides a scalable and flexible security framework that adapts to these diverse ecosystems [11]. In addition, ZTA significantly reduces the opportunities for attackers to exploit vulnerabilities or access sensitive assets by segmenting networks and continuously verifying trust, thereby minimising the attack surface. ZTA also aligns with many global cybersecurity standards, practices and regulations, such as NIST SP 800-207 (Zero Trust Architecture guidelines), GDPR, and HIPAA, ensuring that organisations meet compliance and regulatory requirements [11]. More so, the ZTA's principle of "never trust, always verify" ensures that even trusted insiders are subject to rigorous access controls and moni-

toring, mitigating the risks posed by malicious or negligent employees, which indicates ZTA's resilience to insider threats. Likewise, as organisations adopt new technologies and business models, ZTA supports digital transformation and ensures security is integrated into the fabric of these transformations, enabling innovation without compromising security [1].

Cybersecurity Challenges in Critical Infrastructure

Critical infrastructure (CI) is essential for the functioning of society, and its protection is paramount to ensure economic stability, public safety, and national security. However, CI faces various cybersecurity challenges that make securing these systems increasingly tricky. These challenges are compounded by legacy systems, digital transformation efforts, the evolving threat landscape, and high-profile cyber incidents demonstrating vulnerabilities in CI defences [6].

Legacy systems are a significant cybersecurity challenge for critical infrastructure. Many CI sectors, such as energy, transportation, and manufacturing, still rely on outdated hardware and software systems not designed with modern security needs in mind [12]. The limitations of these systems include outdated security features and software, as many legacy systems lack built-in security features or cannot support contemporary encryption, access control, or multi-factor authentication methods. Also, there is vulnerability to modern attacks as legacy systems may not be patched against known vulnerabilities, making them susceptible to exploitation by cybercriminals and nation-state actors [6]. Securing these systems often involves manual updates and patch management, which can be slow and error-prone. The incompatibility with modern tools is another pressing issue, and this is because integrating legacy systems with newer security technologies, such as next-generation firewalls, Intrusion Detection Systems (IDS), and SIEM platforms, is often difficult [13]. This lack of interoperability can leave security gaps and reduce the effectiveness of contemporary cybersecurity measures. Another limitation is the high maintenance costs, as maintaining and securing ageing infrastructure can be somewhat costly, especially when attempting to retrofit these systems with new security measures [14]. Organisations may prioritise maintaining functionality over investing in necessary updates, leading to a security debt that compounds over time. These limitations make legacy systems an attractive target for attackers and present a substantial barrier to adopting more robust, modern cybersecurity frameworks such as Zero Trust Architecture. Another significant challenge is the digital transformation and the growing adoption of the Internet of Things (IoT), which drive innovation in critical infrastructure sectors. However, these also expand the attack surface significantly because of some key factors [1, 5, 6]. First, as IoT devices proliferate across industries, they become entry points for cyberattacks, leading to many IoT devices with weak security controls, lack robust patching mechanisms, and often have hardcoded passwords that are easy targets for attackers. When connected to critical infrastructure, these devices can be leveraged in attacks such as DDoS (Distributed Denial of Service), ransomware, and even physical sabotage [5]. Likewise, the shift to cloud environments has introduced new complexities in data protection, access control, and securing communication between on-premise and cloud resources. While the cloud offers scalability and flexibility, its decentralised nature means that organisations must manage security across multiple environments and enforce consistent access control policies [8]. The rise of remote work, accelerated by the COVID-19 pandemic, is also a notable problem because this has eroded the traditional network perimeter. According to [6], issues with the integration of Operational Technology (OT) and (Information Technology (IT) cannot be overemphasised because many CI sectors are integrating OT with IT systems. While this integration enhances operational efficiency, it also opens up potential vectors for cyberattacks, as OT systems often have limited security features and are highly vulnerable to exploits.

All these factors contribute to a dramatically expanded attack surface, making it difficult for traditional perimeter-based security systems to safeguard CI effectively. ZTA's emphasis on continuous verification and micro-segmentation can help mitigate some of these risks.

Evolving Threat Landscape: The evolving threat landscape presents increasingly sophisticated and targeted attacks on critical infrastructure. These threats can emanate from various sources, such as:

Nation-State Actors: Nation-state actors pose a growing risk to critical infrastructure, using cyberattacks as part of geopolitical strategies.

These attacks are highly advanced, employ custom malware, and aim to steal intellectual property, gather intelligence, or disrupt key systems. A notable example is the Stuxnet attack on Iran's nuclear facilities, which was attributed to state-sponsored actors [15]. These actors are also suspected of targeting power grids, water systems, and energy facilities to cause long-term damage and disruptions.

Ransomware: The rise of ransomware attacks on critical infrastructure has become one of the most pressing cybersecurity challenges. In ransomware attacks, threat actors encrypt systems and demand ransom payments, often crippling organisations for days or weeks [16]. High-profile attacks, such as the Colonial Pipeline attack, highlight the devastating impact of ransomware on critical sectors, including energy and transportation. In these cases, attackers encrypt data and threaten to release sensitive information unless the ransom is paid.

Supply Chain Attacks: Cybercriminals increasingly target the supply chain, exploiting third-party vulnerabilities to access critical infrastructure systems [17]. For instance, the SolarWinds attack in 2020, where hackers injected malware into software updates for IT management software, is a prime example of a supply chain attack. These attacks can have wide-reaching consequences, providing attackers with trusted access to systems and data across multiple organisations, including those in the critical infrastructure sector.

There are other case studies of cyber incidents targeting critical infrastructure. For instance, the Colonial Pipeline attack of 2021, which represents one of the most notable ransomware attacks in recent history, the colonial pipeline attack led to the shutdown of a critical pipeline that supplies gasoline, diesel, and jet fuel to much of the East Coast of the United States [5]. The attack exploited the company's network vulnerabilities, resulting in widespread fuel shortages, price increases, and significant financial losses. The attackers used a ransomware variant known as DarkSide and initially demanded a ransom payment; such an attack underscored the vulnerability of critical energy infrastructure and the need for stronger cybersecurity measures, including robust identity management and threat detection capabilities [18, 19]. Another case is the Ukrainian power grid attacks in 2015 and 2016, where the Nation-state actors, believed to be affiliated with Russian cyber operatives, launched cyberattacks on Ukraine's power grid in 2015 and 2016. The attackers used spear-phishing emails and malware to infiltrate the grid's control systems, temporarily causing blackouts for over 200,000 people. These attacks demonstrated the potential for cyberattacks to cause widespread disruption in power infrastructure, highlighting the importance of resilience and cybersecurity in critical services [16]. The ransomware attack on the Irish Health Service in 2021 is another talking point, which disrupted essential healthcare systems, including patient records, appointment scheduling, and diagnostic services [20]. The attack was linked to the Conti ransomware group, which demanded a ransom payment for the decryption key. This incident highlighted the vulnerability of the healthcare sector and the need to secure IT and OT systems that support life-critical services. As stated earlier, these threats and other evolving ones require new cybersecurity approaches; hence, ZTA's principles are designed to defend against these advanced and persistent threats.

Application of ZTA in hybrid environments: By integrating on-premises systems with cloud services, modern critical infrastructure systems are increasingly hybrid, with many organisations integrating legacy systems with cloud services [21]. ZTA provides the necessary framework to secure this hybrid environment by extending trust verification and monitoring beyond traditional on-premises systems. It can seamlessly extend to on-premises and cloud environments, ensuring consistent security policies across all assets [22]; this is particularly important as critical infrastructure increasingly relies on cloud services for scalability, remote access, and data processing, and whether data is stored on-site or in the cloud, ZTA ensures that access is controlled and monitored in real-time [3]. One of the challenges of a hybrid infrastructure is managing access to both on-premises and cloud-based resources, and ZTA leverages a unified IAM system that provides seamless access control across both environments [22]; this ensures that identity verification, multi-factor authentication, and least-privilege access are uniformly applied across the entire infrastructure, whether the resource resides on the organisation's premises or in a third-party cloud service [22]. More so, the ability to apply consistent security policies to both on-premises and cloud environments ensures that security measures are not siloed. ZTA's principles, such as continuous verification and least-privilege ac-

cess, can be enforced across all systems and assets, regardless of where they reside, thereby reducing the risk of vulnerabilities arising from inconsistencies in security controls between environments [3]. More importantly, ensuring data protection becomes more complex in a hybrid environment. ZTA addresses this by mandating encryption for data at rest and in transit, whether on-premises or in the cloud. Additionally, data access is strictly controlled and monitored, reducing the potential for unauthorised access or data breaches [3].

Challenges in Adopting ZTA for Critical Infrastructure

While Zero Trust Architecture offers a robust framework for securing Critical Infrastructure (CI), its adoption comes with several challenges. These challenges range from technological and operational barriers to regulatory and compliance issues, and addressing these obstacles is critical to successfully implementing ZTA in vital sectors such as energy, transportation, healthcare, and finance.

The first challenge is associated with technological barriers, which have to do with compatibility issues of the legacy systems. Many organisations in critical infrastructure sectors still rely heavily on legacy systems developed decades ago and not designed with modern cybersecurity frameworks in mind, thereby lacking the flexibility to integrate with newer security measures like ZTA [3]. Similarly, legacy systems typically use outdated communication protocols and security models incompatible with ZTA's core principles of continuous identity verification and micro-segmentation [13]. Integrating these systems with ZTA technologies, such as advanced Identity and Access Management (IAM) or real-time monitoring tools, can be extremely difficult. It makes enforcing ZTA policies across the entire infrastructure hard, leaving critical vulnerabilities [6]. Then, adapting legacy systems to work within a ZTA framework often requires custom solutions (customisation needs), extensive patching, or even complete overhauls [6], which can significantly slow the implementation process, increase complexity, and drive up costs. According to [14], the high implementation costs and resource requirements of implementing ZTA in critical infrastructure environments are both technologically complex and resource-intensive because of the initial setup costs; this is to say that the investment required to deploy ZTA can be significant, especially for organisations that rely on extensive legacy systems. Expenses might include purchasing and deploying new hardware, software, and security tools and integrating them into existing IT and OT infrastructures. Another pressing issue is the need for organisations to train their workforce on ZTA principles, tools, and processes, which can incur additional costs. Implementing IAM, micro-segmentation, and continuous monitoring solutions also demands specialised expertise involving training and skill development, and after initial deployment, maintaining ZTA in CI requires constant investment in monitoring, auditing, and upgrading security systems to stay ahead of emerging threats [6, 23]. These ongoing resource requirements can be a burden, particularly for smaller organisations or those with limited budgets. As a result, the financial and resource-intensive nature of ZTA implementation can be a significant obstacle, particularly for CI sectors with tight budgets or restricted access to advanced technological resources.

The second challenge is associated with operational challenges involving organisational resistance to change. Indeed, adopting a zero-trust framework requires a fundamental shift in how organisations approach security, and the shift can be met with resistance, especially in industries that have long relied on traditional, perimeter-based models [24]. For instance, employees and leadership who are accustomed to a more open or less restrictive approach to network access may be resistant to the stringent policies required by ZTA, such as continuous identity verification and least-privilege access, and overcoming this cultural resistance often requires a strong change management strategy that includes communication about the benefits and long-term necessity of ZTA. Furthermore, implementing ZTA in CI can disrupt day-to-day operations [25]. For example, micro-segmentation may require re-engineering parts of the network, leading to downtime or delays in service delivery. Employees accustomed to a particular way of working may struggle with the more secure (often more complex) access controls enforced by ZTA. At the same time, those who lack cybersecurity expertise in critical infrastructure sectors may face challenges in adopting ZTA [6]. Energy, transportation, and manufacturing industries often focus on Operational Technology (OT) rather than information technology (IT). The convergence of IT and OT in critical infrastructure and ZTA imple-

mentation requires specialised knowledge of both domains [24]. However, many organisations struggle to find professionals proficient in OT security and ZTA-specific technologies. Consequent to the skills, expertise, and training gaps, especially in the sectors that have not traditionally prioritised cybersecurity, there may be a steep learning curve associated with ZTA, while the lack of internal expertise necessary to fully understand and implement the security models and technologies that ZTA demands may force organisations to rely on external consultants, which can increase costs and prolong the implementation timeline [6].

The third challenge is linked to regulatory and compliance issues involving misalignment between ZTA principles and existing regulatory frameworks [5]. ZTA is a modern approach to cybersecurity, and its principles may not always align perfectly with existing regulatory and compliance frameworks. Critical infrastructure sectors are often subject to strict regulatory standards that govern how data is handled, who can access it, and under what circumstances. However, the flexible and dynamic nature of ZTA may conflict with specific prescriptive regulatory requirements [26]. Regarding data access and sharing regulations, ZTA's focus on least-privilege access may clash with regulatory requirements that necessitate broad access to specific data for monitoring or reporting purposes. For example, laws like the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) may have specific guidelines on data access that could conflict with ZTA's model of minimising access rights. Equally, many industries, particularly healthcare and finance, require detailed records of access logs, data sharing, and other security actions. ZTA's real-time, dynamic enforcement of access controls may be at odds with these regulations' static, audit-heavy reporting requirements. Aligning ZTA with existing regulatory frameworks will likely require continuous collaboration between industry stakeholders, regulators, and cybersecurity professionals to ensure compliance without compromising security [27]. Another important aspect is the variability in global cybersecurity standards for CI. The regulatory landscape for critical infrastructure cybersecurity is inconsistent across regions and countries, presenting significant challenges for organisations operating in multiple jurisdictions and regional variability [5]. Different countries have different standards for cybersecurity. For example, the NIST Cybersecurity Framework in the United States, the EU Network and Information Security (NIS) Directive, and the ISO/IEC 27001 standard each contain distinct requirements and guidelines. The lack of a unified, global cybersecurity standard for critical infrastructure creates complexities for multinational organisations trying to implement ZTA consistently across borders [5]. Even within a specific region, the enforcement and interpretation of cybersecurity regulations can vary between states or regulatory bodies; this makes it difficult for organisations to develop a one-size-fits-all approach to implementing ZTA, as they must adapt their strategies to the different regulatory environments in which they operate. For global organisations, navigating multiple regulatory environments and ensuring that ZTA aligns with other standards can be time-consuming and costly.

In conclusion, while Zero Trust Architecture offers a robust solution to the growing cybersecurity challenges faced by critical infrastructure, its adoption is fraught with technological, operational, and regulatory challenges. Compatibility issues with legacy systems, high implementation costs, resistance to change, and a shortage of cybersecurity expertise can all hinder the adoption of ZTA. The misalignment between ZTA principles and existing regulatory frameworks and the variability of global cybersecurity standards further complicate the implementation process. Overcoming these barriers will require a coordinated effort among technology providers, industry leaders, regulators, and cybersecurity professionals to ensure that ZTA can be effectively deployed to protect critical infrastructure from emerging cyber threats.

Strategies and Best Practices in the Implementation of Zero Trust Architecture

Implementing Zero Trust Architecture in critical infrastructure requires a well-thought-out strategy that balances technological, operational, and regulatory considerations. ZTA is a comprehensive, dynamic cybersecurity approach requiring a phased and methodical implementation process. Below are key strategies and best practices to guide organisations through successfully adopting ZTA in protecting critical infrastructure [6, 28]. It is essential to recognise that ZTA implementation is a complex and long-term process that requires careful planning and phased execu-

tion, and to have a seamless implementation; organisations should have a clear roadmap that can provide a structured approach and ensure that the transition to Zero Trust is gradual and manageable [1]. Before implementing ZTA, organisations must conduct a thorough risk assessment to understand their current security posture, identify potential vulnerabilities, and assess the risks to critical systems. Such sequential processes help ensure that ZTA is applied effectively and focused on the areas of most significant concern [14]. Critical infrastructure organisations often operate under existing cybersecurity frameworks and regulations. Proper integration of ZTA with these frameworks ensures a smoother adoption and guarantees compliance with relevant standards. ZTA This appears to be a plausible strategy and best practice to guide organisations through successfully adopting ZTA to protect critical infrastructure.

Building Cross-Sector Partnerships and Fostering Information Sharing in Cybersecurity

Effective cybersecurity requires collaboration across sectors and organisations, especially in critical infrastructure. Cyber threats often target multiple industries simultaneously, and a single breach can have cascading effects on other sectors. Therefore, building partnerships and promoting information sharing are essential strategies for improving ZTA implementation and resilience [6]. Governments and private industry must cooperate to protect critical infrastructure from cyber threats. Public-private partnerships can facilitate information sharing, joint threat intelligence initiatives, and the development of common standards. These collaborations enable essential infrastructure sectors to understand emerging threats better, share best practices, and coordinate incident response efforts. Energy, finance, and healthcare sectors can benefit from collaborating on cybersecurity best practices and threat intelligence [4]. For instance, Industry groups, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) or Energy Sector Cybersecurity Coordination Center (CESER), foster collaboration and help organisations stay informed about current threats, vulnerabilities, and emerging technologies.

Cross-sector partnerships can also facilitate coordinated responses to large-scale cyberattacks. Organisations can quickly identify and mitigate threats by sharing information on attacker Tactics, Techniques, And Procedures (TTPs). In the event of an attack, collaborative response efforts can reduce the overall impact on critical infrastructure. Adopting ZTA is not just a technological transformation but a cultural shift that requires continuous education and awareness, such that employees across all levels must understand the principles of Zero Trust and their role in protecting the organisation from cyber threats and related attacks [29]. Suffice it to say that organisations should invest in regular, up-to-date cybersecurity training programs for employees. These programs should cover ZTA principles such as the importance of identity verification, multi-factor authentication, and the concept of least privilege access. Training should also include recognising and responding to cyber threats, such as phishing attacks, insider threats, or social engineering tactics.

Additionally, specific training should be designed for different organisational roles [6]. For instance, IT professionals will require training on deploying and managing ZTA tools. At the same time, end-users may need guidance on using secure access methods or recognising suspicious activities. Specialised training for security teams on threat detection and incident response is also essential. Security awareness should be an ongoing initiative that fosters a culture of vigilance across the organisation [23]; this can be achieved through regular communication, simulated phishing exercises, and encouraging employees to report potential security issues. Ensuring all employees understand their responsibility in maintaining critical infrastructure security can significantly reduce human error, which is often a key factor in cyber incidents.

CONCLUSIONS

Zero Trust Architecture offers a transformative approach to securing critical infrastructure by eliminating implicit trust and enforcing robust access controls, continuous monitoring, and data protection mechanisms. Principles such as "never trust, always verify" and least privilege access are crucial for defending against modern cybersecurity threats, including ransomware, insider threats, and nation-state attacks. Despite its benefits, adopting ZTA poses challenges such as legacy system compatibility, high implementation costs, and regulatory complexities. Overcoming these barriers requires technological innovation, proactive government policies, and collaborative

efforts among industries, governments, and international organisations. In agreement with [30], technologies such as AI, blockchain, and quantum cryptography, combined with evolving standards and cross-sector partnerships, will play a pivotal role in enabling ZTA adoption. Stakeholders must prioritise ZTA implementation to protect critical infrastructure, ensuring its resilience and security in an increasingly interconnected world. By addressing challenges through concerted efforts and fostering a culture of cybersecurity, organisations can safeguard vital systems and promote long-term security for essential services.

Funding

This research received no funding from any source.

Ethical Considerations

This study was carried out in line with Helsinki's declaration on research guidelines: "anonymity, informed consent, privacy, confidentiality, and professionalism".

Conflict of interest

The authors declared no conflict of interest.

REFERENCES

1. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks, 156*, 103414. doi: 10.1016/j.adhoc.2024.103414

2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *National Institute of Standards and Technology Special Publication 800-207* doi: 10.6028/nist.sp.800-207

3. Adapa, V. R. K. (2024). Zero Trust Architecture Implementation In Critical Infrastructure: a Framework For Resilient Enterprise Security. *International Journal Of Advanced Research In Engineering & Technology, 15*(6), 76–89. doi: 10.34218/ijaret_15_06_006

4. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy, 25*(12), 1595. doi: 10.3390/e25121595

5. Kilovaty, I. (2023). Cybersecuring the Pipeline. *Houston Law Review, 60.*

6. Elete, N. T. Y. (2024). Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations. *Computer Science & IT Research Journal, 5*(12), 2664–2681. doi: 10.51594/csitrj.v5i12.1759

7. Kindervag, J. (2010). No More Chewy Centers: The Zero Trust Model of Information Security. *Forrester Research Inc.*

8. 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*, 1–13. doi: 10.1155/2022/6476274

9. Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces, 89*, 103832. doi: 10.1016/j.csi.2024.103832

10. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28. doi: 10.1016/j.jnca.2017.04.002

11. Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems, 85,* 235–249. doi: 10.1016/j.future.2018.04.007

12. Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access, 8*, 128440–128475. doi: 10.1109/access.2020.3007960

13. Al-Hawawreh, M., Alazab, M., Ferrag, M. A., & Hossain, M. S. (2023). Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. *Journal of Network and Computer Applications, 223,* 103809. doi: 10.1016/j.jnca.2023.103809

14. Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust architecture: Potential solutions and challenges. *Deleted Journal, 21*(2), 294–317. doi: 10.1007/s11633-023-1456-2

15. Buchanan, S. S. (2022). *Cyber-Attacks to Industrial Control Systems since Stuxnet: A Systematic Review* (Thesis; Capitol Technology University).

16. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: a recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3.* doi: 10.3389/fcomp.2021.563060

17. Zhang, Y., Sun, Z., Yang, L., Li, Z., Zeng, Q., He, Y., & Zhang, X. (2020). All your PLCs belong to me: ICS ransomware is realistic. *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 502–509. doi: 10.1109/trustcom50675.2020.00074

18. Dudley, R., & Golden, D. (2021). The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. *ProPublica.*

19. Gawazah, L., Rondla, A., & Balhareth, M.S.A. (2024). To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack. *Thunderbird School of Global Management.*

20. Daly, P. (2022). "Writing on a curved surface" The operational response to the cyber-attack on the Irish health service. *Médecine De Catastrophe - Urgences Collectives, 6*(4), 275–277. doi: 10.1016/j.pxur.2022.10.002

21. Tunc, C., Hariri, S., Merzouki, M., Mahmoudi, C., De Vaulx, F. J., Chbili, J., Bohn, R., & Battou, A. (2017). Cloud Security Automation Framework. *Conference: 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W),* 307–312. doi: 10.1109/fas-w.2017.164

22. Sharma, A., Sharma, S., & Dave, M. (2015). Identity and access management- a comprehensive study. *Conference: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT),* 1481–1485. doi: 10.1109/icgciot.2015.7380701

23. Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and attacks against industrial control systems and critical infrastructures. *arXiv (Cornell University).* doi: 10.48550/arxiv.2109.03945

24. Kara, I., & Aydos, M. (2021). The rise of ransomware: Forensic analysis for Windows-based ransomware attacks. *Expert Systems With Applications, 190*, 116198. doi: 10.1016/j.eswa.2021.116198

25. Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: An Industrial Cyber-Physical Systems (ICPS) perspective. *ACM Transactions on Cyber-Physical Systems, 6*(3), 1–27. doi: 10.1145/3548691

26. Romsom, E. (2022). Global oil theft: impact and policy responses. *In Working Paper Series.* doi: 10.35188/unu-wider/2022/147-1

27. Bobbert, Y. (2020). Zero trust validation: From practical approaches to theory. *Scientific Journal of Research & Reviews, 2*(5). doi: 10.33552/sjrr.2020.02.000546

28. Pookandy, J. (2021). Multi-factor authentication and identity management in cloud CRM with best practices for strengthening access controls. *International Journal of Information Technology and Management Information Systems (IJITMIS), 12*(1), 85-96.

29. Emmanni, P. S. (2024). Implementing a zero-trust architecture in hybrid cloud environments. *International Journal of Computer Trends and Technology, 72*(5), 33–39. doi: 10.14445/22312803/ijctt-v72i5p104

30. 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. *Journal of Physics Conference Series, 1769*(1), 012039. doi: 10.1088/1742-6596/1769/1/012039