INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT

eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 07 (2025)

# INTEGRATING ZERO-TRUST ARCHITECTURE INTO INDUSTRIAL CONTROL SYSTEMS FOR RESILIENCE AGAINST RANSOMWARE AND INSIDER THREATS IN OFFSHORE OIL & GAS CRITICAL INFRASTRUCTURE

**Dr. Ananya Rajiv**

Department of Cybersecurity Studies, Global Institute of Technology and Security, Worldwide University, India

**Abstract:** Critical infrastructure — especially industrial control systems (ICS) underpinning offshore oil and gas operations — faces growing cyber threats, ranging from ransomware to insider exploitation. Traditional perimeter-based defenses have repeatedly proven insufficient: attackers increasingly exploit vulnerabilities both at the network edge and within trusted domains. This paper explores how a comprehensive adoption of zero-trust architecture (ZTA) tailored for industrial control environments can meaningfully mitigate such risks. Through a systematic literature synthesis, threat-to-control mappings, and conceptual modeling, we analyze key vulnerabilities inherent in ICS and critical infrastructure, highlight how ransomware and insider attacks manifest in these contexts, and identify how zero-trust strategies — including identity-centric authentication, micro-segmentation, continuous verification, and contextual access control — can address these gaps. Particular attention is paid to the unique constraints and demands of offshore oil and gas ICS: real-time operations, legacy hardware, and physical process dependencies. Our analysis reveals both substantial potential for risk reduction and non-trivial challenges including latency, interoperability, and organizational readiness. We conclude with recommendations for research and phased deployment approaches that balance secure access with operational continuity.

**Keywords:** Zero-Trust Architecture, Industrial Control Systems, Ransomware, Offshore Oil & Gas, Critical Infrastructure Security, Insider Threat, Access Control.

## Introduction

Industrial control systems (ICS) and other forms of critical infrastructure form the backbone of modern societal functioning — powering utilities, managing water supply, controlling transportation networks, and enabling resource extraction industries such as offshore oil and gas. However, along with increasing digitization, these systems have become prime targets for cyber adversaries. A growing body of work has documented not only vulnerabilities in ICS but also a rising incidence of ransomware and targeted attacks against critical infrastructures. For example, Makrakis et al. (2021) provided a comprehensive survey of vulnerabilities and attacks against ICS and critical infrastructures, underscoring systemic weak points. Meanwhile, sector-specific analyses such as those focused on the offshore oil and gas industry emphasize unique cybersecurity challenges introduced by the convergence of physical and digital control systems (Mohammed et al., 2022).

Concurrently, cyberattack modalities have evolved: ransomware — once associated with commodity targeting of endpoint PCs — has increasingly impacted critical infrastructure sectors (Kara & Aydos, 2021). Insider threats, misconfigurations, supply-chain insecurities, and lack of robust identity and access controls (IAC) have emerged as recurring vulnerabilities, especially when systems rely on legacy ICS protocols and flat network topologies (Kim et al., 2020). Traditional perimeter-based defenses (firewalls, network segmentation, static trust zones) are inadequate in this environment: once an adversary gains a foothold within the trusted network boundary, they can often traverse laterally with minimal resistance.

In parallel, the concept of Zero-Trust Architecture (ZTA) has gained traction as a paradigm shift in defensive posture. Rather than trusting hosts or networks by default, ZTA enforces strict identity verification, least-privilege access, micro-segmentation, continuous authorization, and role-based or context-aware access controls (Bobbert, 2020; He et al., 2022). Research has begun to explore ZTA in cloud computing (Mehraj & Banday, 2020), hybrid cloud environments (Emmanni, 2024), and Internet-of-Things (IoT) domains — including power IoT when combined with blockchain-based validation (Chen et al., 2021). Yet, there remains a significant gap: despite the severe risks faced by ICS — especially in offshore oil & gas contexts — there has been limited systematic exploration of how zero-trust frameworks could be adapted and practically applied in such environments.

This paper seeks to address that gap. By integrating insights from ransomware forensics (Kara & Aydos, 2021), ICS threat taxonomies (Makrakis et al., 2021), offshore oil and gas ICS challenges (Mohammed et log al., 2022), and existing zero-trust research (Bobbert, 2020; Khan, 2023; Alevizos et al., 2022; Pookandy, 2021; Yao et al., 2020), we construct a conceptual model for deploying ZTA within industrial control environments. Our aim is to articulate a theoretically defensible, practical roadmap for enhancing resilience — while acknowledging and analyzing the unique constraints of ICS, including real-time control, legacy hardware, deterministic communication requirements, and human–machine interface (HMI) dependencies.

In the following sections, we first outline our methodology for synthesizing and mapping threat vectors to zero-trust controls. We then present the results of our conceptual modeling, followed by a deep discussion of implications, limitations, and future directions. We conclude with a summary and roadmap for next-phase empirical validation.

## Methodology

Given the exploratory, integrative nature of this research — aiming to bridge conceptual frameworks rather than evaluate a specific dataset — we adopted a structured literature-synthesis and conceptual mapping methodology. This methodology unfolds in three phases: (1) threat and vulnerability characterization; (2) zero-trust control taxonomy construction; (3) mapping and assessment of efficacy in ICS/offshore oil & gas context.

### Threat and Vulnerability Characterization

We conducted a systematic review of literature focusing on vulnerabilities within critical infrastructure — especially ICS — as well as documented attack patterns including ransomware and insider threats. Key sources included Makrakis et al. (2021), who surveyed a broad range of vulnerabilities and attacks targeting ICS and critical infrastructures; studies on ransomware forensic analysis in Windows-based systems (Kara & Aydos, 2021); and industry-specific risk assessments focusing on offshore oil & gas environments (Mohammed et al., 2022; Romsom, 2022). Additionally, insights from insider threat detection in IoT contexts (Kim et al., 2020) and analysis of identity management and multi-factor authentication for cloud CRM (Pookandy, 2021) enriched our understanding of attack surfaces and mitigation strategies. We also reviewed broader zero-trust literature to understand control mechanisms and their potential application in nontraditional environments (Bobbert, 2020; He et al., 2022; Khan, 2023; Emmanni, 2024; Chen et al., 2021; Mehraj & Banday, 2020; Yao et al., 2020; Alevizos et al., 2022).

In reviewing these works, we cataloged the following categories of threats: unauthorized access due to weak or stolen credentials; lateral movement after compromise; ransomware propagation; exploitation of insecure remote access; insider threats (malicious or inadvertent); attacks exploiting legacy protocols; supply chain insertion; and IoT-specific vulnerabilities such as insecure firmware and poor access control.

Zero-Trust Control Taxonomy Construction

Based on the zero-trust literature, we derived a taxonomy of control mechanisms that are central to a zero-trust model. These include: strong identity and access management (IAM) featuring multi-factor authentication and dynamic authorization (Pookandy, 2021; Yao et al., 2020); micro-segmentation and network isolation to prevent lateral movement (Bobbert, 2020); continuous monitoring and verification of device and user context; least-privilege and role-based access control; application of zero-trust in hybrid and cloud-adjacent environments (Emmanni, 2024); and decentralized trust models using blockchain to secure IoT endpoints (Chen et al., 2021; Alevizos et al., 2022). We included theoretical contributions on zero-trust definition and validation (Bobbert, 2020) alongside empirical discussions of zero-trust in sectors with strict compliance and safety requirements (Tyler & Viana, 2021; Chen et al., 2020). We also incorporated recent work specific to microservices (Kesarpu, 2025) to reflect modern software architecture trends relevant for ICS supervisory layers.

Mapping and Assessment in ICS / Offshore Oil & Gas Context

In the final phase, we conducted a conceptual mapping exercise: for each identified threat/vulnerability category, we matched applicable zero-trust controls, evaluating their theoretical efficacy and potential limitations in ICS contexts. This process required analyzing typical ICS characteristics — real-time constraints, deterministic communications, use of legacy protocols (e.g., Modbus, DNP3), limited computational resources at field devices, and sometimes intermittent connectivity (especially offshore). We also analyzed organizational and operational constraints, such as maintenance windows, physical access by engineers, vendor equipment lifecycles, and compliance/regulatory considerations.

To supplement this conceptual mapping, we performed a hypothetical scenario analysis: constructing plausible attack scenarios (e.g., ransomware propagation from compromised HMI workstation; insider exfiltration of control credentials; remote access misuse via VPN) and overlaying zero-trust controls to evaluate whether, how, and to what extent the controls would mitigate the scenario while preserving operational continuity.

Because this is a conceptual and theoretical study — not an empirical experiment or deployment report — the “Results” we present are descriptive, representing the findings of our mapping and scenario analyses rather than measured quantitative data.

## RESULTS

Our conceptual mapping and scenario analysis yielded several key findings, summarized as follows.

1. Significant Overlap between Threats and Zero-Trust Control Leverage Points

The review of threats revealed that many ICS vulnerabilities — whether from ransomware, insider threats, or remote-access misuse — stem from breakdowns in identity assurance, flat network trust models, and insufficient segmentation. For example, ransomware attacks on Windows-based control workstations or servers (common in ICS supervisory and HMI layers) often exploit weak or reused credentials, enabled remote desktop services, or open trust relationships (Kara & Aydos, 2021). Insider threats — including unauthorized privilege escalation or credential misuse — are similarly reliant on weak identity and access controls (Kim et al., 2020). Legacy ICS protocols and poorly segregated networks exacerbate these risks, allowing compromised components to affect the broader system (Makrakis et al., 2021).

Overlaying this with our zero-trust control taxonomy reveals a strong alignment: identity-focused controls (multi-factor authentication, dynamic authorization), micro-segmentation, and continuous verification directly target the root causes of many of these vulnerabilities. In other words, there is conceptual coherence in applying ZTA to ICS settings.

2. Micro-segmentation and Network Isolation Can Thwart Lateral Movement and Ransomware Spread

In our hypothetical ransomware scenario — where a compromised HMI workstation attempts to propagate malware to PLCs (programmable logic controllers) or other control servers — micro-segmentation imposes strict boundaries. By isolating each functional domain (e.g., HMI, DCS servers, historian database, remote access gateway), and enforcing communication only via clearly defined, authenticated, and authorized channels, lateral movement becomes significantly constrained. Even if ransomware executes on one segment, it cannot easily traverse to others without valid credentials and authorization.

Moreover, implementing role-based access control (RBAC) and least-privilege policies ensures that even legitimate communications between segments are minimized to what is strictly necessary, reducing the attack surface. For instance, a remote engineer accessing a maintenance console should not directly reach core control systems; instead, access could be brokered through a just-in-time (JIT) access gateway with session auditing — a pattern inherent in ZTA (Yao et al., 2020; Bobbert, 2020).

3. Identity-Centric Access and Multi-Factor Authentication Reduces Risk of Credential Theft

As many ransomware and insider-led attacks rely on stolen or reused credentials (Kara & Aydos, 2021; Kim et al., 2020), shifting to strong identity-centric authentication mechanisms dramatically reduces such risks. Implementing multi-factor authentication (MFA) at the workstation, VPN, and remote-access gateway levels creates a robust barrier against unauthorized access. Coupled with dynamic authorization (context-aware evaluations — e.g., geolocation, time-of-day, device compliance), the chance that a compromised credential will yield actionable access is significantly lowered (Pookandy, 2021; Yao et al., 2020).

In offshore oil and gas contexts, where maintenance or remote monitoring may originate from various locations — including contractors working from geographically dispersed offices — such identity controls are vital. ZTA can ensure that only authenticated, verified, and authorized users access specific ICS components, even if they originate outside traditional network perimeters.

4. Continuous Monitoring, Context Verification, and Device Trust Reduce Insider and IoT Endpoint Risks

Zero-trust models emphasize continuous evaluation of trust — not one-time authentication. By monitoring device posture (e.g., firmware integrity, patch level), user behavior (e.g., unusual command patterns or volume of data retrieval), and session context (e.g., origin, timing), ZTA can detect anomalous behavior indicative of insider threats or compromised endpoints. Research into zero-trust for IoT (Chen et al., 2021; Alevizos et al., 2022) supports the viability of combining blockchain-based device attestation with continuous verification, especially for resource-constrained devices common in ICS.

In offshore oil and gas ICS — where remote sensors, actuators, and IoT-like devices control physical processes — this capability is particularly important. An attacker inserting malicious firmware or manipulating endpoint configuration could cause physical damage or process disruptions; continuous device verification and anomalous behavior detection provide a critical defense layer.

5. Compatibility Challenges: Legacy Protocols, Real-Time Constraints, and Operational Overhead

While zero-trust controls offer substantial mitigation potential, our scenario analysis revealed serious compatibility and operational challenges when applied to ICS — and especially to offshore oil/gas environments. Many field devices (PLCs, RTUs, sensors) use legacy protocols (e.g., Modbus, DNP3) that were never designed with authentication or encryption in mind. Wrapping them into a zero-trust framework may require protocol encapsulation or gateway mediation; such gateways may introduce latency or single points of failure, which are unacceptable in real-time control contexts (Mohammed et al., 2022).

Moreover, micro-segmentation and strict access control could interfere with legitimate operational practices. For instance, field engineers performing emergency maintenance may need rapid access; imposing MFA, just-in-time authorization, or waiting for approval workflows may introduce dangerous delays. Likewise, continuous monitoring and device attestation may strain limited computational resources on edge devices or require additional infrastructure, increasing cost and complexity.

6. Organizational and Human Factors: Readiness, Governance, and Culture

Beyond technical constraints, adopting ZTA in ICS environments — especially in complex oil and gas operations — demands organizational readiness. Systems are often managed by multiple stakeholders: corporate IT, operational technology (OT) teams, third-party vendors, contractors, and on-site engineers. Creating unified identity management, defining granular access roles, and enforcing least-privilege requires governance, role definition, and cultural change. Many operators may resist perceived overhead or believe existing perimeter defenses are “good enough,” especially if they have never experienced a major breach. Training, awareness, and buy-in across teams are therefore critical; without them, even a technically robust ZTA deployment may fail in practice.

## Discussion

The results of our conceptual mapping and scenario analysis illustrate both the promise and the complexity of applying a zero-trust architecture to ICS and offshore oil & gas critical infrastructure. In the following discussion, we interpret these findings, consider counterarguments and limitations, and explore a path forward — both academically and operationally.

Interpretation: Why Zero-Trust Aligns Well with ICS Security Needs

The alignment between ICS threat vectors and zero-trust control mechanisms is conceptually strong. Traditional ICS defenses — built around segregated OT networks, air-gapping (where feasible), and perimeter firewalls — assume that the majority of threats originate outside the network. However, as documented by Makrakis et al. (2021) and Mohammed et al. (2022), many real-world attacks exploit internal trust relationships: stolen credentials, compromised vendor laptops, misconfigurations, social engineering of insiders, and exploitation of shared network segments. Zero-trust architecture flips this assumption: by default, no user or device is trusted — every access request is verified, every segment is treated as insecure, and every device is continuously evaluated.

This shift fundamentally addresses the two most dangerous phases of many ICS attacks: initial compromise and lateral movement. Even if a workstation is infected, micro-segmentation and strong IAM prevent the attacker from moving freely. Similarly, strong identity assurance and continuous verification reduce the likelihood that insiders (malicious or negligent) can misuse their access or escalate privileges. In sum, ZTA offers a defense-in-depth model tailored to modern threat realities.

Operational Feasibility and Challenges

However, theory only goes so far — operational feasibility in ICS environments presents significant challenges. The primary tension lies between security and real-time operational requirements. ICS are designed for deterministic, low-latency, high-availability operations; adding gateways, segmentation, authorization delays, or device attestation can introduce latency, complicate failover, and possibly reduce reliability. In offshore oil and gas environments — where physical safety, process stability, and environmental compliance are critical — such disruptions are not acceptable.

The problem is exacerbated by legacy equipment and proprietary protocols. Many sensors and actuators cannot support modern encryption or authentication; retrofitting may require gateway devices, which represent both points of vulnerability and potential single points of failure. These gateway devices themselves must be hardened, monitored, and redundantly provisioned, raising cost and complexity.

From an organizational perspective, implementing ZTA requires governance — defining roles/privileges, establishing identity management databases, creating approval workflows, managing lifecycle of credentials, onboarding/offboarding contractors, and training personnel. For large oil and gas operators with global supply chains, multiple vendors, and varying levels of cybersecurity maturity, this represents a substantial undertaking. Resistance may arise due to perceived costs, disruption to established workflows, or lack of cybersecurity culture.

Counterarguments and Limitations

A counterargument often raised is that zero-trust may not be necessary if perimeter defenses and network segmentation are properly maintained. Indeed, many ICS were originally designed with network-level segmentation (i.e., separate VLANs, physically separated OT environments). However, empirical evidence suggests that segmentation often degrades over time — for convenience, access shortcuts are introduced, firewalls misconfigured, VLANs collapsed after migration or expansion, and remote access systems (VPNs, remote desktop, vendor access clients) are added. These changes introduce complexity and often inadvertently create new attack vectors (Makrakis et al., 2021). In contrast, ZTA enforces a principled, identity-centric control model which remains robust even when network topology changes.

However, as previously discussed, constraints in ICS may make full ZTA deployment impractical. The need for deterministic timing, minimal latency, and high availability may conflict with ZTA components — particularly authentication, authorization, and device attestation. There is also the risk of single point of failure: if a zero-trust gateway fails, it may disrupt operations. Furthermore, given resource constraints on many field devices, continuous monitoring may be infeasible without additional hardware, which introduces maintenance overhead, costs, and possibly new vulnerabilities.

Finally, organizational challenges cannot be underestimated. Implementing ZTA effectively requires cross-functional coordination between IT, OT, operations, vendors, and contractors. For smaller operators or those with limited cybersecurity governance, this may not be achievable without significant investment, long-term commitment, or regulatory push.

Recommendations and Future Research Directions

Given the benefits and challenges, what path forward is advisable — both for practitioners (oil and gas operators, ICS administrators) and for researchers? Below we outline several recommendations and areas for future work.

1. Phased, Hybrid Deployment Approach: Rather than attempting a “big bang” ZTA rollout across all

ICS components, operators should adopt a phased approach. Start with less critical systems (e.g., corporate IT → OT interfaces, maintenance consoles, remote-access gateways), then progressively extend to more critical control layers. This reduces risk, allows gradual acclimatization, and provides early security wins.

2. Gateway-Based Wrapping of Legacy Protocols: For field devices using legacy protocols, deploy hardened gateway devices or protocol translators that mediate communications, enforce authentication, and provide encryption or encapsulation. These gateways should themselves be managed via ZTA principles: minimal trust, strict identity assurance, robust patching, redundant failover.

3. Just-in-Time (JIT) Access and Role-Based Privileges: Implement JIT access mechanisms and role-based least-privilege policies for all access — especially vendor contractors and maintenance engineers. Access should only be granted when needed, for limited time windows, and only to necessary resources. Each session should be logged, audited, and revocable in real time.

4. Continuous Monitoring, Device Attestation, and Anomaly Detection: Deploy continuous monitoring infrastructure — for device health, configuration drift, unusual traffic patterns, and behavior anomalies. For IoT and edge devices, consider using blockchain-based attestation or lightweight cryptographic verification (as suggested by Chen et al., 2021; Alevizos et al., 2022).

5. Governance, Identity Lifecycle Management, and Organizational Readiness: Build governance structures to manage identity provisioning, role assignment, credential lifecycle (onboarding/offboarding), and periodic review. Train and sensitize staff — both IT and OT — on zero-trust principles, identity hygiene, security awareness, and incident response.

6. Empirical Pilot Studies & Performance Evaluation: Researchers should collaborate with willing operators to conduct empirical pilot deployments. Such pilots should monitor not only security outcomes (reduced unauthorized access, blocked lateral movement, thwarted ransomware) but also operational metrics: latency, reliability, process interruptions, maintenance overhead, cost implications, and human factors. This empirical data will be invaluable in refining zero-trust models for ICS.

7. Design of ICS-Optimized ZTA Frameworks: There is a clear need for tailored ZTA frameworks optimized for ICS: that account for real-time constraints, legacy hardware, deterministic communications, and minimal latency. Such frameworks might include lightweight identity tokens, attestations with minimal overhead, segmented network overlays with redundant failover, and policy engines aware of process-state semantics (i.e., contextual access control that recognizes when physical process constraints preclude delays). Development of open-source reference architectures in this space could accelerate adoption.

## Conclusion

The cybersecurity landscape confronting industrial control systems — especially those underpinning offshore oil and gas critical infrastructure — is evolving rapidly. Traditional perimeter-based defenses and network segmentation are increasingly inadequate in the face of ransomware, insider threats, credential theft, and supply-chain vulnerabilities. Our conceptual analysis demonstrates that zero-trust architecture, with its core principles of identity centricity, least-privilege access, continuous verification, and micro-segmentation, aligns strongly with the security needs of modern ICS.

However, significant practical challenges remain. Legacy hardware, legacy protocols, real-time requirements, hardware resource constraints, and organizational inertia all present non-trivial obstacles. That said, by adopting a phased deployment strategy, employing hardened gateways, embracing continuous monitoring, and investing in organizational governance, operators can progressively build a resilient zero-trust posture without sacrificing operational continuity.

Moving forward, empirical pilot deployments, performance evaluations, and the development of ICS-optimized ZTA frameworks are essential. As cyber threats against critical infrastructure continue to rise, and as digital convergence deepens, embracing zero-trust may no longer be optional — but rather a vital component of resilient, secure ICS and critical infrastructure strategy.

## References

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

2. 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

3. 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

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

5. 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

6. 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.

7. 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

8. 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

9. Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 105-116.

10. Tyler, D., & Viana, T. (2021). Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences, 7499.

11. 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, 10248–10263.

**12.** Mehraj, S., & Banday, M. T. (2020). Establishing a zero trust strategy in cloud computing environment. International Conference on Computer Communication and Informatics, 1–6.

**13.** Alevizos, L., Ta, V. T., & Hashem Eiza, M. (2022). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. Security and Privacy, 191.

**14.** Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. IEEE Access, 78847–78867.

**15.** Kesarpu, S. (2025). Zero-Trust Architecture in Java Microservices. International Journal of Networks and Security, 5(01), 202–214.

**16.** Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic access control and authorization system based on zero-trust architecture. Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System, 123–127.

**17.** 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.