5. Zero-Trust model for smart manufacturing industry

Paul, B., & Rao, M. (2022). Zero-Trust model for smart manufacturing industry. *Applied Sciences*, *13*(1), 221. https://doi.org/10.3390/app13010221

1. **Transition from Perimeter-Based to Zero Trust Security Models**: The traditional perimeter-based security models in industrial environments are being challenged by the need for more dynamic security architectures to protect against emerging technologies like serverless applications, IoT, and cyber-physical systems.
2. **Adoption of Zero Trust in Response to Industry 4.0**: The fourth industrial revolution (Industry 4.0) and the rise of smart manufacturing necessitate a shift to zero-trust security models. This approach treats all networks and hosts as potentially hostile, regardless of their location.
3. **Principles, Architecture, and Implementation of Zero Trust**: The paper aims to explore and document the zero-trust approach, including its principles, architecture, and implementation procedure, especially in the context of smart manufacturing industries.
4. **Cybersecurity Challenges in Smart Manufacturing**: Smart manufacturing, characterized by IoT, Cyber-Physical Systems (CPS), and smart factories, faces significant cybersecurity challenges, necessitating robust security models like zero trust to ensure data integrity and security.
5. **Proposed Zero Trust Model for Smart Manufacturing**: The paper proposes a zero-trust model tailored for the smart manufacturing environment, addressing vulnerabilities in communication channels, data handling, and administrative access.
6. **Comprehensive Security Solutions in Zero Trust Architecture**: The proposed zero-trust architecture involves various security solutions such as micro-segmentation, device discovery, compliance management, and encryption of communication channels, aiming for complete security within the smart manufacturing context.
7. **Methodological Approach and Implementation**: The methodology involves multiple security aspects, including authentication processes, authority validation, removal of implicit trust, isolation of manufacturing phases, and secure cloud integration. This comprehensive approach aims to protect the smart manufacturing environment effectively.

The paper is structured to provide an overview of zero trust, discuss its implementation in smart manufacturing, highlight security challenges, review existing cybersecurity solutions, and

propose a comprehensive security solution, concluding with a discussion of the implications and effectiveness of this approach.