Security and Privacy

Anton Odén
Dept. of Maths and Computer Science
Karlstad University
651 88 KARLSTAD, Sweden
anton.oden@outlook.com

***Abstract*—**

I. Introduction: The Growing Need for IIoT Security

The groving interconnectivity between devices, sensors and cloud systems exposes industrial networks to various cyber security threats. Industry 4.0 goal with Internet of things connect all things create such great mass of data and datapoints being impossible by human to handle without advanced security algorithms. This article is based upon two recent articles providing insights into how technologies within big data analytics, deep learnig and edge computing can strengthen IIoT security. Discussing condidentiality, integrity, validity, authentication, access control etc.

The first paper, a ”A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities” by Bandar Alotaibi discuss key security challenges in IIoT ecosystems, highligting vulnerabilities across perception (end nodes), network and application layer. It is rich in examples being a survey of many papers and promotes implementing intrusion detection systems in edge computing locations for easier findings and blocking of maliouses software.

Second paper ”Internet of Things Security Based on Big Data and Deep Learning” by Jian-Liang Wang and Ping Chen, focuses on how deep learning techniques can enhance IoT security.

II. Security Challenges in Industrial IoT: An Overview

As industries continue to implement IoT technologies the digital transformation also exposes vulnerabilities, making security a priotity within Industrial IoT (IIoT). Unlike traditional IT infrasturcture, IIoT enviroments consist of distributed devices of which many operates in remote industrial locations. This decentralization creates a wide attack surface being more difficult to monitor and defend against cyber threats.

Many industrial machinery also rely on outdated hardware and software, originally designed with less or no modern cybersecurity considerations. These systems often lack encryption, secure authentication and patching protocols, making them easy targets. Additionally, the absence of universal security standards complicates efforts to implement consistent protection across different IIoT deployments. Security breaches aren’t all coming directly from external sources either. Insider threats, wheter intentional or accidental pose a big risk to IIoT systems. Weak access controls, improper credential managegment, and lack of employee cybersecurity awareness can lead to unauthorized access, data leaks, system failures, ransomware etc.

IIoT networks are also reliant or often integrate components from multiple vendors, introducing risks related to third-party software vulnerabilities and potential backdoor access. If a supplier experiences a security breach, attacker could use compromised informeration about that vendors devices to infiltrate industrial infractstructure.

In this artice I will

III. Types of Cyberattacks Threatening IIoT Systems

IV. Essential Security Requirements for IIoT Protection

V. The Role of AI in Industrial IoT Cybersecurity

VI. Leveraging Edge Computing for Enhanced Security

VII. Case Studies: Real-World Security Breaches in IIoT

VIII. Future Perspectives: Strengthening IIoT Defenses

IX. Conclusion: Towards a Secure IIoT Ecosystem