National Institute of Technology Rourkela

Registration Seminar

Seminar Title	: Securing Industrial IoT: Designing a Robust End-to-End Secure Gateway for Industrial Cyber-Physical Systems
Speaker	: Lopamudra Samal (Rollno : 522ec7006)
Supervisor	: Prof. Kamalakanta Mahapatra
Venue	: EC Seminar Hall (EC303), MS Team Link-https://tinyurl.com/m9kccp5c
Date and Time	: 16 May 2024 (11:00 AM)
Abstract	: The integration of Internet of Things (IoT) technologies in industrial settings has significantly transformed data acquisition and analysis processes, leading to increased efficiency and productivity. However, the inherent vulnerabilities in IoT networks, particularly concerning security and data privacy, pose significant challenges, especially in the context of industrial cyberphysical systems. The motivation behind this research stems from the critical need to address these challenges and develop a robust end-to-end secure gateway specifically tailored for industrial IoT environments. The primary motivation arises from the recognition that while IoT technologies offer unparalleled advantages in terms of data collection and real-time monitoring, they also introduce new avenues for potential cyber threats and data breaches. Traditional cloud-based analytics, while beneficial, can introduce latency issues and may not always prioritize security measures at the gateway level, leaving industrial systems vulnerable to attacks. Moreover, the authentication and encryption methods commonly employed in existing solutions may not be sufficient to meet the stringent security requirements of industrial IoT applications. The objectives of this research are multifaceted. Firstly, the aim is to design and implement an IoT gateway architecture optimized for industrial cyber-physical systems, ensuring seamless communication and data exchange between resource-constrained sensor nodes and the central cloud infrastructure. A novel device fingerprinting mechanism is proposed to enhance authentication processes, thereby bolstering the overall security posture of the system. Additionally, robust end-to-end encryption protocols are integrated into the gateway to guarantee the confidentiality and integrity of data transmitted across the network. Furthermore, the research endeavors to leverage machine learning algorithms within the gateway for real-time data analysis. This integration not only enables proactive decision making and predictive maintenance but also contributes to the overall resilience and adaptability of industrial IoT systems in dynamic operational environments. By achieving these objectives, this research seeks to advance the state-of-the-art in IoT security for industrial applications, laying a strong foundation for resilient and trustworthy cyber-physical systems within Industry 4.0 paradigms. In summary, this research addresses critical gaps in existing IoT security frameworks by focusing on authentication, encryption, and machine learning integration within an industrial IoT gateway. The ultimate goal is to enhance security, optimize performance, and facilitate seamless integration with cloud-based platforms, thereby enabling secure and efficient data management and analysis in industrial settings.