Industrial IoT

I. Introduction

**Welcome to the World of Industrial Internet of Things (IIoT)**

In today's digital age, industries around the globe are undergoing a transformative revolution driven by cutting-edge technologies. At the forefront of this revolution lies the Industrial Internet of Things (IIoT), a powerful ecosystem of interconnected devices, sensors, and software applications poised to redefine the way we work, produce, and innovate.

**IoT != IIoT**

The Internet of Things (IoT) paradigm has important applications in industrial environments. The Industrial

Internet of Things (IIoT), also known as Industry 4.0, is an emerging technology that can revolutionize manufacturing and production by using a significant number of networked embedded sensing devices and

integrating cutting-edge computing technologies [6].

IoT, or the Internet of Things, has revolutionized connectivity by linking everyday devices. Leveraging IoT principles, IIoT extends connectivity and data exchange to industrial machinery, equipment, and processes, fostering greater automation, efficiency, and insights in manufacturing plants, supply chains, and infrastructure facilities.

**Components**

IIoT encompasses a variety of key elements, including sensors, actuators, connectivity protocols, edge computing devices, and cloud platforms. These components work together to enable real-time data collection, analysis, and decision-making, empowering industries to optimize processes, predict maintenance needs, and enhance overall efficiency.

**But what is IIoT?**

The Industrial Internet of Things (IIoT) represents the convergence of industrial operations with the power of the Internet and advanced computing capabilities. It encompasses a vast network of interconnected devices, machinery, and systems embedded with sensors, actuators, and software applications that communicate and exchange data in real-time. The IIoT is a development of the distributed control system (DCS), which makes use of cloud computing to enhance and optimize the process controls, thus allowing a greater level of automation [1, 2].

**CPS (Cyber-physical systems)**

Cyber-Physical Systems (CPS) merge computational and physical processes, using hardware, software, and communication components to monitor and control the physical world in real-time. In the IIoT, CPS form the backbone, enabling connectivity and intelligence in industrial settings. By embedding smart components into physical objects, IIoT creates systems that communicate, analyze data, and make autonomous decisions, ultimately enhancing efficiency and productivity in industrial operations [1].

**Industry 4.0**

Industry 4.0, often known as the IIoT, offers manufacturing businesses tremendous financial prospects and challenges. Connectivity is the one-word summary for Industry 4.0 revolution, therefore, the ability to collect, exchange, and analyze data is made possible by this connectivity, which may lead to increases in output and efficiency as well as financial benefits [3].

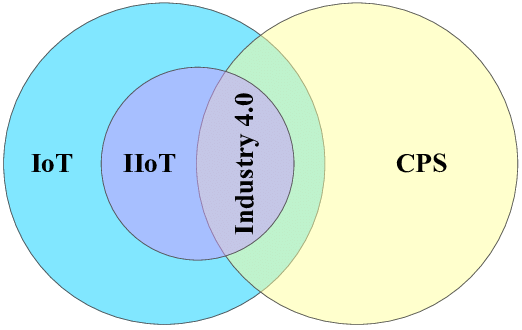


Figure 1. Intersections of IoT, IIoT, CPS, and Industry 4.0 [5]

The intersections of IoT, IIoT, CPS, and Industry 4.0 are depicted in a Venn diagram, as seen in the figure below. After identifying the main problems and possible uses of the Internet of Things (IoT) in the manufacturing sector, Yang et al. [10] came to the conclusion that the IoT envisioned the seamless integration of the real world and cyberspace and their ubiquitous presence. In addition, Wan et al. [11] presented the cyber-physical production system (CPPS), which facilitated dependable communication technology and intelligent network management tools for effective data transmission—characteristics of CPPS information interaction.

**Objectives of IIoT [4]**

* **Collection of data** related to industrial manufacturing, transport or distribution processes
* **Real-time management** of the physical resources of a productive company
* **Optimizing manufacturing processes**, material consumption, material and human resources
* **Maintenance** of manufacturing processes
* **Data security** regarding manufacturing processes
* Monitoring of **pollution factors** (emissions of CO2, SO2, nitrates, etc.)
* Support for: **smart cities, smart transport**, monitoring of environmental factors, computerized medical services (eHealth), smart administration (eGovernance), etc.
* **Sustainability and Circular Economy** - waste becomes raw material for the next manufacturing cycle

**A diagram of various types of data

Description automatically generatedIoT vs IIoT**

IoT (Internet of Things) and IIoT (Industrial Internet of Things) are both technologies that involve the interconnectivity of devices, but they have distinct applications and focuses.

IoT is centered around consumer-oriented applications and involves the networking of everyday objects, such as smart home devices and wearable technology, to collect and exchange data over the internet.

IIoT extends the concept of IoT to industrial settings, integrating IoT technologies into manufacturing, energy, transportation, and other industrial sectors. IIoT aims to optimize industrial processes, improve operational efficiency, and enhance productivity through real-time data monitoring, analysis, and automation.

In essence, while IoT targets consumer applications, IIoT is tailored specifically for industrial environments, driving advancements in manufacturing, logistics, energy, and other industrial sectors through the integration of IoT technologies.

A diagram of a system

Description automatically generatedII. IIoT Architecture

Figure . Potential IIoT architecture. [7]

There are several architecture models for IIoT systems, no general one is selected.

The typical infrastructure of an IIoT system is in the figure below:

The architecture of the Industrial Internet of Things (IIoT) typically consists of several key components that work together to enable connectivity, data exchange, and automation in industrial settings. According to the document provided:

Physical Components: This includes all physical objects within the manufacturing system, such as machines, sensors, actuators, and gateways. These components play a crucial role in industrial production processes.

Communication Methods: IIoT heavily relies on wireless protocols for data transfer between network elements. Communication methods in IIoT must meet specific requirements like low power consumption, high communication capacity, and stable interconnection. The choice of communication methods may vary based on the sector's needs.

Generalization: IIoT offers common characteristics like data collection processes, network protocols, and physical devices. Standardization in IIoT can help address challenges in scalability and heterogeneity within the industry.

Monitoring and Maintenance: IIoT enables monitoring and predicting industrial environments to establish safety procedures and alarms. By limiting human intervention, IIoT can reduce human errors and streamline maintenance processes.

Potential Architecture: The potential architecture of IIoT involves the collaboration of various components or levels to achieve the integration objectives. This architecture typically includes physical components and communication methods to support seamless workflow and efficiency in industrial processes.

These components collectively form the architecture of IIoT, enabling the implementation of advanced technologies for improved productivity and operational efficiency in industrial environments.

III. IIoT challenges

There are numerous obstacles to implementing IIoT in the industrial sector; these obstacles are mostly caused by IoT features. Problems with IIoT are not inherently different from those with IoT, depending on how IIoT and IoT are related. The most well-known IoT features are limited to low power consumption, wireless connectivity, memory capacity, and computing power limitations [7].

A diagram of a diagram

Description automatically generated with medium confidence

Figure . IIoT challenge and techniques summary [7].

1. Connectivity [7]

The Industrial Internet of Things (IIoT) faces diverse challenges, particularly regarding connectivity. These challenges include:

Performance Expectations: IIoT demands improved performance in areas like energy efficiency, reduced latency, quicker response times, and scalability. Real-time streaming is essential for time-sensitive tasks, necessitating stringent low-latency requirements.

Cloud Limitations: Despite its scalability benefits, cloud computing struggles with the growing data volume, leading to bandwidth constraints. Fog computing emerges as a solution, enabling local data processing near the data source to alleviate these constraints.

Integrated Architectures: Architectural approaches that blend IoT, fog, and cloud computing are proposed to tackle IIoT connectivity challenges effectively. These architectures aim to optimize response times by strategically deploying fog nodes within the network.

Quality of Service Management: Effective management of Quality of Service (QoS) is crucial for improving data processing efficiency and bandwidth utilization in fog computing environments. Hierarchical system structures and resource allocation strategies based on QoS criteria are employed to enhance network performance.

Optimization Using Matching Theory: Matching theory is applied to optimize resource allocation and minimize latency in fog networks. Distributed algorithms facilitate node discovery and resource allocation, leading to enhanced latency and throughput.

Deployment of Mini-Clouds: Mini-clouds are strategically placed within IoT networks to minimize data collection latency. These mini-clouds utilize shared software-defined storage solutions and algorithmic data transfer mechanisms to reduce access latency effectively.

Resource Management Strategies: Various strategies, including fog computation and tiered fog network architectures, are proposed to address connectivity issues in IoT devices. These strategies optimize resource allocation and network governance to minimize delays and improve connectivity.

Integration with 5G: The evolution of 5th generation wireless communication offers opportunities to overcome connectivity challenges in IIoT networks. 5G-enabled IoT gateways and optimized traffic classification strategies maximize uplink traffic load and leverage wireless resources efficiently.

Task Optimization: Algorithms such as graph coloring are employed to optimize heterogeneous task allocation in 5G networks. Fog nodes relay task requests to base stations for centralized resource allocation, ensuring optimal task execution within latency constraints.

2. Heterogenity [7]:

Industrial Internet of Things (IIoT) environments present unique challenges stemming from their inherent heterogeneity, characterized by diverse communication protocols, data formats, and technologies. Addressing these challenges is crucial for optimizing operations and unlocking the full potential of IIoT applications across various industrial sectors.

Semantic Interoperability: IIoT systems often comprise devices and sensors from different vendors, each employing distinct communication protocols and data formats. Semantic interoperability-based architectures offer a solution by integrating semantics into data, ensuring seamless communication and interaction among heterogeneous devices. These architectures enhance data meaning and facilitate effective data analytics, driving operational efficiency and decision-making.

Semantic Fusion Crowdsourcing: Harnessing collective wisdom from social users, semantic fusion crowdsourcing mechanisms streamline data processing in IIoT environments. By converting semantic knowledge into standardized formats and minimizing redundancy, these mechanisms enhance data consistency and integrity. Distributed storage solutions ensure reliable access to semantic data, empowering industrial applications with actionable insights.

Data Unification: IIoT ecosystems often involve disparate data sources, ranging from sensors on the factory floor to cloud-based analytics platforms. Frameworks for data unification harmonize these heterogeneous data sources, enabling seamless sharing and integration. Middleware solutions facilitate data aggregation and processing, unlocking the full potential of industrial data for predictive maintenance, process optimization, and quality control.

Attribute Identification and Retrieval: IIoT systems require efficient storage and retrieval mechanisms to manage diverse data attributes effectively. Solutions for attribute identification and retrieval analyze and classify heterogeneous data, optimizing storage and retrieval processes. By leveraging specialized databases and access control mechanisms, these solutions ensure timely access to critical industrial data, supporting real-time decision-making and operational insights.

Ontology-Based Resource Description: Describing IIoT devices and services using ontology-based models enhances resource sharing and interoperability in industrial settings. These models provide a unified view of heterogeneous sensing systems, facilitating seamless connectivity between industrial assets and cloud-based applications. Access control mechanisms ensure secure data exchange and facilitate collaboration across distributed IIoT environments.

AI and Learning Concepts: Machine learning and cognitive computing play a pivotal role in addressing IIoT heterogeneity. By applying advanced learning algorithms, IIoT systems can adapt to dynamic environments, optimize resource allocation, and improve operational efficiency. Cognitive hierarchy theory offers a promising approach for modeling complex IIoT systems, enabling adaptive decision-making and proactive maintenance strategies.

In conclusion, navigating IIoT heterogeneity requires a comprehensive approach that combines semantic interoperability, data unification, resource description models, and AI-driven learning concepts. By embracing these solutions, industrial organizations can unlock new opportunities for innovation, efficiency, and competitiveness in the digital era of manufacturing and automation.

3. Scalability [7]:

Navigating Scalability Challenges in IIoT Environments

Scalability stands as a pivotal consideration in the design of Industrial Internet of Things (IIoT) systems, ensuring they can adapt to evolving demands and grow seamlessly over time. Within the realm of IIoT, scalability encompasses two key dimensions: horizontal scalability, involving the expansion of network capabilities to accommodate increasing numbers of connected devices and software components, and vertical scalability, which pertains to the enhancement of existing resources to meet escalating performance requirements [73]. Tackling scalability challenges in IIoT necessitates strategic planning and the implementation of robust frameworks.

Protocol-Based Approaches: Protocol-based solutions are a cornerstone in managing scalability within IIoT ecosystems. For instance, the architecture proposed in [68] underscores interoperability across gateways to bolster scalability and synchronization. By leveraging protocols like MQTT and CoAP, the system optimizes communication efficiency among nodes and streamlines resource management. MQTT facilitates seamless inter-node connectivity, while CoAP servers ensure synchronization within the hierarchical tree architecture of IIoT devices.

Software-Defined Networking (SDN): SDN emerges as a potent tool for achieving scalability in IIoT environments. The solution outlined in [69] endeavors to automate device provisioning and triggering using SDN principles. Through dynamic provisioning and data transmission management, the system facilitates efficient service delivery and application provisioning, ultimately enhancing overall scalability.

Cloud and Edge Computing Integration: The integration of cloud and edge computing architectures holds promise for enhancing scalability in IIoT systems [74]. In [70], a multi-layered IIoT architecture is proposed, comprising sensor platforms, edge servers, and cloud-based systems. This layered approach empowers independent operation of sensor networks, scalable deployment of edge servers, and flexible resource allocation in cloud environments, ensuring robust scalability across all layers.

Innovative Techniques for LoRa Networks: To address scalability challenges specific to LoRa networks, [71] introduces the exponential windowing technique (EWS). This method optimizes resource allocation based on distance parameters, maximizing the success probability of packet transmissions. By leveraging principles of stochastic geometry, EWS enhances packet success rates and scalability in LoRa networks.

Application of OneM2M OCEAN Platform in Industrial Settings: In [72], the focus is on evaluating the scalability of the OneM2M OCEAN open-source platform in industrial settings. IoT devices such as multiplexers and transponders are seamlessly integrated into the network architecture, enabling scalable monitoring and management. The IoT server platform, acting as the network controller, dynamically reconfigures devices based on real-time network status information, ensuring scalability amidst the evolving demands of industrial environments.

In summary, effectively addressing scalability challenges in IIoT environments demands a holistic approach encompassing protocol optimization, network automation, cloud-edge integration, and innovative resource management techniques. By adopting scalable architectures and strategic methodologies, IIoT ecosystems can seamlessly adapt to evolving requirements and unlock their full potential across diverse industrial applications and sectors.

4. Real-Time Processing in IIoT: Addressing Data Complexity

In the realm of Industrial Internet of Things (IIoT), efficient real-time processing stands as a critical imperative given the substantial volume and complexity of generated data [86]. Conventional big data processing methods often fall short in addressing the time and location constraints, as well as the heterogeneity inherent in IIoT datasets. Enhancing real-time processing capabilities is essential for facilitating timely decision-making and feedback mechanisms within IIoT ecosystems.

Resource Discovery and Search:

The Web of Things (WoT) framework [87] emerges as a promising avenue for enhancing search and discovery functionalities within IIoT environments. Leveraging evolved cooperation among stakeholders, WoT offers a unique architecture to define IoT operations and streamline search operations [88].

DiscoWoT [75], a semantic web-based search engine, employs mapping schemes to facilitate resource discovery based on semantic definitions. By constructing internal models of entities, DiscoWoT enhances the search process and delivers relevant information to users.

Data Collection and Preparation:

Efficient data collection and preparation are vital for minimizing data transfer over the Internet and optimizing energy usage [78]. Solutions like data summarization mechanisms contribute to local data fusion, reducing the burden on cloud storage systems.

Fog-based data analytics systems [79] leverage edge computing capabilities to process data locally before transmitting it to the cloud, thereby minimizing data consumption and latency.

Scalable Architectures:

Architectures integrating distributed data storage and analysis, such as the one proposed in [80], offer scalable solutions for IIoT applications. By fusing geographically dispersed data and minimizing data transfer to the cloud, these architectures enhance response times and efficiency.

Serverless computing platforms [81] provide on-demand backend services for real-time IoT applications, enabling seamless scalability and resource optimization.

Big Data Processing and Analytics:

Advanced big data processing architectures, like the one outlined in [82], manage and analyze vast amounts of IoT data efficiently. Leveraging technologies like Hadoop and Apache Spark, these architectures enable parallel processing and real-time analytics.

Frameworks for monitoring IoT-based systems, such as the one proposed in [83], integrate real-time data processing with batch processing using Hadoop and Spark, facilitating comprehensive analytics and decision-making.

Integrated Systems:

Integrated IoT systems combining semantic approaches, cloud computing, AI, and big data analytics promise efficient context awareness and decision-making mechanisms [84]. By orchestrating data collection, semantic processing, learning, and action, these systems enable intelligent IIoT operations.

Context-aware middleware platforms [85] facilitate real-time monitoring and decision-making in IIoT devices. By integrating hardware components, cloud computing resources, network frameworks, and application entities, these platforms enable seamless data processing and analytics.

In conclusion, the evolution of real-time processing capabilities in IIoT is crucial for unlocking the full potential of industrial automation and optimization. By leveraging advanced technologies and scalable architectures, IIoT ecosystems can effectively manage and analyze vast volumes of data in real-time, driving efficiency, productivity, and innovation across industrial sectors.

5.

Enhancing Mobility in IoT Systems

Mobility is paramount in ensuring the availability and efficiency of Internet of Things (IoT) systems, operating across internet-based domains. Key mobility objectives include data aggregation, coverage expansion, accessibility enhancement, and energy node optimization [95]. As technologies advance, mobility within IoT environments experiences exponential growth, offering benefits such as load balancing, energy conservation, and reduced transmission hops. IoT mobility is classified into sensor node mobility, event mobility, and sink mobility, each addressing specific mobility challenges [95].

Innovative Solutions for IoT Mobility:

A peer-to-peer overlay network, proposed in [91], facilitates sensor and host mobility by establishing endpoints for sensors. This distributed framework ensures seamless communication between mobile peers and enables real-time information sharing.

Utilizing parallel search techniques and priority algorithms, the approach in [92] streamlines data acquisition by identifying the nearest IoT systems offering required network services. Devices are categorized and prioritized based on mobility frequency, optimizing service delivery.

Machine learning techniques, such as principal component analysis (PCA) and gated recurrent units (GRU), are leveraged in [93] to predict mobility patterns in urban environments. By analyzing Wi-Fi and cellular signals, this model enhances positioning accuracy in IoT systems.

The introduction of a Software-defined IoT framework [94] in heterogeneous urban networks revolutionizes mobility management and flow control. Through distributed controllers and regional partitions, this framework optimizes handovers, access point selection, and flow preparation, ensuring efficient IoT operations.

These innovative solutions demonstrate the diverse approaches to addressing mobility challenges in IoT systems. By leveraging peer-to-peer networks, machine learning algorithms, and software-defined frameworks, IoT environments can achieve seamless mobility, enhanced accessibility, and optimized resource utilization, paving the way for more efficient and scalable IoT deployments.

6.

Optimizing Resource Usage in IoT Environments

IoT devices are inherently resource-constrained, facing limitations in processing power, memory, and energy [102]. Efficient management of these resources is crucial for meeting the diverse demands of IoT applications, from latency-sensitive tasks to complex data analysis. Various approaches, including leveraging cloud computing and integrating machine learning at the edge, have emerged to address these resource limitations.

Innovative Solutions for Resource Management:

Cloud Computing Integration: Cloud computing offers on-demand computational resources, providing a solution to bypass or mitigate IoT device limitations. By offloading processing and storage tasks to remote cloud servers, IoT systems can overcome resource constraints [96].

Edge Machine Learning: In [97], a novel approach integrates IoT and cloud computing using lambda and middleware from CoAP. This architecture enhances IoT systems with the necessary storage, processing, and networking capabilities, enabling real-time data analysis and processing on a large scale.

Optimized Edge Computing: [98] proposes a solution to effectively utilize minimal computational resources at the edge for optimal learning performance. By processing raw data at edge nodes and training machine learning models locally, the need to transmit large volumes of data to remote cloud servers is minimized, enhancing resource efficiency.

Dynamic Resource Allocation: Machine learning strategies dynamically improve resource usage in IoT systems. In [99], an implementation scheme for online sampling intervals adjusts wireless sensor network (WSN) activity based on real-time environmental conditions, reducing unnecessary data transmissions and conserving energy.

Energy-Efficient Communication: [100] introduces a technique to minimize energy consumption by optimizing communication attempts. Leveraging reinforcement learning algorithms for flexible spectrum access reduces the need for repeated transmission attempts, thus conserving energy.

Ultra-Low-Voltage Machine Learning: In [101], energy efficiency is achieved by implementing machine learning algorithms directly on IoT devices, operating at ultra-low-voltage minimum energy levels. This approach reduces reliance on cloud resources, optimizing energy usage within IoT systems.

These innovative solutions demonstrate the diverse strategies employed to optimize resource usage in IoT environments. By integrating cloud computing, leveraging edge computing capabilities, and implementing machine learning algorithms, IoT systems can effectively manage resource constraints, enhance performance, and ensure sustainable operation.

A white sheet with black text

Description automatically generated

Figure . Resource Limitations Solutions Summary [7]

IV. Open Issues and Future Directions [7, 12]

A table of text with words

Description automatically generated with medium confidence

Figure . Summary of Future Techniques and Open Issues [7]

1. Deep Learning: Deep learning offers a powerful solution for addressing the challenges of machine learning in IIoT applications. By automatically classifying raw data features, deep learning overcomes human-defined feature limitations. Techniques like feed-forward neural networks, recurrent neural networks (including LSTM), and convolutional neural networks (CNN) form the basis of deep learning implementations. These methods enable efficient data analysis, predictive maintenance, and resource allocation in IIoT environments. Federated Learning (FL) further enhances privacy and data heterogeneity handling. However, integrating deep learning into IIoT faces performance and data processing challenges, which can be mitigated through hardware acceleration, approximate computation, and distributed algorithm computation.

2. Edge Comptuing: Edge computing revolutionizes data processing by bringing computation closer to data sources, reducing latency and enhancing efficiency. It complements cloud computing, providing real-time processing capabilities crucial for time-sensitive applications like IIoT. Edge infrastructure optimizes resource allocation and network connectivity, addressing challenges such as resource limitations and real-time processing. By moving data analytics closer to sensors, edge computing minimizes latency and optimizes data transmission. However, challenges remain, including programmability of edge devices, efficient task scheduling, data offloading, and AI model training limitations due to computational constraints. Despite these challenges, edge computing continues to play a crucial role in enhancing industrial productivity and efficiency.

3. Big Data: Big Data is a term encompassing various data processing concepts, including the aggregation of large volumes of data and the utilization of sophisticated digital tools to reveal trends in human behavior. In the context of IIoT, efficient analytic solutions are crucial across various industrial applications, requiring systems capable of managing the unique characteristics of large data sets generated by IIoT devices. Big data tools offer cost savings and time efficiency, enabling businesses to process vast amounts of data effectively and make faster decisions. Staging approaches, preprocessing methodologies, and data analytics are key components in the utilization of big data for IIoT applications. These methods help address challenges such as real-time computation and data heterogeneity, enhancing system health and defect-free component production. Future research should focus on standardizing principles for data exchange, scalability, and developing end-to-end industrial analytics pipelines capable of managing big data from multiple sources.

4. IoT and 5G: 5G serves as the standard for mobile networks, specifically engineered to provide swift data throughput and minimal latency. With the capability to sustain download speeds of up to 20 Gigabits per second and achieve sub-millisecond latency, 5G is poised to significantly impact the utilization of IIoT devices. Primarily, the advent of 5G is set to transform IIoT practices in two major ways. Initially, its high throughput and low latency facilitate real-time data sharing among devices, a feat previously restricted to private networks with high-speed connectivity. This advancement opens avenues for applications like autonomous vehicles and intelligent urban infrastructure. Moreover, the widespread adoption of 5G is anticipated to lead to a surge in the deployment of IIoT devices. Industrial operations could potentially harness thousands of 5G-connected devices, leveraging the network's rapid speed and minimal latency. Additionally, previously inaccessible remote sites may now become viable for IIoT utilization, as 5G bridges the connectivity gap that previously hindered their practicality.

6. IIoT vendors?

There are numerous vendors that offer IIoT platforms, including the following examples:

ABB Ability. ABB specializes in connectivity, software and machine intelligence.

Aveva. Acquired by Schneider Electric in early 2023, Aveva develops AI, digital transformation, IIoT and IoT edge platforms for original equipment manufacturers and end users.

Cisco IoT. Cisco offers platforms for network connectivity, connectivity management, data control and exchange as well as edge computing.

Fanuc. Fanuc combines robotics, automation and advanced analytics to provide industrial IoT offerings.

GE Predix Platform. This IIoT software platform helps connect, optimize and scale digital industrial applications.

Plataine. Plataine specializes in using AI to generate actionable insights in manufacturing.

Siemens Insights Hub. Insights Hub offers industrial IoT based on AI and advanced analytics.

IV. Security

The paper "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures" discusses the application of Industrial Internet of Things (IIoT) in high-stake manufacturing industries, the potential security threats faced by IIoT systems, various attacks possible in the layered IIoT architecture, and proposes an IIoT attack taxonomy to mitigate risks.

**Based on [13], some of the common security threats faced by industries implementing IIoT are:**

1.Denial of Service (DoS) Attacks: These attacks aim to restrict a server from serving its clients by targeting network bandwidth or services. In IIoT, DoS attacks can be more damaging, especially in cloud environments, where innocent hosts in the network (zombies) send demands, leading to service disruption.

2.Side Channel Attacks: Malicious virtual machines placed in the cloud can target the system implementation of cryptographic algorithms, posing a threat to IIoT security.

3.Cloud Malware Injection: Attackers inject malicious services or worms into virtual machines in the cloud, capable of infecting targets within the cloud system.

4.Authentication Attacks: Many cloud services still rely on simple username and password authentication, making them vulnerable to attacks. Implementing multi-factor authentication and account locking can help prevent unauthorized access.

5.Malware Attacks: Malware can be deployed within isolated OT networks, compromising the system's security. This threat is particularly concerning as OT components were not initially designed with security in mind.

6.Data Manipulation: Attackers may manipulate data in SCADA control systems, HMI, and other critical components, leading to operational disruptions and safety risks.

These threats highlight the importance of implementing robust security measures to safeguard IIoT systems in industrial environments.

**How can cyber-physical systems be vulnerable to attacks in the context of IIoT?**

Cyber-physical systems can be vulnerable to attacks in the context of IIoT due to various factors:

1. Malfunction and Breakage: Malfunctioning devices in industrial settings can have disastrous consequences. For example, the Stuxnet worm caused centrifuges to malfunction, leading to their destruction in Iranian nuclear facilities.
2. Loss of System Availability: Attacks on IIoT systems can result in the loss of system availability, causing service outages and disconnecting critical components, as seen in the cyber-attack on a Ukrainian power plant.
3. Environment Disaster: Failure of critical systems, such as leakage detection in oil and gas plants, can result in environmental disasters with far-reaching consequences.
4. Health Issues: Malfunctioning machinery, exposure to harmful chemicals, gases, or radiations due to cyber-attacks can pose health risks to individuals working in industrial environments.
5. Data Manipulation: Cyber-attacks on SCADA control systems, HMI, and operator stations can lead to data manipulation, compromising the integrity of industrial processes and potentially causing safety hazards.
6. Unauthorized Access: Vulnerabilities in distributed control systems, PLCs, gateways, sensors, motors, actuators, and other embedded devices can be exploited by attackers to gain unauthorized access, disrupt operations, or manipulate critical processes.

These vulnerabilities underscore the importance of implementing robust security measures, conducting regular security assessments, and staying vigilant against potential cyber threats in IIoT-enabled cyber-physical systems.

**Preventive measures are recommended to enhance the security of IIoT systems in industrial settings:**

To enhance the security of IIoT systems in industrial settings, the following preventive measures are recommended:

1.Implement Network Segmentation: Segregate OT and IT networks to prevent unauthorized access between critical industrial systems and enterprise networks.

2.Use Firewalls and Intrusion Detection Systems (IDS): Deploy firewalls to control access and monitor network traffic. IDS can help detect and respond to suspicious activities, including potential cyber-attacks

3.Conduct Regular Security Audits: Perform security audits and assessments to identify vulnerabilities, assess risks, and ensure compliance with security best practices.

4.Implement Multi-Factor Authentication: Enhance authentication mechanisms by implementing multi-factor authentication to strengthen access control and prevent unauthorized access.

5.Update and Patch Systems: Regularly update firmware, operating systems, and applications to address known vulnerabilities and protect against potential exploits.

6.Educate Employees: Provide cybersecurity training to employees to raise awareness about security best practices, phishing attacks, and social engineering tactics.

7.Monitor System Activity: Implement continuous monitoring of system activity to detect anomalies, unauthorized access attempts, or suspicious behavior that may indicate a security breach.

8.Encrypt Data: Use encryption to protect sensitive data in transit and at rest, ensuring that data remains secure even if intercepted by unauthorized parties.

9.Implement Access Controls: Enforce strict access controls based on the principle of least privilege to limit user access to only necessary resources and functionalities.

10.Collaborate with Security Experts: Work with cybersecurity professionals and experts to assess risks, develop security strategies, and implement effective security controls tailored to the specific needs of IIoT systems in industrial environments.

By implementing these preventive measures, industrial organizations can enhance the security posture of their IIoT systems and mitigate the risks associated with cyber threats and attacks.

V. Protocols

The following protocols are presented in [3], as used in IIoT technology:

[17, 18] IIoT key protocols: which enable seamless data exchange and control

A diagram of a computer server

Description automatically generated1. MQTT – Message Queuing Telemetry Transport

-MQTT primarily operates at the Application Layer

-is a lightweight published subscribed messaging protocol, design for remote monitoring and low bandwidth, high latency networks.

-ideal for scenarios where reliable communication and efficient data transmission are crucial.

-it is suited for applications like smart agriculture, logistics, and remote asset management.

A screen shot of a computer

Description automatically generated2. CoAP – Constrained Application Protocol

-CoAP primarily operates at the Application Layer.

-is designed for resource constraint devices and low power networks.

-it is suited for IoT scenarios with energy efficient requirements.

-it works well in environments where devices have limited processing power and memory.

-it is often used in applications like smart cities, industrial automation and home automation.

A computer screen with text and icons

Description automatically generated with medium confidence3. OPC UA – Open Platform Communications – Unified Architecture

-is an industry standard protocol for secure and reliable data exchange in industrial automation

-it focuses on providing interoperability between different systems and platforms

-it is essential in applications such as industrial control systems, manufacturing processes and SCADA systems

4. Modbus

A diagram of a computer network

Description automatically generated-is a simple and widely adopted protocol for communication between electronic devices

-it is widely used in SCADA systems process automation and industrial control applications

-it comes at different variants including Modbus RTO, serial, and Modbus TCP ethernet

-it facilitates communication between programmable logic controllers, PLCS, and other devices

5. LoRa – Long Range

A computer screen shot of a tower

Description automatically generated-is a wireless communication technology designed for long range low power applications

-it is suitable for remote sensing monitoring and control in industrial environments

-it enables long range communications while conserving battery life

Comparison:

A black and white text on a black background

Description automatically generatedA diagram of a computer network

Description automatically generated with medium confidence

VII. Implementation examples

The following ideas have been the subject of in-depth study and discussion. Technologies such as cybersecurity, cyber-physical systems, cloud computing, edge computing, cognitive computing, mobile computing, big data, artificial intelligence, 3D printing, advanced robotics, internet of things, machine-to-machine, and RFID technologies have been identified as examples of IIoT-enabled technologies. The important subject of gathering and evaluating large data is covered in about most of the literature which exists [6].

[3]:

1. Connected cars – this can also be considered an IoT technology, depends on the area we use it

Industrial IoT technologies allow vehicles to evolve by the integration of technologies that allow them to take decisions autonomously without any human intervention. This allows vehicles to communicate with many external entities in context that is now referenced as Vehicle to Everything (V2X) . V2X enables the following scenarios in vehicles:

* Vehicle-2-Vehicle (V2V)
* Vehicle-2-Infrastructure (V2I) /Infrastructure-2-Vehicle (I2V)
* Vehicle-2-Pedestrian (V2P) /Pedestrian-2-Vehicle (P2V)
* Vehicle-2-Network (V2N) /Network-2-Vehicle (N2V)
* Infrastructure-2-Network (I2N) /Network-2-Infrastructure (N2I)

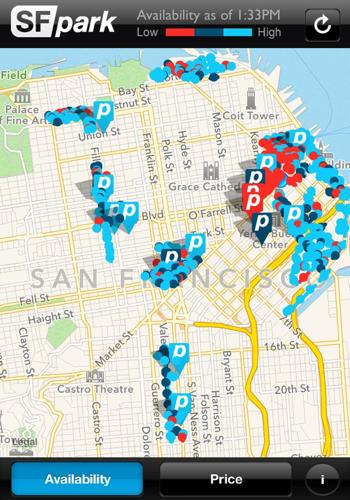
A diagram of a cloud network

Description automatically generatedThese types along with their interactions are demonstrated in figure below.

The ultimate goal of the integration would be the fleet management by each industrial manufacturer, that would allow remote diagnostics and monitoring for each factory-built vehicle. Specific use-cases for fleet-management are:

* Fault prediction based on analytics
* Remote maintenance
* Energy management.

\*Smart parking system - 30% of the traffic in a big city is generated by the big search for a parking space. 10-11 years ago, the city of San Francisco was a nightmare when it came to parking, especially in the morning. Today, they have one of the best parking systems in the world. What did they do? They installed sensors on every parking space in the city, they made an application that allows you to see the free space and reserve it, and the application routes you to the parking space, and what's more, they created a dynamic pricing model, that is, if there is a lot of traffic on the street and the demand for parking is high, the price increases, if the demand is low, the price decreases.

30% of the traffic in a big city is generated by the big search for a parking space. The city of San Francisco has significantly improved its parking management system over the past decade, addressing the challenge of traffic congestion caused by the search for parking spaces. Taking effect in April 2011, with SFpark system, by installing sensors on every parking spot and introducing a user-friendly mobile application, San Francisco allows drivers to easily find and reserve parking spaces. Additionally, the city implemented dynamic pricing, adjusting parking prices according to location, time of day, and day of the week, with the goal of keeping about 15% of spaces vacant on any given block. This innovative approach has transformed San Francisco's parking landscape, serving as a model for effective urban parking management worldwide [15].

A diagram of a business process

Description automatically generatedLearn more: [16]

To manage parking effectively, data in an up-to-date and easily usable format is required. SFpark staff along with Oracle consultants created a parking data warehouse with various data inputs.

The data warehouse enabled SFpark staff to analyze parking occupancy to make data driven pricing decisions, provide real-time parking availability information to the public, manage the city’s on-street spaces, and monitor the performance of the meter, sensor, and garage vendors. It not only stored, but also normalized incoming data, addressing any inconsistencies. The data were used not only for collecting and analyzing parking occupancy rates but also for enforcement management decisions and general parking management agency-wide.

The system diagram below outlines the relationship between the data sources, and end user. There are sensors, meters, and garages that collect and send data to their respective external management systems (operated by the vendor of each product or service), which were then sent to the SFMTA’s internal data hub. The SFMTA’s SFpark data management system then made that data ready to be stored in the operational data store, which both pushed out a real-time data feed as well as stored the data for later use by business analysts.

\*\*\*\*Sensor Technology: SFpark utilized in-ground magnetic sensors installed in parking spaces. These sensors could detect changes in the Earth's magnetic field caused by the presence or absence of a vehicle. They provided real-time occupancy information about parking spaces.

Energy Source: The sensor technology used in SFpark relied on battery power for operation. The specific type of battery or energy source used may vary based on the sensor model employed.

Accuracy: The sensor technology used in SFpark generally had high accuracy in detecting vehicle occupancy. The reported accuracy was typically above 95%, but specific accuracy rates may depend on the sensor model and implementation.

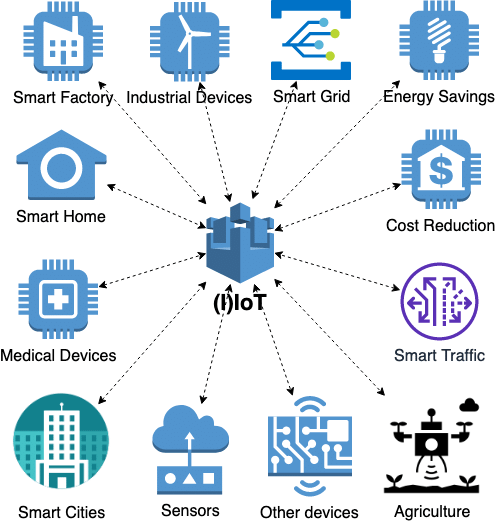
Communication Protocols: The sensor data was transmitted wirelessly using various communication protocols. The exact protocols used may include technologies such as Zigbee, Bluetooth, or other wireless communication standards.

Data Storage: The collected parking occupancy data was stored and managed in a centralized system. The SFpark program likely utilized a database or data storage infrastructure to retain and process the collected data.

Data Analysis: The collected parking data was analyzed to gain insights into parking patterns, occupancy rates, and pricing effectiveness. Data analysis techniques, such as statistical analysis and data mining, may have been employed to extract meaningful information.

Integration with Other Systems: SFpark's technical infrastructure likely integrated with other systems and platforms. This includes the integration of parking data with mapping systems, mobile applications, and online tools to provide real-time parking availability information to drivers.

Data Privacy and Security: SFpark would have taken measures to ensure the privacy and security of the collected data. This may include encryption protocols, access controls, and adherence to relevant data protection regulations.

-----------------------------------------------------------------------------------------------------------------------------

Manufacturing: Businesses can automate and increase the operational efficiency of their manufacturing processes.

Oil and gas: Companies improve productivity and reduce risks by proactively identifying threats.

Energy: Organizations use IIoT to lower costs, enhance worker and plant safety, and improve reliability.

Agriculture: Farming businesses strive to adopt smart farming by collecting data and extracting meaningful insights to enhance productivity.

Construction: Companies leverage the technology to collect construction-related data, improve project delivery time, and centralize site monitoring.

Automotive: IIoT solutions aid organizations in creating safer and more efficient smart vehicles.

Healthcare: Hospitals and clinics utilize technology to gather real-time patient health data, automate operations, and minimize human error.

**Real-life Business Examples of IIoT Applications:**

**Airbus: Smart Factory [19]**

Airbus is a leading manufacturer of aircraft and a pioneer of innovation. Assembling millions of components without making a single mistake is a tough undertaking, especially considering the cost of such a mistake. In pursuit of minimizing errors and optimizing the assembly process, the company launched what they call the Factory of the Future. They installed sensors in the machines and workers’ uniforms to increase safety and reduce errors. For example, Airbus offers smart glasses that allow employees to decipher complex blueprints and convert measurements from imperial into metric.

To say that assembling a commercial jetliner is an elaborate affair would be an understatement. Such craft have millions of components and tens of thousands of assembly steps, and the cost of mistakes during the process can be enormous. To tackle the complexity, Airbus has launched a digital manufacturing initiative known as Factory of the Future to streamline operations and bolster production capacity. The company has integrated sensors to tools and machines on the shop floor and given workers wearable technology — including industrial smart glasses — designed to reduce errors and bolster safety in the workplace. In one procedure, known as cabin-seat marking, the wearables enabled a 500% improvement in productivity while nearly eliminating errors.

Airbus, a renowned German company, has embraced cutting-edge IIoT technologies, positioning itself as a key player in the aviation industry. As a leading European aircraft manufacturer, Airbus incorporates various IoT technologies throughout its production processes. This allows for the extensive collection of data during manufacturing on the plant floor and even after the deployment of products in actual aircraft. Additionally, valuable data can be gathered from flight recorders while flights are in operation. The accumulation of flight data contributes to improving the in-flight experience, while workers on the factory floor utilize IoT devices to track manufacturing progress, identify gaps, and enhance overall efficiency. Airbus spearheads the digital manufacturing initiative known as the Factory of the Future, shaping the path for advanced manufacturing practices.

Within the Factory of the Future, Airbus focuses on diverse components, including IoT sensors for supply chain management. The implementation encompasses modular equipment, robotics, robotic arms, and concepts like industrial augmented reality, computer vision, real-time image processing, and video processing. Airbus has established mechanisms for digital tracking and monitoring by integrating sensors into tools, machines, and wearable devices like smart glasses with augmented reality support. By leveraging these technologies, Airbus achieves 3D real-time visualization of the production process. These advancements have been deployed in the assembly lines of A330 and A350 models at the Toulouse manufacturing plant, as well as in the assembly operations for the A400M model in the UK.

**Amazon: Reinventing warehousing [20]**

The online retail giant doesn’t often get called an IIoT company, but, to be sure, the company is an innovator when it comes to warehousing and logistics. As MIT Technology Review has put it:

Amazon is “testing the limits of automation and human-machine collaboration.” While the company’s ambitions to use drones for delivery has won considerable media attention, the firm’s fulfillment warehouses make use of armies of Wi-Fi-connected Kiva robots. The basic idea behind the Kiva technology, which Amazon acquired for $775 million in 2012, is that it makes more sense to have robots locate shelves of products and bring them to workers rather than have employees go to the shelves to hunt for products. In 2014, the robots helped the company cut its operating costs by 20%, according to Dave Clark, a senior vice president at Amazon.

Robotic Shelves: Amazon has robotic shelves, and as this name suggests, Amazon uses different types of robots that will carry these shelves and rearrange them. Amazon basically is an e-commerce company and these shelves and their rearrangement robotically are very important and that makes the processes much more autonomous and efficient. So, the good part of this thing is that because it is an autonomous robotic system, using this system, the robots can efficiently locate and search different items from different shelves. Thus, in 2014, the operating cost was cut down by 20% using these robotic shelves by Amazon.

**ABB – Smart Robotics [20]**

Power and robotics firm ABB is one of the most visible to embrace the concept of predictive maintenance, using connected sensors to monitor its robots’ maintenance needs — across five continents — and trigger repair before parts break. Also related to IoT is the company’s collaborative robotics. Its YuMi model, which was designed to collaborate alongside humans, can accept input via Ethernet and industrial protocols like Profibus and DeviceNet.

**Caterpillar: Augmented Reality App [19]**

Caterpillar has the augmented reality (AR) app which is integrated with IoT; Caterpillar is a heavy equipment maker, and it has come up with the augmented reality app that generates end-to-end view of the factory floor. So, the machine operators can detect the need for tool replacement whenever it is required after viewing the end-to-end view through that particular AR app. This app sends instructions for doing things like tool replacement, air filter change, and fuel monitoring.

Caterpillar has the IoT-driven ship maintenance that is done by their marine division. They use the shipboard sensors to perform predictive maintenance analytics. The sensors that are deployed can monitor generators, engines, GPS, air-conditioning systems, and fuel meters. The analysis of the sensed data provides useful insights with respect to the power usage of refrigerated containers, cost of hull cleaning, and optimized cleaning schedule and their data; these are all provided through the analysis of the data that are obtained through these different sensors that are deployed in the onboard devices of the ships.

So, preventive maintenance analytics talks about the use of all these machine learning techniques. Tools and techniques like Python and Weka could be used to come up with these different predictive analytics and so on. It is used to have easier fault correction, reduced downtime, and increased profitability, using predictive maintenance analytics, and this is what Caterpillar is doing.

Bibliography:

1. Boyes, Hugh; Hallaq, Bil; Cunningham, Joe; Watson, Tim (October 2018). "The industrial internet of things (IIoT): An analysis framework". Computers in Industry. 101: 1–12. doi:10.1016/j.compind.2018.04.015. ISSN 0166-3615.
2. Brauner, Philipp; Dalibor, Manuela; Jarke, Matthias; Kunze, Ike; Koren, István; Lakemeyer, Gerhard; Liebenberg, Martin; Michael, Judith; Pennekamp, Jan; Quix, Christoph; Rumpe, Bernhard (2022-02-15). "A Computer Science Perspective on Digital Transformation in Production". ACM Transactions on Internet of Things. 3 (2): 15:1–15:32. doi:10.1145/3502265. ISSN 2691-1914. S2CID 246883126.
3. Sari, A., Lekidis, A., Butun, I. (2020). Industrial Networks and IIoT: Now and Future Trends. In: Butun, I. (eds) Industrial IoT . Springer, Cham. <https://doi.org/10.1007/978-3-030-42500-5_1>.
4. Curs\_infoind\_m\_2\_IoT\_IIoT\_cyber\_systems, UTCN
5. Lee, C. & Huo, Yunzhang & Zhang, Shuzhu & Ng, Kam K.H.. (2020). Design of a Smart Manufacturing System With the Application of Multi-Access Edge Computing and Blockchain Technology. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2972284
6. Peter, Onu, Anup Pradhan, and Charles Mbohwa. "Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies." Procedia Computer Science 217 (2023): 856-865.
7. Alabadi, Montdher, Adib Habbal, and Xian Wei. "Industrial internet of things: Requirements, architecture, challenges, and future research directions." IEEE Access 10 (2022): 66374-66400.
8. Jaidka, Himanshu, Nikhil Sharma, and Rajinder Singh. "Evolution of iot to iiot: Applications & challenges." Proceedings of the international conference on innovative computing & communications (ICICC). 2020.
9. Schneider, Stan. "The industrial internet of things (iiot) applications and taxonomy." Internet of Things and Data Analytics Handbook (2017): 41-81.
10. C. Yang, W. Shen, and X. Wang, "The Internet of Things in Manufacturing: Key Issues and Potential Applications," IEEE Systems, Man, and Cybernetics Magazine, vol. 4, no. 1, pp. 6-15, 2018.
11. J. Wan et al., "Toward Dynamic Resources Management for IoT-Based Manufacturing," IEEE Communications Magazine, vol. 56, no. 2, pp. 52-59, 2018.
12. TechTarget. "What is IIoT (Industrial Internet of Things)? | Definition from TechTarget." IoT Agenda. Accessed March 30, 2024. URL: <https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT>.
13. Panchal, Abhijeet C., Vijay M. Khadse, and Parikshit N. Mahalle. "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures." 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). IEEE, 2018.
14. Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., Sinopoli, B.: Cyber-physical security of a smart grid infrastructure. Proc. IEEE 100(1), 195–209 (2011).
15. Wikipedia contributors. "SFpark." Wikipedia, The Free Encyclopedia. Retrieved November 16, 2023, from <https://en.wikipedia.org/wiki/SFpark>.
16. SFpark Technical Manual: Guide to the Information Technology behind SFpark, Author(s): San Francisco Municipal Transportation Agency (SFMTA), Publication Date: June 2014 URL: <https://www.sfmta.com/sites/default/files/reports-and-documents/2018/05/sfpark_tech_manual_web.pdf>
17. Exploring the Ins and Outs of Industrial Protocols for Industrial IoT, Website: Softobotics, URL: <https://www.softobotics.com/blogs/exploring-the-ins-and-outs-of-industrial-protocols-for-industrial-iot/>
18. Jaloudi, Samer. "Communication protocols of an industrial internet of things environment: A comparative study." Future Internet 11.3 (2019): 66.
19. Grover, Jyotsana. "Industrial IoT and Its Applications." IoT for Sustainable Smart Cities and Society. Cham: Springer International Publishing, 2022. 107-124.
20. "IoT World Today: The Top 20 Industrial IoT Applications." IoT World Today. Retrieved from <https://www.iotworldtoday.com/iiot/the-top-20-industrial-iot-applications#close-modal>