

# IoT for Industrial Automation: A Review on Industry 4.0 Applications

## **Rafiul R. Zahid**

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: 2001004@iot.uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0005-4298-7805>

## **Rakibul H. Rakib**

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: 2001007@iot.uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0002-7185-1737>

## **Iftekhhar Rahman**

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: 2001012@iot.uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0006-1085-0203>

## **Md. A. Amin**

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: 1901027@iot.uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0001-6547-9185>

## **Tanjum R. Akanto**

Department of Electrical and Electronic Engineering, Daffodil International University, Dhaka, 1216, Bangladesh  
E-mail: tanjumrahiakanto.eee@diu.edu.bd  
ORCID iD: <https://orcid.org/0009-0001-6708-6166>

## **Fahmida A. Antara**

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: fahmida0001@uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0003-0005-1510>

## **Sadia Enam\***

Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh  
E-mail: sadia0001@uftb.ac.bd  
ORCID iD: <https://orcid.org/0009-0001-3424-8042>  
\*Corresponding Author

Received: 30 September, 2025; Revised: 18 December, 2025; Accepted: 02 February, 2026; Published: 08 April, 2026

**Abstract:** The beginning of the fourth industrial revolution or Industry 4.0 has changed the concept of automation in industries by adopting the Internet of Things (IoT) in manufacturing, logistics, and production processes. The IoT is the digital foundation of Industry 4.0 that allows real-time monitoring, predictive maintenance, data-based decision making, and autonomous processes with in-between devices and smart sensors. This review explores the uses of the IoT in industrial automation through analyzing the enabling technologies, communication protocols, integration with cloud computing, wireless sensor networks, edge computing, artificial intelligence (AI) and machine learning (ML), as well as

presenting important applications, current challenges, and future trends in smart industrial systems. Instead of considering the technologies separately, this paper takes the system-level viewpoint by integrating the way IoT architecture, communication protocol, intelligent analytics, and security controls collectively facilitate Industry 4.0 automation.

**Index Terms:** Industry 4.0, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Industrial Automation, Smart Manufacturing, Cloud Computing

## 1. Introduction

The broad adoption of the Internet of Things (IoT) and its industrial counterpart, the Industrial Internet of Things (IIoT), changes face of the manufacturing landscape. This combination of machines and data is what Industry 4.0 is based on and it is a clear indication of the fact that machines, data, and people are linking up via smart systems [1,2]. The advancement of industrial devices makes IoT achieve real-time sensing, autonomous control and remote monitoring. This improves predictive and preventive maintenance of objects in Operational Technology that spans a broad spectrum of industrial assets across such industries as the manufacturing or energy and transportation sectors, as well as healthcare. Connected devices and analytics can be used by smart factories to boost productivity, quality, and responsiveness to a significant degree [3,4]. Industrial automation has significantly improved production efficiency, product quality, and cost effectiveness in the era of Industry 4.0 by reducing human error and enhancing precision and speed in manufacturing tasks [5].

However, to make the potential of Industry 4.0 complete, we should address the issue of data integration, interoperability, and communication between various systems. The industrial environments are normally comprised of aged machines, tied platforms and the incommensurate protocols. Architectural frameworks and middleware solutions have been proposed to secure connections between operational technologies by researchers [6, 7]. The unification of the protocols by use of technologies such as MQTT, CoAP, LoRaWAN and OPC UA has been promising and aids in enhancing data communications within the devices that have varying abilities. These standardized communication techniques facilitate easy real time monitoring and control which is important in high demand industrial installations such as energy grids and manufacturing lines [6].

In addition to connectivity, artificial intelligence (AI) and machine learning (ML) play an important role in enhanced industrial automation. Technologies that enable the big data collection, processing and analysis are able to translate into the construction of predictive models through the sensors, actuators, and production systems. Such models can diagnose equipment failure, streamline resource utilization, and suggest measures prior to failure [8, 9]. For example, it is possible to connect the Machine Learning algorithms and the SCADA systems to introduce the ability to optimize the working parameters in real-time, which will improve the efficiency of the systems and reduce the time of system downtimes [10, 11]. Industries are moving away towards predictive maintenance as real-time feedback loops supported by AI. Regardless of these benefits in technology, security stands out as a major challenge to the large-scale use of IIoT. The industrial systems are more vulnerable to cyber threats because they have a bigger digital footprint. The security lapses, such as insecure communication channels, outmoded equipment, and so on, may have a serious negative effect on the continuity of operations and safety [12,13]. Researchers focus on the need of securing authentication and access control of industrial devices and encryption. In addition, blockchain solutions are also investigated in order to increase transparency, data integrity and traceability in industrial communication networks as well as, offer the opportunity of decentralized and tamper-free systems to share data and carry out transactions securely. Besides these developments, the coming up with wireless sensor network (WSN) and low-power communication is essential in the scalability of the IIoT. WSNs facilitate the prolific use of sensing nodes to track the environmental conditions, machine conditions as well as energy consumption [14]. Recent standards such as cognitive radio and Low Power Wide Area Networks (LPWANs) are highly scalable and can adapt to spectrum constraints, and thus are a good fit to complex industrial systems [15]. These technologies decrease the cost of infrastructure and the life of battery-operated devices besides satisfying the real-time communication requirements. Time critical tasks also demand high reliability and low latency communication in industrial automation. BLE has potential to fulfill these requirements in IIoT-based applications [16].

Lastly, the adaptation of such technologies in a dynamic industrial environment is more difficult. These are to optimize the network design, guarantee reliability of the data, guarantee that all the distributed systems are in synchronization, and combine with the older legacy systems that are not designed to support the IoT [17]. Addressing these issues is essential for creating a scalable, and efficient smart manufacturing ecosystem.

In this paper, we present a review of the latest advancements, technical challenges, and future trends in IoT-enabled industrial automation. We focus on architectural design, communication technologies, intelligent analytics, and strong security measures to facilitate the shift toward fully autonomous and intelligent industrial environments. Overall, a contribution matrix is presented in Table 1. The contribution matrix was built through explicit coverage of themes in each of the studies. A checkmark means that the specific topic was in the top priority or was touched upon substantially.

Table 1. Contribution Mapping of Core Industry 4.0 Application

| Ref. | Study                             | IoT Architecture | Communication Protocols | Machine Learning | Security and Privacy | Wireless Sensor Network | Future Trends |
|------|-----------------------------------|------------------|-------------------------|------------------|----------------------|-------------------------|---------------|
| [1]  | F. Qiu et al., 2025               | ✓                | ✓                       | ✓                | ✓                    | ✓                       | ✓             |
| [2]  | Lampropoulos et al., 2019         | ✓                |                         | ✓                |                      |                         |               |
| [3]  | M. Soori et al., 2023             |                  | ✓                       |                  |                      |                         | ✓             |
| [4]  | P. Nirmala et al., 2022           | ✓                |                         |                  |                      |                         |               |
| [5]  | V. S. Gurav et al., 2024          |                  | ✓                       |                  |                      |                         | ✓             |
| [6]  | S. Gil et al., 2022               | ✓                | ✓                       |                  |                      |                         |               |
| [7]  | T. Lennvall et al., 2017          | ✓                |                         |                  |                      |                         |               |
| [8]  | S. K. Pandey et al., 2022         |                  |                         | ✓                |                      |                         | ✓             |
| [9]  | P. Visconti et al., 2024          | ✓                | ✓                       | ✓                |                      |                         |               |
| [10] | Babayigit & Abubaker, 2024        | ✓                | ✓                       |                  |                      |                         |               |
| [11] | A. Deshpande et al., 2016         | ✓                |                         |                  |                      |                         |               |
| [12] | Kamran Shaukat et al., 2021       |                  |                         |                  | ✓                    |                         | ✓             |
| [13] | T. Alladi et al., 2019            |                  |                         |                  | ✓                    |                         |               |
| [14] | M. Majid et al., 2022             | ✓                | ✓                       | ✓                | ✓                    | ✓                       | ✓             |
| [15] | Nurelmadina et al., 2021          | ✓                | ✓                       |                  |                      |                         |               |
| [16] | Rondon et al., 2017               |                  | ✓                       |                  |                      | ✓                       |               |
| [17] | H. S. Chandu, 2024                | ✓                |                         | ✓                | ✓                    |                         | ✓             |
| [18] | Rao & Chandrakanth, 2021          |                  |                         | ✓                |                      |                         | ✓             |
| [19] | M. Williams et al., 2024          |                  |                         |                  | ✓                    |                         |               |
| [20] | N. Yadav et al., 2024             |                  |                         |                  |                      |                         |               |
| [21] | J. Ansari et al., 2022            |                  | ✓                       |                  |                      |                         |               |
| [22] | B. Kaur et al., 2023              |                  |                         |                  | ✓                    |                         |               |
| [23] | M. Sujatha et al., 2022           |                  |                         | ✓                |                      |                         | ✓             |
| [24] | A. Enemosah & O. G. Ifeanyi, 2025 | ✓                |                         |                  | ✓                    |                         |               |
| [25] | R. F. Muniz et al., 2023          |                  |                         | ✓                |                      | ✓                       | ✓             |
| [26] | I. Behnke et al., 2023            |                  | ✓                       | ✓                |                      |                         | ✓             |
| [27] | L. D. Nguyen et al., 2020         |                  |                         | ✓                |                      |                         | ✓             |
| [28] | R. A. Khalil et al., 2021         |                  |                         | ✓                |                      |                         | ✓             |
| [29] | Adam and Baroudi., 2024           |                  |                         | ✓                |                      |                         | ✓             |
| [30] | F. A. Hussein et al., 2025        | ✓                | ✓                       |                  |                      |                         | ✓             |
| [31] | T. Zhukabayeva et al., 2023       | ✓                | ✓                       | ✓                | ✓                    |                         | ✓             |

Here, papers are check marked under IoT Architecture when they either suggest or discuss system-layer designs, reference models, or architectural frameworks of industrial IoT environments [1,17,24]. Articles are indicated under communication protocol which discussed numerous network protocols and connectivity options. Out of these, MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) were mentioned in [1,10,17], communication-layer and network-level architecture enabled by cognitive radio and LPWAN was discussed in [15]. The Machine Learning column features publications that incorporate data-driven models to predict, classify, or optimize processes in Industry 4.0, among which are fault detection and process optimization [1,4]. The security and privacy column highlights the security issues with distributed and resource-constrained systems: data confidentiality, data integrity, data authentication, data availability, and data privacy. The main concerns include obtaining data provenance, access control, denial-of-service attacks, service integrity and vulnerabilities at physical, network, middle, and application levels. The constraints on hardware and software like limited energy, memory, computing power, dynamic network properties and vulnerability to tampering, replay, and intrusion attacks were also discussed in [1,13, 14,19,22], [24,31]. Researches are included under WSN while they covered the usage of WSN and the Internet of Things (IoT) in Industry 4.0 with particular emphasis on the network security, threats, and research issues. These not only focused on the discussion of security attacks, intrusions, weaknesses and constraints to industrial systems based on IoT and WSN, but also discussed the role of automation, smart applications, and industrial data communication [1,13,25]. Most of the analyzed articles are dedicated to upcoming developments in the sphere IIoT, which indicates the fast dynamism of the sphere and it's prospective to change smart factories. Some new directions that these studies discuss include the adoption of digital twins in conjunction with AI and edge computing, real-time predictive maintenance, dynamic production scheduling, and autonomous decision-making.

Additionally, the responses of the following research questions are discussed based on the analysis of review papers that are selected for this study.

- **RQ1.** How do IoT and Industrial IoT transform traditional industrial automation into decentralized intelligent systems?
- **RQ2.** What challenges hinder the implementation of IoT-driven automation in Industry 4.0?

- RQ3. What IoT innovations will drive the future of intelligent automation in Industry 4.0?

Addressing these questions will help develop a scalable, efficient, and secure smart manufacturing ecosystem. The remainder of this paper is organized as follows: A total methodology of this study in section 3. Section 4 provides the background and evolution of industrial IoT. Again, the key characteristics are discussed in Section 5. Section 6 discusses IoT frameworks and architectures. Section 7 examines communication protocols. Section 8 presents data integration and interoperability. Section 9 covers the role of machine learning in smart automation. Section 10 presents wireless sensor networks and low-power connectivity technologies. Section 11 outlines security and privacy concerns. Section 12 highlights current limitations and ongoing research issues. Section 13 discusses emerging trends, and section 14 answers the research questions those arrived with the research has started, section 15 discusses the whole study. Finally, Section 16 concludes the paper.

## 2. Foundations and Motivation for Smart Industry

### 2.1 Importance of IoT/IIoT in Industry 4.0

Industry 4.0 is the fourth industrial revolution that brings significant transformations in the field of manufacturing and industrial operations. The transformation is due to the incorporation of the Internet of Things (IoT), Industrial Internet of Things (IIoT), cyber-physical systems, and data analytics. These technologies enable real-time data transfers and automation and ease of control throughout the production [1, 2]. Smart factories have a digital nervous system in IoT and Industrial IoT. They link sensors, machines and cloud platforms to ensure productivity, quality, and agility [3, 4]. The transition to IoT-enabled structures is a big move to complete autonomy in the industrial settings that were previously done in the traditional SCADA system [10].

### 2.2 Motivation for Smart Automation

Conventional automation systems tend to be hard, disconnected and require human control. This restricts their scalability and flexibility to adaptation in changing industrial environments. These issues are solved by intelligent automation that is powered by IoT and machine learning. It implements adaptable, data-oriented models that are able to self-monitor and adjust to evolving circumstances [8, 9]. The increasing demands to have energy-efficient, cost-effective and real-time industrial processes necessitate the implementation of intelligent automation technologies. Additionally, the need to have resilient manufacturing systems, which can be operated remotely, is reinforced by the global disruptions like pandemics and supply chain challenges [11, 17].

### 2.3 Scope and Objectives of the Review

This review paper dwells on the convergence of IoT, Industrial IoT and intelligent systems in industrial automation. Consequently, instead of being introduced as independent technological surveys, issues are debated in an integrative manner. It aims:

- To present an overview of IoT architectures, protocols, and frameworks used in Industry 4.0.
- To examine the role of AI and machine learning in predictive maintenance and decision-making.
- To discuss security and privacy challenges that are unique to industrial IoT environments.
- To analyze wireless communication technologies like WSNs, cognitive radio, and LPWANs in industrial settings.

## 3. Methodology

The review was carried out according to the PRISMA 2020 guidelines so as to have transparency and reproducibility, which is presented in Figure 1.

### 3.1 Search Strategy

The systematic review was done under the PRISMA 2020 guidelines. An extensive literature search of five large electronic databases was done: IEEE Xplore, ScienceDirect, Springer, ACM Digital Library and Google Scholar. The search encompassed the publications in the period between January 2015 and March 2025, which indicates the emergence and development of Industry 4.0 and Industrial IoT study.

The search strategy employed structured Boolean query logic combining core concepts related to IoT-enabled industrial systems, Industry 4.0 technologies, and associated enabling domains. The primary search string was defined as:

“Internet of Things” OR “Industrial Internet of Things” OR “IoT” OR “Industrial IoT”) AND (“Industry 4.0” OR “Smart Manufacturing” OR “Industrial Automation”) AND (“architecture” OR “communication protocols” OR “machine learning” OR “security” OR “privacy” OR “wireless sensor networks”)

The query syntax was also modified to suit the particular requirements of this study. Only Peer-reviewed journal articles and conference papers published in English were taken into account. Using this strategy, a total of 600 records were initially identified, including 100 from IEEE Xplore, 100 from ScienceDirect, 100 from Springer, 100 from ACM Digital Library, and 200 from Google Scholar.

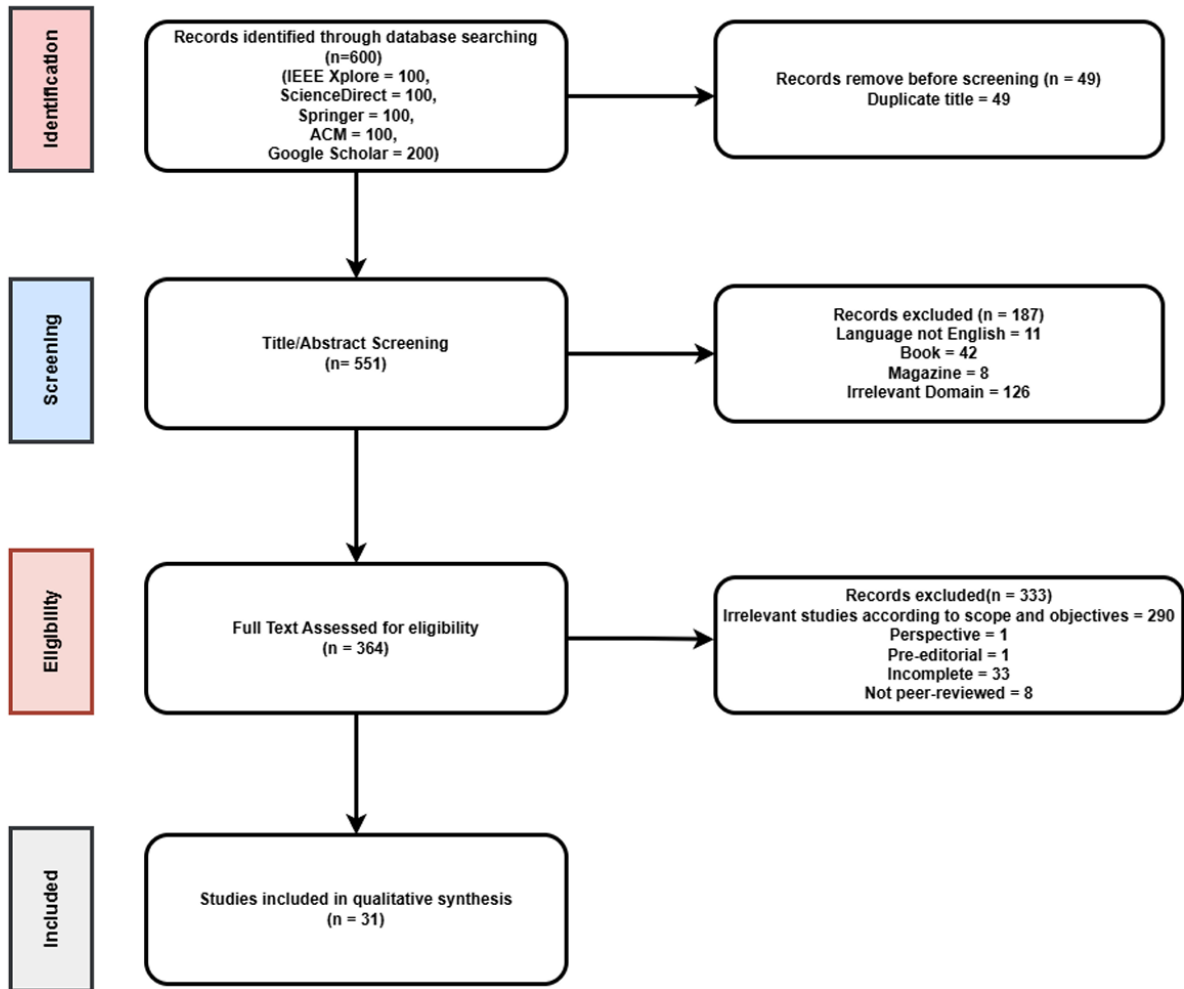


Fig. 1. Paper selection process using PRISMA guideline.

### 3.2 Inclusion and Exclusion Criteria

The inclusion criteria defined the conditions that studies must satisfy to be considered relevant and eligible for this research.

- Peer-reviewed journal and conference articles.
- Articles published in the English language.
- Studies directly related to the application of Internet of Things (IoT) and Industry 4.0.
- Research works aligned with the objectives and scope of the present study.

The exclusion criteria defined the factors according to which the studies have been excluded in order to preserve the quality and relevance of the selected literature.

- Non-English language publications.
- Books, magazines, and non-peer-reviewed sources.
- Duplicate records across multiple databases.
- Incomplete articles and pre-editorial content.
- Studies not relevant to the domain of IoT and Industry 4.0.

### 3.3 Screening

Screenings were carried out by first eliminating all records that were duplicated (49). The other 551 records were rated on the title and abstract levels. Among them, 187 were excluded, and they included non-English articles (11), books (42), magazines (8), and irrelevant studies in the domain of study (126).

### 3.4 Eligibility Assessment

A total of 364 articles were subjected to full-text assessment. After applying the eligibility criteria, 333 articles were excluded, including irrelevant studies with respect to the scope and objectives (289), perspective papers (1), pre-editorials (1), incomplete studies (33), and non-peer-reviewed works (8).

### 3.5 Final Selection

Lastly, 31 studies were included in the qualitative synthesis since they met all the inclusion criteria. This systematic and strict method helped to ensure that the review contained only the high-quality, relevant literature, and peer-reviewed literature to bring a complete picture in terms of research involving IoT, industrial automation and Industry 4.0.

### 3.6 Quality Assessment of Selected Study

This is a systematic review of primary research articles and high impact review articles. To create background context, summarize existing knowledge, determine current research trends, and define gaps in the research, a large amount of review articles was used. This is indicative of the field with a huge percentage of the contributions being on surveys, reference architectures and conceptual frameworks.

The quality of methodology of included primary studies was subsequently assessed with Mixed Methods Appraisal Tool (MMAT) [32]. Since no original empirical data is reported in review and survey paper, they were not evaluated through MMAT. Two screening questions were initially used to screen out all candidate studies:

- Are the research questions clearly stated in the studies?
- Are the collected data adequate to answer those research questions?

Primary studies that met both screening questions were only included to evaluate them on the quality of methods of study. There were four MMAT criteria, which are summarized in Table 2. Each of the criteria was rated in Yes, No, or Can't tell.

Intake of MMAT was followed and studies which met at least three of four criteria were considered as high quality and those which met two criteria were considered as moderate quality whereas those which met one criterion or less criteria were considered as low quality. The authors independently conducted quality assessment, and disagreement was overcome by discussing it. The synthesis was carried out using only high- and moderate-quality studies.

Table 2. Quality Classifier Criteria (According to MMAT)

| SL No. | Criteria                                                                                      | Response to the criteria |
|--------|-----------------------------------------------------------------------------------------------|--------------------------|
| 1      | Are measurements appropriate regarding both the outcome and intervention (or exposure)?       | Yes / Can't tell / No    |
| 2      | Are there complete outcome data?                                                              | Yes / Can't tell / No    |
| 3      | Are the confounders accounted for in the design and analysis?                                 | Yes / Can't tell / No    |
| 4      | During the study period, is the intervention administered (or exposure occurred) as intended? | Yes / Can't tell / No    |

## 4. Background and Evolution

### 4.1 From Traditional Automation to Industry 4.0

Automation of industries has evolved a lot over the last several decades. The traditionally rigid and hierarchical automation systems were based on programmable logic controller (PLC) based control, supervisory control and data acquisition (SCADA) system, and special hardware interfaces. Although these systems were effective for the fixed processes, they were not flexible, adaptable, and scalable. Industry 4.0 represents a move toward decentralized, intelligent, and connected manufacturing environments [1]. It connects physical production systems with digital technologies, allowing for dynamic and autonomous operations. Unlike traditional automation, modern systems can self-optimize, perform predictive maintenance, and adapt based on real-time data and analytics. Figure 2 shows the evolution of industrial automation toward Industry 4.0.

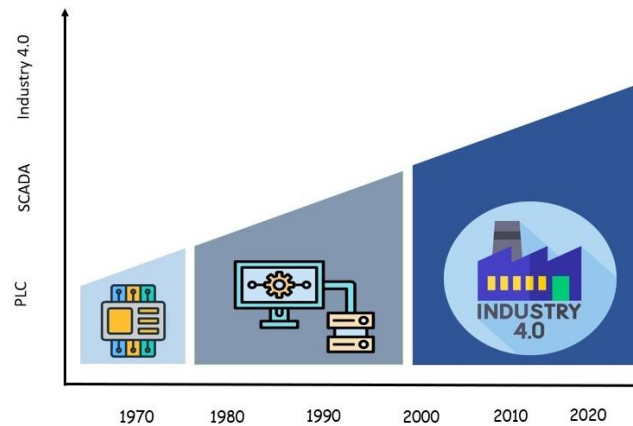


Fig. 2. Evolution of industrial automation toward Industry 4.0.

## 4.2 Definitions and Key Concepts

The Internet of Things (IoT) is a network of tangible things that are fitted with sensors, software, and connectivity. The configuration allows them to collect and communicate information on the internet. IoT devices can provide the capability to monitor and track production assets in real time in an industrial environment. A particular application to the industrial field is the Industrial Internet of Things (IIoT), a subdivision of IoT. It specializes in the merging of machines, control systems, and data analytics to increase efficiency, safety, automation in aspects such as manufacturing, energy and logistics. Cyber-Physical Systems (CPS) are the integration of computation, networking and physical processes. Embedded systems in CPS, physical processes are monitored and controlled and, in many cases, connected with a feedback loop, with physical actions affecting the amount of computation and conversely. Smart factories are strengthened by CPS, which means that machines and systems interact seamlessly.

Conventionally, SCADA system is used to monitor and control industries. They tend to operate within closed networks and have problems with interoperability and real-time analysis. Instead, IoT goes beyond plant boundaries, is compatible with multiple devices and can integrate with cloud platforms and machine learning systems [10, 11].

## 5. Key Characteristics and Enabling Technologies

### 5.1 Scalability and Interoperability

Industrial environments need scalable architectures to handle a rising number of connected devices, sensors, and machines. Interoperability across different systems is achieved with standard communication protocols like MQTT, OPC UA, and RESTful APIs [6]. These protocols allow for smooth data exchange between older devices and modern platforms.

### 5.2 Real-Time Monitoring and Decision-Making

In real-time, it is possible to view equipment and processes and make decisions in advance. IoT sensors are collecting data continuously including temperature, vibration, and pressure. This information is analyzed and trends are found and detected anomalies. Auto response can be used by systems so that they can react to predetermined limits or by operator action to enhance safety and functionality. [8].

### 5.3 Modularity and Flexibility

Contemporary industry systems are modular and it is relatively simple to add new components and technologies without disrupting the system. This versatility enables prompt modifications in work processes to suit changing standards of production [4].

### 5.4 Edge and Cloud Computing

An edge-cloud computing hybrid solution provides the balance between speed and scalability. Local processing is done by devices to minimize latency, whereas heavier computations, long-term storage, and so forth are done on cloud platforms. This structure is particularly convenient in predictive maintenance, as well as aggregating large volumes of data [17].

### 5.5 Artificial Intelligence and Machine Learning

Machine learning algorithms and AI enable machines to analyze the information and enhance their functioning. For predictive maintenance and process optimization, and for intelligent fault detection these methods are necessary. Moreover, these facilitate an independent decision-making process and reduce the amount of manual interaction in the industrial process [9].

### 5.6 Cybersecurity and Resilience

The higher the level of connectivity, the higher the risk of a cyber-attack. Intrusion detection systems, secure access control, and encryption are some of the security measures that are significant in achieving data integrity and the safeguarding of operations [12]. The effectiveness of industrial automation systems based on the use of IoT depends on a specific set of features and technologies. These aspects are the basis of smart factories and the digital transformation of Industry 4.0. This part elaborates on the major characteristics that characterize the IIoT systems nowadays and the technologies underpinning the systems.

### 5.7 Wireless Connectivity and Sensor Integration

Industrial wireless technologies have become reliable and high-speed, including LPWAN, LoRaWAN, and 5G. These technologies are in favor of mobility, simple deployment and scalability. Wireless sensor networks (WSNs) are crucial for remote monitoring or detecting disastrous environments [14].

### 5.8 Digital Twins and Simulation Models

Digital twins replicate the physical assets in terms of their real-time status and behavior. Combined with data of the IoT, they make it possible to perform predictive analytics, virtual testing, and performance optimization. These models enhance planning and minimize the downtime by enabling efficient experimentation and prognostication.

### 5.9 Green IoT

Green IoT is used in the industrial automation sector to pursue energy efficient sensing, communication, and data processing to lower the environmental effects and operation costs. Green IoT helps in achieving effectiveness and sustainable intelligent manufacturing systems through integration of low-power products, intelligent management of resources, and green networking technologies [8]. The enabling technologies discussed above are the solutions to emerged challenges related to IoT. Table 3 presents a comparative summary of implementation challenges, solution approaches, and industrial impacts reported in the reviewed literature.

Table 3. Implementation Characteristics of Reviewed Studies

| Ref. | Study                      | Implementation Challenge                   | Solution-Approach                             | Success Factors                                | Industry-Impact                              |
|------|----------------------------|--------------------------------------------|-----------------------------------------------|------------------------------------------------|----------------------------------------------|
| [1]  | Qiu et al., 2025           | Security, system integration               | IIoT, CPS, IACS, AI/ML, 5G                    | Flexibility, efficiency, reliability           | Linked infrastructure, automation            |
| [2]  | Lampropoulos et al., 2019  | Early-stage adoption, interoperability     | IIoT, CPS, Cloud, Big Data                    | Digital-physical integration, analytics        | Smart factories, cost reduction              |
| [3]  | Soori et al., 2023         | Machine failures, energy inefficiency      | IoT sensors, real-time monitoring             | Predictive analytics, energy optimization      | Reduced downtime, improved safety            |
| [4]  | Nirmala et al., 2022       | Rigid legacy systems                       | AI-assisted IoT automation system             | Flexibility, real-time intelligence            | Improved responsiveness, control             |
| [6]  | Gil et al., 2022           | Protocol incompatibility                   | Standardized IoT protocol framework           | Interoperability, real-time integration        | Enhanced communication in electrical systems |
| [7]  | Lennvall et al., 2017      | Industrial IoT adoption barriers           | IoT infrastructure planning                   | Robustness, scalability                        | Practical guidelines for adoption            |
| [8]  | Pandey et al., 2022        | Data utilization, real-time analytics      | ML-based industrial analytics framework       | Predictive accuracy, automation                | Downtime reduction, optimization             |
| [9]  | Visconti et al., 2024      | Integration of diverse systems             | Comparative analysis of IoT/ML solutions      | Architectural flexibility, data analysis       | Enhanced monitoring, resource management     |
| [10] | Babayigit & Abubaker, 2024 | SCADA limitations, lack of connectivity    | IoT architectures replacing SCADA             | Real-time control, modularity                  | Modernized control systems                   |
| [11] | Deshpande et al., 2016     | Hardware deployment, sensor interfacing    | IoT-enabled microcontroller systems           | Practical design, cost-effectiveness           | Entry-level industrial IoT deployment        |
| [12] | Shaukat et al., 2021       | IoT security threats                       | Threat analysis, encryption techniques        | Risk mitigation, secure communication          | Improved industrial cybersecurity            |
| [13] | Alladi et al., 2019        | Centralized vulnerabilities                | Blockchain, DAG, Encryption                   | Decentralized cryptographic security           | Data integrity, cost efficiency              |
| [14] | Majid et al., 2022         | Security, automation complexity            | WSN, Deep Learning, Blockchain                | Data security, intelligent analysis            | Operational control, sustainability          |
| [15] | Nurelmadina et al., 2021   | Infrastructure limitations, spectrum usage | Cognitive LP-WAN, Cognitive Radio             | Efficient spectrum management, AI integration  | Improved network reliability                 |
| [17] | Chandu, 2024               | Network generalization, resource usage     | Federated Learning, Blockchain, Digital Twins | Security, data integrity, robotics integration | Cost savings, reliability, safety            |

## 6. IoT Architectures and Frameworks in Industry 4.0

Development of effective and scalable IoT models is a prerequisite to Industry 4.0 objectives. These architectures describe the flow of data between physical sensors and decision-making systems. They also demonstrate the way in which industrial processes can be automated, tracked and enhanced.

### 6.1. Layered IoT Architecture

A widely used structure in industrial IoT is the layered architecture, which typically has four main layers:

- **Perception Layer:** Perception layer is the lowest layer that is added and it comprises sensors, actuators, RFID tags and embedded machines. It gathers the physical environment data.
- **Network Layer:** It is the layer that handles the transportation of data among devices and systems that are central. It comprises wireless and wired communication protocols.
- **Middleware Layer:** This layer involves the provision of middleware platforms on which data is filtered, aggregated, stored and semantically translated.
- **Application Layer:** Application layer is considered as the uppermost layer which comprises user-facing services such as dashboards, control systems, and analytics. It aids in decision making and business logic.

This architecture is scalable, fault-isolated and easier to manage in complex industrial systems. They demonstrate that edge and fog computing paradigms reduce real-time and bandwidth limitations by pushing compute to the edge, support low-latency analytics, and minimize network overhead in smart factory implementations [33].

### 6.2. Industrial Reference Architectures

Several standardized frameworks have been introduced to guide developing and deploying industrial IoT systems:

- **RAMI 4.0 (Reference Architectural Model for Industry 4.0):** This 3-D model shown in Figure 3 maps the IT layers and product lifecycle stages as well as the levels of hierarchy in a system. It assists in linking operational systems and IT systems.

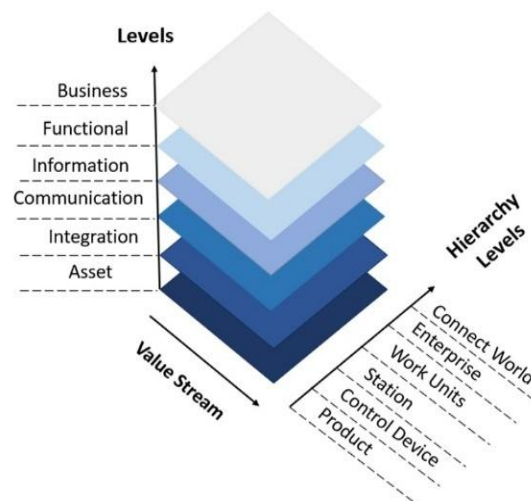


Fig. 3. RAMI 4.0 architecture highlighting IT layers and hierarchy levels.

- **IIRA (Industrial Internet Reference Architecture):** Proposed by the Industrial Internet Consortium (IIC) [34], IIRA focuses on business, usage, and functional perspectives across various industrial fields. As shown in Figure 4, the architecture consists of relationship of four viewpoints.

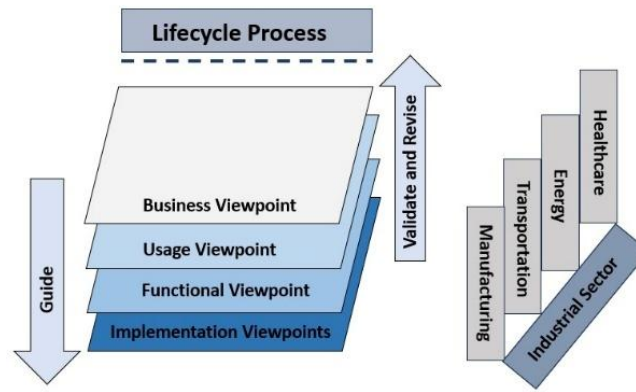


Fig. 4. Relationship among IIRA Viewpoints.

These reference architectures help connect hardware, software, and organizational workflows into cohesive Industrial IoT strategies.

### 6.3. Role of Cloud, Edge, and Fog Computing

Modern Industrial IoT architectures use a hybrid computing model. A schematic diagram of such model is shown in Figure 5:

- **Cloud Computing:** Provides high computational power and long-term storage. It is useful for centralized analytics, digital twin models, and enterprise-level decision support.
- **Edge Computing:** Processes data locally near the source, such as on a machine or gateway. It reduces latency and improves response time for time-sensitive applications.
- **Fog Computing:** Connects cloud and edge computing by allowing distributed processing in intermediate layers. It is ideal for systems that require real-time interaction with some centralization.

Qiu et al. [1] showed how these computing models are being combined with CPS and Industrial IoT infrastructures to improve system responsiveness and data-driven control. Similarly, Nirmala et al. [4] demonstrated an AI-enabled industrial automation system that uses cloud-based analytics and real-time sensor data at the edge.

The way industrial data is analyzed, stored, and processed is determined by edge and cloud computing. Edge computing provides real time control with reduced latency, and cloud computing provides large scale analytics and model training. The decision and tradeoff between the edge and the cloud have a direct effect on the AI performance, network traffic, and security demands. Thus, the computing strategies should be synchronized with sensing, intelligence, and architecture layers to ensure effective operation of the system on the system level.

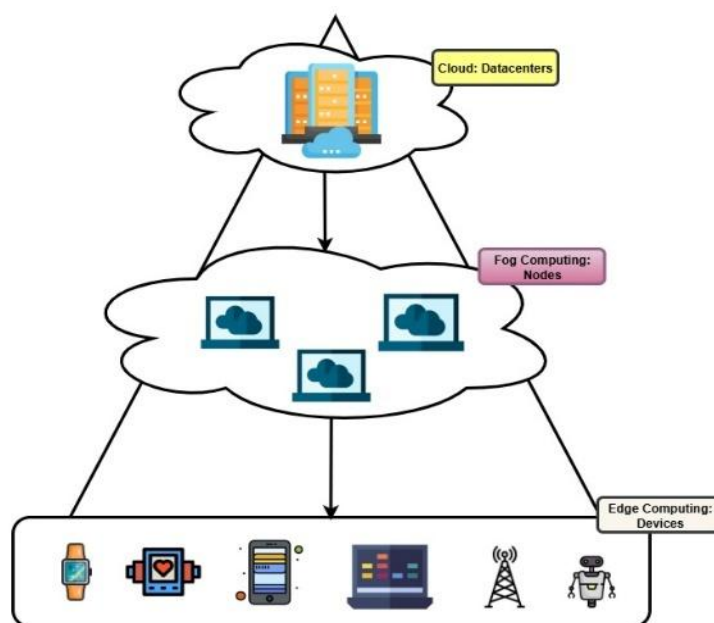


Fig. 5. The architecture of IIoT using hybrid computing model

#### 6.4 PLC and Middleware Integration in Smart Factories

The industrial IoT automation model combines the Programmable Logic Controllers (PLCs) with the middleware platforms like Node-RED to facilitate the process of acquiring, processing, and communicating data seamlessly among smart analytics and scalable automation of smart industrial environments.

The industrial architectures offer the structural framework that connects the sensing, intelligence, and security layers. The use of centralized or distributed architectures impacts the latency, reliability and scalability of the system as a whole. Executions on this tier are relayed to the AI deployment, location of the sensors, and security measures and this shows that the architecture/system level design cannot be separated. Coherent and efficient Industry 4.0 systems are provided by integrated planning on all layers.

### 7. Communication Protocols and Standards

Reliable communication is crucial for Industrial IoT systems. It ensures smooth data exchange between sensors, machines, controllers, and cloud platforms. Various protocols are used in IIoT, each designed for specific constraints like latency, bandwidth, reliability, and compatibility.

#### 7.1 IoT Protocols in Industrial Environments

The following protocols are commonly found in Industry 4.0 deployments:

- **MQTT (Message Queuing Telemetry Transport):** This is a lightweight publish-subscribe protocol that is suitable in low bandwidth networks with a limited number of devices. It is also extensively applied to IIoT in terms of telemetry and state reports [6].
- **CoAP (Constrained Application Protocol):** This is a protocol created to support resource-restricted devices and enables communication between these devices using a RESTful style of communication over UDP. It is suitable in sensor networks of industrial monitoring.
- **AMQP (Advanced Message Queuing Protocol):** This is a powerful queuing protocol that provides message orientation, queuing and routing. It offers middleware integration into business-level middleware.
- **OPC UA (Open Platform Communications Unified Architecture):** This is one of the most important standards of industrial automation. It offers a platform-independent and secure communication between industrial devices and systems [6].
- **Zigbee and LoRaWAN:** These are low power wireless protocols that can use mesh networking and long-range communication. They can be employed to monitor the environment and track assets in factories [7].

#### 7.2 Protocol Convergence and Interoperability Challenges

Integrating different protocols into a unified IIoT system presents challenges such as semantic mismatch, timing problems, and varying levels of quality of service. Older systems often do not support modern IP-based protocols, making protocol gateways and middleware necessary. Gil et al. [6] suggested a protocol convergence model that merges OPC UA and MQTT to connect legacy systems with new Industrial IoT platforms which is shown in Figure 6. Lennvall et al. [7] pointed out the difficulties of synchronizing real-time data in industrial environments, particularly with mixed-protocol setups.

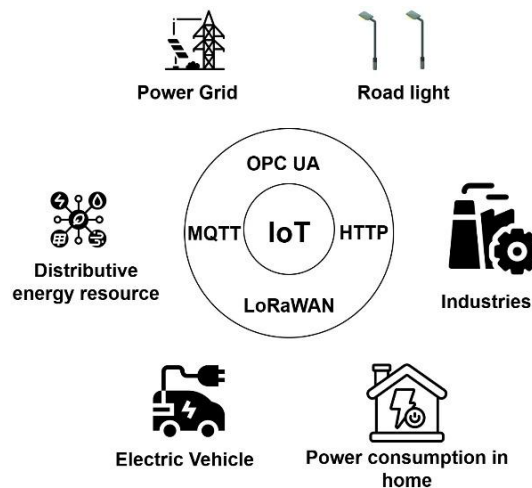


Fig. 6. IoT ecosystem in automated industry.

### 7.3 5G Communication Trials in Industrial Automation

While protocols like MQTT and OPC UA are central to Industrial IoT communication, 5G, particularly Ultra Reliable Low-Latency Communication (URLLC), provides a significant improvement in real-time performance. Ansari et al. [21] showed through European industrial trials that advanced 5G setups can achieve latencies below 1.12ms with 99.9% reliability. Measurements of latency of industrial traffic on 5G networks were conducted in that study with periodic messages (8, 16, 32 ms periods) with 100 bytes and 1024 bytes message size simulating protocols like PROFINET (Process Field Net) and CIP (Common Industrial Protocol). The findings demonstrate that 5G systems with Mobile Broadband results in the low average latencies (3.76 to 6.9 ms uplink, 5.2 to 6.2 ms downlink) but the percentiles (99th, 99.9th) indicate the great diversity of latency differences, particularly in the case of larger messages. Even within the same modem chipset, there was a difference in the performance of the devices, revealing that it was affected by the hardware. Reliability can be enhanced with the help of configuring the RAN and relying on the redundant communication paths like FRER, which also helps decrease the latency spikes. By comparison, 5G systems configured by URLLC have ultra-low and very reliable latencies 1.2 ms at 99.9% on both small and large messages, which are appropriate in highly demanding industrial internet applications.

### 7.4 Protocol Comparison

Table 4 compares common industrial IoT communication protocols. The column known as Transport in the table shows the underlying communication layer used by every protocol. The column of Quality of Service (QoS) gives the degree of reliability and delivery guarantee of messages. The actual or realistic size of data typically or actually found in industrial applications, not theoretical protocol sizes, is called the Payload Size. The Resource Usage shows the proportionate overhead of computational, memory, and energy used to run the protocols. Lastly, the Industrial Suitability also captures the general applicability of any given protocol to the industrial settings in terms of scalability, robustness and the interoperability.

Table 4. Comparison of Common Communication Protocols in IIoT

| Protocol | Transport         | Quality of Service | Payload Size | Resource Usage | Industrial Suitability |
|----------|-------------------|--------------------|--------------|----------------|------------------------|
| MQTT     | TCP               | Medium             | Small–Medium | Low            | High                   |
| CoAP     | UDP               | Low                | Small        | Very Low       | Medium                 |
| AMQP     | TCP               | High               | Medium–Large | Medium         | High                   |
| OPC UA   | TCP               | High               | Large        | High           | Very High              |
| Zigbee   | IEEE 802.15.4     | Low                | Small        | Very Low       | Medium                 |
| LoRaWAN  | LoRa PHY (Custom) | Medium             | Very Small   | Very Low       | Medium                 |

Communication protocols define how data flows between sensors, controllers, and processing units, affecting both reliability and latency. The choice of protocols affects the responsiveness of AI models, network congestion, and security enforcement. End-to-end integration of the system requires the interoperability of heterogeneous devices. Therefore, the protocols cannot be viewed in isolation; they should be analyzed within the overall architecture and between the layers.

## 8. Data Integration and Interoperability

Since Industry 4.0 is becoming a reality, the seamless exchange of data between various systems is the only way to realize smart industrial automation. One of the requirements is interoperability, which enables different elements such as sensors and controllers and enterprise systems to interact with each other. The section addresses the issues of critical elements of semantic interoperability, middleware solutions, and integration case studies.

### 8.1 Semantic Interoperability

Semantic interoperability is a guarantee that the received information is not simply correct in its form but also has a sense in context. This works in industrial settings to enable automated systems to interpret sensor readings, control commands and process state correctly. Ontologies and shared vocabularies are systems that are often promoted to achieve inter-system understanding. OPC UA and Automation ML among other standards are used to enable similar interpretation of data on different platforms. This makes integration less complicated and enables real-time integration [6].

### 8.2 Data Formats, Ontologies, and Middleware

Many different data formats are common in industrial systems: JSON, XML, or binaries. Middleware solutions act as a bridging solution that:

- Interprets communication protocols,
- Collects and filters incoming data,
- Applies semantic tags using standard ontologies.

Middleware platforms examples are Eclipse Ditto, Kaa IoT, and ThingWorx. These platforms facilitate flexible modeling, RESTful APIs, as well as event-based architectures.

### 8.3 Case Studies of System Integration

Gil et al. [6] proved that, combining protocols, such as MQTT and OPC UA, enhances interoperability in electrical automation systems through a unified protocol stack.

Majid et al. [14] proposed a model which links wireless sensor networks, deep learning and blockchain technology to help in real-time monitoring and secure exchange of data within smart factories. These researches indicate that semantic alignment, protocol translation, and middleware intelligence is essential to successful IIoT implementation and integration within organizations.

## 9. Artificial Intelligence and Machine Learning in Industrial IoT

Machine Learning (ML) and Artificial Intelligence (AI) have an important role to play in accomplishing the objective of intelligent automation in the industry. They enable predictive, adaptive and autonomous behaviors that enhance efficiency, reliability and decision making of Industrial IoT systems.

### 9.1 Predictive Maintenance and Anomaly Detection

Predictive maintenance is one of the typical applications of ML in the Industrial IoT. ML models can identify the faults of equipment in time and recommend their servicing thanks to sensor data analysis to mitigate potential failures. This will minimize unplanned downtime, the cost of maintenance, and extend the life of the machinery used [8], [23]. The integration of IoT and ML makes smarter automation in industrial settings, and some applications, such as adaptive quality control, predictive maintenance, and real-time fault detection are now possible with the use of deep learning techniques in Industrial IoT environments [28]. Figure 7 shows the excellence of DL over other algorithms in the applications of IIoT.

### 9.2 Process Optimization and Quality Control

The optimization of processes can also be done with the assistance of ML models that learn based on previous data about production to suggest optimal operating conditions. Such approaches as reinforcement learning and genetic algorithms contribute to the optimization of manufacturing parameters to achieve efficiency and energy savings. In quality control, computer vision with deep learning enables real-time defects to be detected on assembly lines and reduces the human task of inspecting products and enhances consistency of products.

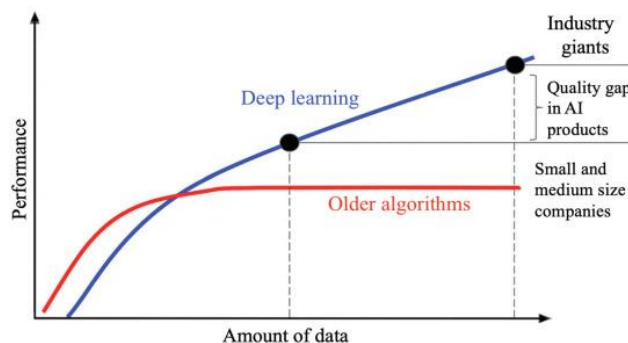


Fig. 7. Comparison Deep Learning with traditional algorithm in Industrial IoT in [28].

### 9.3 ML Model Integration and Edge Intelligence

The use of ML models in industrial systems is associated with the following challenges: latency, resource availability, and privacy of the data. This has seen the rise of edge AI where processing is performed on industrial gateways or embedded controllers. Visconti et al. [9] demonstrated that edge-optimized machine learning models can assist real-time analytics in intelligent manufacturing environments minimizing the use of centralized cloud computing.

### 9.4 Machine Learning Workflow in Industrial IoT Systems

An industrial IoT ecosystem is a powerful information flow that is supported by machine learning and data processing to allow the making of data-driven decisions. It begins with the sensor data-collection where the environmental and operating data such as temperature, pressure, vibration or light intensity are recorded by the use of

IoT-based sensors. This raw information is moved to an edge gateway upon which certain preliminary processing is performed. This incorporates data-quality filtering, noise removal and normalization such that data are not subjected to as much latency before being sent to cloud systems or centralized systems. After preprocessing, feature extraction is done on the data. This step consists of the calculation of the various measures of interest including statistical properties (mean, variance), frequency domain properties (e.g., FFT coefficients) and time series properties that reflect important behavior of raw signals. The features obtained are then fed into a machine learning model. Popular algorithms are Support Vector Machines (SVM), Random Forest, and XGBoost, based on the application, e.g. anomaly detection, predictive maintenance, or quality control. The model provides predictions or classifications, which are transferred to the decision layer. It has been demonstrated in the article [18] that a combination of IoT and better Random Forest algorithm can greatly increase the accuracy and scalability of the industrial load regulation and automation.

Actionable results are produced at the decision layer, e.g. maintenance notifications, process optimization messages, or fault messages. This data is then channeled to the last phase actuation or visualization that encompasses real-time dashboards, alerts through email/SMS, and signals transmitted to PLCs (Programmable Logic Controllers) to be operated automatically. The machine learning workflow has a simple pipeline as described in Figure 8.

The pipeline is end-to-end, increases system autonomy, allows it to detect faults early, and helps to perform efficient data-driven industrial activities.

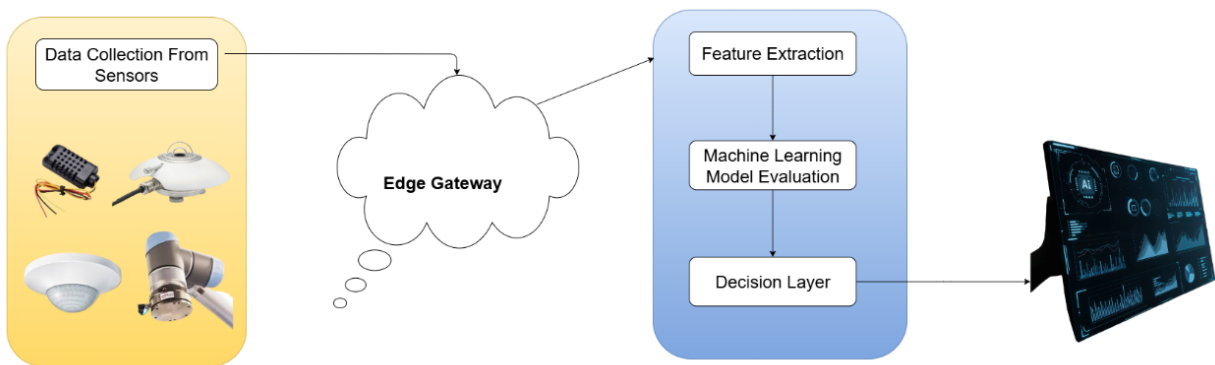


Fig. 8. Typical machine learning pipeline in IIoT environments.

### 9.5 Example: Predictive Maintenance in a Smart Factory

Imagine a smart factory that has several CNC (Computer Numerical Control) machines. Each machine has temperature and vibration sensors that gather time-series data. To find anomalous patterns that predate component wear or failure, a trained machine learning model (such as Random Forest or LSTM) continuously examines the data. Before an actual breakdown happens, the system notifies maintenance staff when the model indicates that a spindle bearing problem in a particular machine is likely to arise. This prevents costly production halts and reduces spare part overuse.

### 9.6 Future Research Directions in AI-Driven Industrial IoT

Future research in AI-driven Industrial IoT is expected to focus on advanced learning paradigms such as federated learning and probabilistic Poisson-based modeling to enable scalable, privacy-preserving, and event-aware industrial automation systems. Federated Learning can be trained privately and de-centrally over distributed devices with the IoT of the industrial in a decentralized manner through the exchange of only model parameters rather than raw data. As Adam and Baroudi [29] point out, the strategy is highly practical in terms of automation effectiveness, strength, and scalability in data-intensive industrial settings. Also, Poisson modeling is a popular tool in the Industrial IoT automation to describe the stochastic occurrence of events-driven processes, including machine faults, sensor alerts, and maintenance requests. It allows precise forecasting of the occurrence of events, which facilitates proactive control, predictive maintenance, and effective optimization of production [35].

At the system level, the success of Artificial Intelligence and machine learning is tied to the availability of accurate information in real-time at the right time, collected by the devices that are linked together. Prediction reliability is closely related with the communication network and the accuracy of sensing. Further, processing latency and computational resources can determine the way AI models can be deployed at edge or cloud. Thus, intelligence cannot be assessed in isolation but it should be regarded in terms of sensing, connectivity, and architecture.

## 10. Wireless Sensor Networks (WSNs) and Connectivity

Wireless Sensor Networks (WSNs) are essential to Industrial IoT, allowing for decentralized, real-time monitoring and control in industrial settings. Such networks have their sensors spread across the environment or facility and gather the operational or environmental data which they transmit wirelessly to central gateways or clouds. In the work of Muniz and Thomaz [25], the role played by Wireless Sensor Networks (WSNs) in enhancing industrial automation

through flexible and probative real-time process control as well as consideration of challenging or risky environments was reported.

### 10.1 Role of WSNs in Industrial Monitoring

WSNs enable constant check-ups of aspects such as temperature, pressure, vibration and humidity in remote or hostile industries. Their use improves:

- Process transparency and traceability
- Future maintenance functionality.
- Energy conservation and operational safety

Majid et al. [14] demonstrated that smart automation and anomaly detection of Industry 4.0 systems can be achieved through the combination of WSNs and deep learning.

### 10.2 Connectivity Technologies: LPWAN and Cognitive Radio

To meet the needs of large-scale industrial deployments, such as long-range communication, low power use, and high scalability, Low Power Wide Area Networks (LPWANs) have become important. Common LPWAN protocols include:

- NB-IoT (Narrowband IoT)
- LoRa (Long Range)
- Sigfox

Nurelmadina et al. [15] indicated that cognitive radio, together with the LPWANs, could be a potential solution to the need to utilize the spectrum more efficiently and increase network flexibility in IIoT applications.

Data collection in industries is based on the wireless sensor networks. The practicality of the information will rely upon the sensor coverage as well as the reliability of the communication systems. Such networks have a direct impact on the work of AI algorithms and the general decision-making process. As a result, sensing and connectivity layers are highly interdependent on intelligence and system level architecture and there is a need to design them together.

## 11. Security and Privacy Challenges

The emergence of IoT and Industrial IoT in the industrial systems is a massive leap towards their evolution, yet also a demanding degree of security and privacy issues. Such high device to device connections and connections, real time data flows and interdependence increase the attack surface and require strong security. The problem of how to design security measures that should be implemented on the variety of IoT devices has been on the center stage in the recent past. A part of the traditional defensive methods (anti-virus software, firewalls) can be very weak due to the heterogeneity of the protocols and the restrictions of the devices [22]. Lots of devices can be attacked by zero-day exploits and other threats due to the absence of security defaults and standardization of the updates. Kaur et al. classify security attacks by IoT protocol layers, which gives an extensive taxonomy. They emphasize the access to the latest information and forensic methodology, which is crucial to the creation of efficient intrusion detection systems (IDS) that would fit in an IoT setup.

### 11.1 Common Security Threats in IIoT

The threats to industrial IoT systems include:

- **Device-level threats:** The unauthorized access to edge devices and sensors may lead to false readings or wrong control acts [36].
- **Network-level attacks:** These attacks involve Denial of Service (DoS), eavesdropping, spoofing, and man-in-the middle (MitM) attacks [36]. They interfere with industrial communications and reduce reliability.
- **Data integrity and confidentiality breaches:** Manipulated information may result in making erroneous decisions and safety and performance may be jeopardized [36].
- **Insider threats:** Special access can be stolen or modified by the internal individuals who have the special access to the sensitive data [36].

As noted by Shaukat et al. [12], the convergence of Information Technology and Operational Technology systems in Industry 4.0 settings poses problems that cannot be resolved using the established network security models.

### 11.2 Security Mechanisms and Countermeasures

A number of measures are worked out to deal with such risks:

- **End-to-end encryption:** It involves the transmission of secure data across untrusted networks in cryptography protocols [37].
- **Blockchain technology:** It offers decentralized authentication, tamper-proof logging, and access control. Alladi et al. [13] emphasized that it can be used to provide trustworthiness among distributed IIoT components.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Detect the existence of unusual activity and block suspicious packets as they arrive [38].
- **Secure boot and firmware validation:** Stops the injection of malicious code at system start-up [39].

Moreover, Williams et al. [19] offered an edge-computing-based forensic model that enhances incident response and postattack investigation outcomes because it allows an unmodifiable collection of evidence and acts as an anomaly detector in IIoT systems.

### 11.3 Privacy and Data Protection Strategies

In addition to security, the industrial systems must also address the privacy issue especially when information is related to operators, places, or business process sensitivities:

- **Data anonymization:** Protects privacy while allowing for analytics.
- **Federated learning:** Allows collaborative model training across devices without sharing raw data, which maintains privacy and reduces bandwidth use.

It is important to note that as major drivers of Industry 4.0, blockchain, AI-enhanced intrusion detection, and zero-trust architecture are essential to ensure data integrity, real-time monitoring, and threat resilience over distributed industrial networks. Enemosah and Ifeanyi [24] suggested a multi-layered cloud security framework designed for IoT–SCADA systems in order to improve the cybersecurity and dependability of industrial automation.

Security and privacy are the mechanisms that affect the performance and reliability of the system. Encryption, authentication and intrusion detection all add computational load as well as may affect network latency, which further influences AI processing and real-time control. The security design must consider the interaction amongst the layers of the system but not consider the security as a supplement. This combination stresses the fact that it is impossible to consider the idea of trust in the absence of connectivity, data processing, and intelligence.

## 12. Challenges

Despite significant progress in IIoT and smart industrial systems, several challenges remain that limit widespread adoption and robust performance in Industry 4.0 settings which is summarized in Table 5.

### 12.1 Legacy System Integration

Many industries still operate on legacy SCADA and proprietary automation systems, making integration with IIoT infrastructures difficult. Bridging this gap often involves complex middleware solutions or hardware retrofitting, which increases deployment costs and complexity [17].

### 12.2 Standardization Gaps

The lack of the universal data format, communication protocols, and semantic models contributes to the fragmentation of the ecosystems. This has reduced their interoperability, requiring cross-vendors and platforms to exchange data smoothly, becoming a challenge to scalable deployments. The other broadcasted hazard is the absence of commonality in publicly accessible IoT security data sets. As Kaur et al. [22] highlight, many existing datasets are outdated, limited in scope, or lack diversity in attack scenarios. This hampers the development and benchmarking of robust intrusion detection models for diverse industrial environments.

### 12.3 Scalability and Real-Time Constraints

Recent reviews highlight that real-time industrial IoT scenarios like motion control often lack standardized networking mechanisms capable of delivering deterministic latency and reliability. Especially when wireless and mobile nodes are involved [26].

The IT and OT systems convergence increases the attack surface of the industrial networks. The overwhelming majority of IIoT devices do not contain the effective security mechanisms, and therefore, they can suffer the cyber risks like spoofing, man-in-the-middle attacks, and ransomware [12].

### 12.4 Cost and Return on Investment

The costs of implementing Industrial IoT solutions are quite high initially due to the hardware, connectivity, cloud infrastructure and analytics platforms. In the case of small and medium-sized enterprises (SMEs), adoption may be hampered by the cost index and unidentified ROI. Industrial automation greatly lowers the cost of business operations

and increases ROI by optimizing the workflow and predictive maintenance. Nonetheless, high initial investment is one of the greatest impediments to SMEs even though they can achieve efficiency in the long run. [5].

### 12.5 Workforce Readiness and Skills Gap

The effective deployment and maintenance of IIoT systems demand multidisciplinary skills spanning embedded systems, networking, cloud computing, and AI. Accurate modeling under dynamic environments remains a challenge. While Poisson models improve event forecasting, their precision can drop when external variables like market shifts are introduced [35].

Table 5. Summary of Challenges and Open Issues in IIoT Implementation

| Challenge                           | Description                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Legacy System Integration           | Difficulty in integrating outdated SCADA and proprietary systems with modern IIoT platforms; requires middleware and raises cost [17]. |
| Lack of Standardization             | Absence of universal protocols and data formats creates interoperability issues, hindering multi-vendor integration.                   |
| Scalability and Latency Constraints | Managing large-scale, real-time industrial data with low latency and high throughput remains technically demanding.                    |
| Security and Privacy Risks          | IIoT systems face increased exposure to cyber threats due to the convergence of IT and OT, with limited device-level protections [12]. |
| Cost and ROI Concerns               | High initial deployment cost and difficulty demonstrating short-term return on investment, especially for SMEs.                        |
| Workforce and Skill Gaps            | Lack of professionals skilled in both OT and advanced IT (e.g., cloud, ML) hampers adoption and maintenance of IIoT systems.           |

## 13. Future Trends and Emerging Technologies

The evolution of Industry 4.0 is increasingly shaped by emerging technologies and shifting industrial demands. Among the most promising developments is the rise of digital twins, which are virtual representations of physical assets or processes. According to future automation architectures, Hussein et al. [30] suggested a lightweight PLC-Node-RED integration in Industrial IoT environments, enabling edge processing, low-latency communication, and user-friendly control workflows without the need for complex SCADA infrastructure. An alternative privacy-preserving scenario to train machine learning models is provided by the so-called federated learning that does not expose raw data even to distributed IIoT nodes. This is particularly pertinent in the setting where there are confidential operation information. On-going work examines effective aggregation mechanism, communication optimization and secured model updates to facilitate scalable federated learning in the industrial domain.

Green IoT has become an idea that focuses on low-power communication, energy-conscious design, and renewable energy incorporation to achieve the global sustainability objectives. Such areas of focus as edge intelligence, hardware miniaturization, and life-cycle based analytics are mentioned in [8]. Also, the emerging edge and fog computing have enabled decentralized processing nearer to the source of the data. This will enable real-time analytics, fault and actuation detection through minimization of latency and bandwidth consumption. Scientists are focusing on fault tolerance architecture, edge coordination, and low-weight artificial intelligence (AI) models to improve the reliability of industry. Efforts are made to improve operational risk forecasting of smart industry and defect prediction using Poisson-based modeling and machine learning with the aim of improving these processes [35]. Lastly, the absence of universal standardization structures has also been a hindrance to the adoption of IIoT. To facilitate smooth scalability in the industrial environment and facilitation of cross vendor integrations of systems, there are attempts to create open, semantic, and interoperable reference models [6]. Zhukabayeva et al. [31] highlighted that federated learning, blockchain, and AI must be integrated into the Industrial IoT-edge computing systems to address the changing cybersecurity threats and improve the automation structures in industries in the future.

## 14. Answers to The Research Questions

**RQ1.** How do IoT and Industrial IoT transform traditional industrial automation into decentralized intelligent systems?

**Answer:** IoT and IIoT transform the traditional, inflexible automation systems including SCADA and PLC-based architecture to decentralized, flexible, and networked intelligent ecosystems. By enabling real-time data monitoring, edge and cloud computing, Machine Learning integration, wireless sensor networks, and digital twins, industrial systems move away from centralized command-control to autonomous, adaptive decision-making. This transformation helps in supporting scalability, predictive maintenance, optimization of resources and resilient manufacturing processes, which was not easy with conventional automation.

**RQ2.** What challenges hinder the implementation of IoT-driven automation in Industry 4.0?

**Answer:** IoT-based automation has a high barrier to its potential. These are challenges in integrating legacy systems, global lack of standardization, limited scalability, excessive implementation cost, cyber vulnerabilities, and workforce preparedness. These challenges must be overcome without exposing industries to fragmented adoption and exposure to operational risks, lowering the competence of Industry 4.0 transitions.

**RQ3.** What IoT innovations will drive the future of intelligent automation in Industry 4.0?

**Answer:** The next generation of industrial automation will be based on federated learning of privacy-aware AI, green IoT of energy efficiency and sustainability, and low-code/no-code orchestration platforms that make integration systems easier. There will also be intelligent, adaptable and sustainable factories using AI-powered analytics, 6G-based ultra-reliable communications, digital twins, and cybersecurity systems. This will render Industry 4.0 more self-reliant, green, and robust.

## 15. Discussion

Instead of treating architecture, communication, intelligence, and security layers separately, the discussion focuses on a system-level synthesis of the reviewed literature, emphasizing their interdependence. From the reviewed literature, it is evident that IoT has successfully shifted from rigid, centralized setups like PLCs and SCADA to decentralized, intelligent, and flexible ecosystems. Such technologies as real-time monitoring, edge and cloud computing, AI-driven analytics, and wireless sensor networks have enabled predictive maintenance, enhanced decision-making abilities and enhanced operational resilience. The tradeoff between flexibility and interoperability is one of the key lessons to be learned. Despite promising scalability and responsiveness of layered structures and hybrid cloud-edge computing, industries are yet to experience universal standards. Making protocols integrate, e.g., the use of MQTT with OPC-UA, is getting much better, however, real semantic interoperability among platforms and vendors at a practical level is a problem. This inconsistency does not support massive implementations, particularly in attempts to integrate old systems with modern IIoT infrastructure. The other notable fact is that there is an uneven upkeep of IoT applications. The literature indicates predictive maintenance and smart manufacturing, which have definite advantages in the reduction of downtimes and increase in productivity. On the other side, such categories as Green IoT, sustainable automation, and low-code orchestration platforms are relatively under-researched, yet they are essential to future alterations in the industry. Likewise, the use of digital twins in industries remains pilot projects and test-cases despite the discussed technology as a revolutionary one. The use of ML and AI is an additional breakthrough especially in the area of anomaly detection and predictive maintenance. Nevertheless, the reliance on big and high-quality datasets indicates a significant gap in the research. Industries do not have standardized and varied datasets to build effective models. The most important and unsolved solution is cybersecurity. Though there have been some solutions that exist on blockchain, encryption, and intrusion detection systems, most of them rely on small-scale experiments. The fact is that outdated hardware, a multitude of devices, and insufficient training of the workforce are still the weaknesses in industries. Table 6 summarizes the major challenges, existing solutions, research gaps, and future directions spotted in this review.

Table 6. Comparative Summary of Challenges, Existing Solutions, Research Gaps, and Future Directions in Industrial IoT

| Challenge                                  | Existing Solutions                                                                   | Research Gaps                                                                                   | Future Directions                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Legacy System Integration                  | Middleware frameworks, protocol converters, IoT gateways                             | High cost and complexity in retrofitting; limited vendor-neutral platforms                      | Design inexpensive, lightweight integration solutions and support open-source standards for legacy connectivity                    |
| Lack of Standardization & Interoperability | Use of OPC-UA, MQTT, and hybrid protocol stacks                                      | No universal semantic models; fragmented ecosystems across vendors                              | Establish global interoperability frameworks; develop semantic ontologies for cross-platform communication                         |
| Scalability & Latency Constraints          | Edge and fog computing for local analytics; 5G trials for URLLC                      | Limited real-world validation in large-scale factories; deterministic latency still a challenge | Integrate 6G and advanced edge orchestration; optimize network slicing for time-critical IIoT applications                         |
| Cybersecurity & Privacy Risks              | Blockchain, end-to-end encryption, intrusion detection/prevention systems            | Most solutions are tested only in small-scale or simulated environments                         | Deploy multi-layered zero-trust security; enhance federated learning for privacy-preserving analytics                              |
| High Cost & ROI Concerns                   | Predictive maintenance and workflow optimization for long-term savings               | SMEs face barriers due to high upfront investment and uncertain short-term ROI                  | Develop cost-sharing models, cloud-based IoT-as-a-service; promote modular, scalable deployments                                   |
| Workforce Skill Gap                        | Training programs in IoT, AI, and cybersecurity                                      | Shortage of multidisciplinary experts combining IT + OT skills                                  | Industry-academia collaboration for capacity building; AI-assisted no-code/low-code tools/simulators to reduce reliance on experts |
| Green IoT & Sustainability                 | Energy-efficient WSNs, low-power communication (LPWAN, LoRaWAN)                      | Limited focus on lifecycle sustainability and carbon footprint reduction                        | Promote Green IoT frameworks, renewable-powered IoT, and energy-efficient AI/ML algorithms                                         |
| Digital Twin & AI/ML Integration           | Predictive maintenance, quality control using ML; pilot digital twin implementations | Deficiency of standardized datasets; scalability and real-time twin updates remain limited      | Develop industrial-scale digital twin platforms; adopt federated learning and transfer learning for data-efficient AI              |

## 16. Conclusion

This review examined how the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) play an important role in the future of industrial automation in Industry 4.0. It emulated architectures, communications protocols, data integration plans, machine learning applications, and cybersecurity designs. The article demonstrated that operational technology (OT) integrated with IT-based infrastructure is producing intelligent, adaptive, and connected manufacturing ecosystems. There is artificial intelligence (AI) based predictive maintenance, digital twins, wireless sensor networks, edge-cloud hybrid computing, and federated learning, which are making operations more efficient, flexible, and responsive. The linkage between legacy systems and modern industrial platforms should use standardization of protocols, semantic interoperability, and middleware platforms, e.g., MQTT and OPC UA. Although such advances have been made, there are still issues. The inter-integration of legacy systems, the real-time constraints of data processing, the possibility of cyber security threats, the confidentiality of data, and the training of personnel are still current challenges. Addressing these issues requires scalable, secure, and interoperable designs with zero-trust models and green IoT practices. In the future, the merging of 6G networks, artificial intelligence (AI)-based analytics, and sustainable computing models will accelerate the digital revolution of the industry. Also, predictive control in smart factories can be enhanced by combining real-time analytics with deterministic techniques such as Poisson modeling [35]. In conclusion, IoT-enabled industrial automation has leveled up from a vision to a necessity. Ongoing research across disciplines, standardization, and innovation will be crucial for creating secure, scalable, and sustainable IIoT systems that can meet the needs of Industry 4.0 and beyond.

## Author Contributions Statement

Rafiul R. Zahid, Rakibul H. Rakib, Iftekhar Rahman and Md A. Amin – Conceptualization, Methodology, Data Curation: Proposed research ideas, Constructed the overall framework, Performed literature survey, data curation. They also drafted the initial manuscript and documented the technical background of the study.

Fahmida Ahmed Antara, Sadia Enam and Tanjum R. Akanto – Review and Editing: Reviewed and edited the manuscript, ensured clarity and coherence, and helped coordinate research milestones and deadlines.

All authors have read and agreed to the published version of the manuscript.

## Conflict of Interest Statement

The authors declare no conflicts of interest.

## Statement Funding Declaration

This research received no external funding.

## Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed during the current study.

## Ethical Declarations

This study did not involve human participants or animals, and therefore ethical approval was not required.

## Acknowledgements

The authors express their gratitude to Nabonita Mitra, Ph.D. candidate at Texas Tech University, USA, for her invaluable help during the literature review process.

## Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, the authors used generative AI tools to improve language clarity, grammar, and readability. The authors carefully reviewed and edited the content, and take full responsibility for the accuracy and integrity of the work.

## Abbreviations

The following abbreviations are used in this manuscript:

AI - Artificial Intelligence  
 IIoT - Industrial Internet of Things  
 IoT - Internet of Things  
 ML - Machine Learning  
 MQTT - Message Queuing Telemetry Transport  
 CoAP - Constrained Application Protocol  
 LoRaWAN - Long Range Wide Area Network  
 OPC UA - Open Platform Communications Unified Architecture  
 SCADA - Supervisory Control and Data Acquisition  
 LPWAN - Low Power Wide Area Networks  
 WSN - Wireless Sensor Network  
 BLE - Bluetooth Low Energy  
 RFID - Radio Frequency Identification  
 PLC - Programmable Logic Controller  
 TCP - Transmission Control Protocol  
 UDP - User Datagram Protocol  
 JSON - JavaScript Object Notation  
 XML - Extensible Markup Language  
 LSTM - Long Short-Term Memory  
 SVM - Support Vector Machine  
 CNC - Computer Numerical Control  
 XGBoost - Extreme Gradient Boosting

## References

- [1] F. Qiu, A. Kumar, J. Hu, P. Sharma, Y. B. Tang, Y. X. Xiang, and J. Hong. A review on integrating iot, iiot, and industry 4.0: A pathway to smart manufacturing and digital transformation. *IET Information Security*, 2025.
- [2] G. Lampropoulos, K. Siakas, and T. Anastasiadis. Internet of things in the context of industry 4.0: An overview. *International Journal of Entrepreneurial Knowledge*, 2019.
- [3] M. Soori, B. Arezoo, and R. Dastres. Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, 2023.
- [4] P. Nirmala, S. Ramesh, M. Tamilselvi, G. Ramkumar, and G. Anitha. An artificial intelligence enabled smart industrial automation system based on internet of things assistance. In *Proceedings of the 2022 International Conference*. IEEE, 2022.
- [5] V. S. Gurav, A. Gugani, Y. R. Meena, V. Marathe, S. A. Vijay, and S. Nanda. The impact of industrial automation on the manufacturing industry in the era of industry 4.0. In *Proc. 2024 15th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–6. IEEE, 2024.
- [6] Santiago Gil, Germán D. Zapata-Madrigal, Rodolfo García-Sierra, and Luis Alberto Cruz Salazar. Converging iot protocols for the data integration of automation systems in the electrical industry. *Journal of Electrical Systems and Information Technology*, 9(1), 2022.
- [7] T. Lennvall, M. Gidlund, and J. Åkerberg. Challenges when bringing iot into industrial automation. In *Proceedings of the 2017 IEEE AFRICON*, 2017.
- [8] Sunil Kr Pandey, S. Vanithamani, Padmakar Shahare, Sayed Sayeed Ahmad, S. Thilagamani, Mohamed M. Hassan, and Enoch Tetteh Amoatey. Machine learning-based data analytics for iot-enabled industry automation. *Wireless Communications and Mobile Computing*, 2022.
- [9] P. Visconti, G. Rausa, C. del Valle-Soto, R. Velázquez, D. Cafagna, and R. Fazio. Machine learning and iot-based solutions in industrial applications for smart manufacturing: A critical review. *Future Internet*, 2024.
- [10] Bilal Babayigit and Mohammed Abubaker. Industrial internet of things: A review of improvements over traditional scada systems for industrial automation. *IEEE Systems Journal*, 18(1), 2024.
- [11] Ashwini Deshpande, Prajakta Pitale, and Sangita Sanap. Industrial automation using internet of things (iot). *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, 5(2), February 2016.
- [12] Kamran Shaukat, Talha Mahboob Alam, Ibrahim A. Hameed, Wasim Ahmed Khan, Nadir Abbas, and Suhui Luo. A review on security challenges in internet of things (iot). In *Proceedings of the 2021 26th International Conference*. IEEE, 2021.
- [13] T. Alladi, V. Chamola, R. Parizi, and K.-K. R. Choo. Blockchain applications for industry 4.0 and industrial iot: A review. *IEEE Access*, 2019.
- [14] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. Gadekallu, and C.-W. Lin. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. In *Italian National Conference on Sensors*, 2022.
- [15] N. Nurelmada, M. Hasan, I. Memon, R. Saeed, K. A. Z. Ariffin, E. Ali, R. Mokhtar, S. Islam, E. Hossain, and M. A. Hassan. A systematic review on cognitive radio in low power wide area network for industrial iot applications. *Sustainability*, 2021.
- [16] R. Rondón, M. Gidlund, and K. Landernæs. Evaluating bluetooth low energy suitability for time-critical industrial iot applications. *International Journal of Wireless Information Networks*, 24:278–290, 2017.
- [17] H. S. Chandu. Leveraging iot for enhanced industrial automation: Innovations and applications. In *Proc. 2nd Int. Conf. Advances in Computation, Communication and Information Technology (ICACCT)*, 2024.
- [18] B. B. V. Rao and H. G. Chandrakanth. Iot based machine learning automation algorithm for controlling the industrial loads. *International Journal of Intelligent Engineering and Systems*, 14(4):146–156, 2021.

- [19] M. Williams, I. Emeterkeve, O. J. Adeyeye, and O. Emehin. Enhancing data forensics through edge computing in iot environments. *International Journal of Research Publication and Reviews*, 5(10):2970–2985, October 2024.
- [20] N. Yadav, V. Gupta, and A. Garg. Industrial automation through ai-powered intelligent machines—enabling real-time decision-making. In R. Arya, S. C. Sharma, A. K. Verma, and B. Iyer, editors, *Recent Trends in Artificial Intelligence Towards a Smart World*, pages 145–178. Springer, September 2024.
- [21] Junaid Ansari, Christian Andersson, Peter de Bruin, János Farkas, Leifeke Grosjean, Joachim Sachs, Johan Torsner, Balázs Varga, Davit Harutyunyan, Niels König, and Robert H. Schmitt. Performance of 5g trials for industrial automation. *Electronics*, 11(3), 2022.
- [22] B. Kaur, S. Dadkhah, F. Shoeleh, E. C. P. Neto, P. Xiong, S. Iqbal, P. Lamontagne, S. Ray, and A. A. Chorbani. Internet of things (iot) security dataset evolution: Challenges and future directions. *Internet of Things*, 22:100780, July 2023.
- [23] M. Sujatha, N. Priya, A. Beno, T. B. Sheeba, M. Manikandan, I. M. Tresa, P. S. H. Jose, V. Perumol, and S. P. Timothy. Iot and machine learning-based smart automation system for industry 4.0 using robotics and sensors. *Journal of Nanomaterials*, 2022:6807585, 2022.
- [24] Aliyu Enemosah and Ogboma George Ifeanyi. Cloud security frameworks for protecting iot devices and scada systems in automated environments. *World Journal of Advanced Research and Reviews*, 22(3):2232–2252, January 2025.
- [25] R. F. Muniz and A. C. F. Thomaz. Revolutionizing industrial automation with wireless sensor networks. *Big Data and Computing Visions*, 3(3):76–83, 2023.
- [26] I. Behnke and H. Austad. Real-time performance of industrial iot communication technologies: A review. *IEEE Internet of Things Journal*, 2023.
- [27] L. D. Nguyen and A. Kortun. Real-time optimisation for industrial internet of things: Overview, challenges and opportunities. In *EAI International Conference on Industrial IoT*, 2020.
- [28] R. A. Khalil, N. Saeed, M. Masood, Y. M. Fard, M.-S. Alouini, and T. Y. Al-Naffouri. Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. *IEEE Internet of Things Journal*, 8(14):11016–11040, July 2021.
- [29] Mumin Adam and Uthman Baroudi. Federated learning for iot: Applications, trends, taxonomy, challenges, current solutions, and future directions. *IEEE Open Journal of the Communications Society*, 5:7842–7877, 2024.
- [30] F. A. Hussein, M. T. Yaseen, and M. O. Mustafa. The future of intelligent industrial systems: Plc, node-red, and iot/iiot. *AUIQ Technical Engineering Science*, 2:53–66, July 2025.
- [31] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi. Cybersecurity solutions for industrial internet of things—edge computing integration: Challenges, threats, and future directions. *Sensors*, 25(1):213, January 2025.
- [32] Quan Nha Hong, Sergi Fàbregues, Gillian Bartlett, Felicity Boardman, Margaret Cargo, Pierre Dagenais, Marie-Pierre Gagnon, Frances Griffiths, Belinda Nicolau, Alicia O’Cathain, et al. The mixed methods appraisal tool (mmat) version 2018 for information professionals and researchers. *Education for Information*, 34(4):285–291, 2018.
- [33] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya. Industrial internet of things applications of edge and fog computing: A review and future directions. *IEEE Access*, 2019.
- [34] Jun Li, Jun-Jiang Qiu, Yong Zhou, Sha Wen, Ke-Qin Dou, and Qing Li. Study on the reference architecture and assessment framework of industrial internet platform. *IEEE Access*, 8:164950–164971, 2020.
- [35] Shashikala H. K. and Surjeet Dalal. The smart analysis of poisson distribution pattern based industrial automation in industry 4.0, pages 1–6, April 2023.
- [36] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranay Goyal, and Biplab Sikdar. A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.
- [37] Tanishq Varshney, Nikhil Sharma, Ila Kaushik, and Bharat Bhushan. Architectural model of security threats and their countermeasures in iot. In *Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 2019.
- [38] Esra Altulaihan, Mohammed Amin Almaiah, and Ahmed Aljughaiman. Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions. *Electronics*, 11(20), 2022.
- [39] Xiaotao Feng, Xiaogang Zhu, Qing-Long Han, Wei Zhou, Sheng Wen, and Yang Xiang. Detecting vulnerability on iot device firmware: A survey. *IEEE/CAA Journal of Automatica Sinica*, 10(1):25–41, 2023.

## Authors’ Profiles



**Rafiul R. Zahid** is currently pursuing his B.Sc. Engg. degree in Internet of Things and Robotics Engineering (IRE) from the University of Frontier Technology, Bangladesh. He has a strong academic and practical foundation in IoT-based system design, embedded programming, and smart automation solutions. He is proficient in multiple programming languages, including C, Python, and MicroPython, and has hands-on experience with ESP32, Arduino. His research interests lie at the intersection of the Internet of Things, Artificial Intelligence, and Machine Learning, with a particular focus on integrating Large Language Models for intelligent data processing and human–machine interaction. He is also exploring emerging topics such as Natural Language Processing, Retrieval-Augmented Generation (RAG).



**Rakibul H. Rakib** is currently pursuing his B.Sc. Engg. degree in Internet of Things and Robotics Engineering (IRE) from the University of Frontier Technology, Bangladesh. He has strong expertise in software development and modern web technologies. He is proficient in multiple programming languages and frameworks, including C, Python, Java, JavaScript, React, React Native, FastAPI and MicroPython. His primary research interest lies in web-based intelligent systems and AI-assisted application development. He is also interested in Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL), with a special focus on integrating AI models into dynamic and responsive web environments.



**Iftekhar Rahman** is a B.Sc. student in Internet of Things and Robotics Engineering at the University of Frontier Technology, Bangladesh. His background combines academic knowledge with hands-on experience in robotics, IoT-based automation, drone projects, and mobile robotics, with emphasis on intelligent control and real-time data communication. He is skilled in Python, Dart, Arduino, and Flutter, and has developed cross-platform mobile applications and IoT solutions. His recent work explores computer vision to enhance robotics and drone systems. His professional interests include IoT, robotics, drones, computer vision, and mobile app development, with a focus on building innovative systems that advance automation and intelligent decision-making.



**Md A. Amin** is currently an undergraduate student at the University of Frontier Technology, Bangladesh (UFTB) pursuing a degree in Internet of Things and Robotics Engineering. He is passionate about innovative technologies and smart system development, with practical experience in IoT devices, sensor integration, and embedded systems. He is skilled in programming languages such as C, Python, and MATLAB, and works with microcontrollers, wireless communication modules, and automation tools. His academic and research interests include smart infrastructure, sustainable technology solutions, machine learning, wireless communication networks, and automation for environmental monitoring and intelligent systems.



**Tanjum R. Akanto** is currently pursuing her M.Sc. in Electrical and Electronic Engineering (EEE) at Khulna University of Engineering and Technology (KUET), from where she also completed her B.Sc. in EEE in March 2020. She is working as a Lecturer in the Department of Electrical and Electronic Engineering (EEE) at Daffodil International University (DIU) since February 2, 2021. Her area of interests is Biomedical Engineering, Image Processing, IoT and Machine Learning.



**Fahmida Ahmed Antara** has been currently employed as Lecturer in the department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh from 2023. She pursued the Bachelor in Science in Electrical and Electronic Engineering from Rajshahi University of Engineering and Technology in 2016, Masters in Science in Biomedical Physics and Technology from University of Dhaka in 2021. She has experience of 8 years of teaching and conducting research in different universities. Her research interest includes biomedical signal processing, machine learning and electric vehicle technology.



**Sadia Enam** obtained her M.Sc. in Electrical and Electronic Engineering (EEE) from Rajshahi University of Engineering & Technology (RUET) in 2022, and her B.Sc. was also in EEE from RUET in 2016. She worked as a lecturer in the Department of EEE at North Bengal International University (NBIU) from October 14, 2016 to November 25, 2022, and at Bangladesh Army University of Engineering & Technology from December 1, 2022 to November 30, 2023. Currently, she is a lecturer in the Department of Internet of Things (IoT) and Robotics Engineering (IRE) at University of Frontier Technology, Bangladesh, starting from January 15, 2023. Her research interest includes antenna simulation and propagation and control theory and control applications.

**How to cite this paper:** Rafiul R. Zahid, Rakibul H. Rakib, Iftekhar Rahman, Md. A. Amin, Tanjum R. Akanto, Fahmida A. Antara, Sadia Enam, "IoT for Industrial Automation: A Review on Industry 4.0 Applications", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.18, No.2, pp. 170-191, 2026. DOI:10.5815/ijieeb.2026.02.11