Volume 12, No. 11, November 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

AI-DRIVEN DECISION MAKING IN INDUSTRIAL IOT NETWORKS: A REVIEW OF TECHNIQUES AND FRAMEWORKS

Mr. Deepak Mehta[1]

[1] Assistant Professor, Department of Computer Sciences and Applications, Mandsaur University, Mandsaur
deepak.mehta@meu.edu.in

Abstract: The integration of the Industrial Internet of Things (IIoT) with AI-based decision-making frameworks is reshaping industrial operations by enabling continuous monitoring, intelligent automation, and context-aware optimization. As IIoT environments produce high-frequency, heterogeneous sensor data, industries increasingly depend on advanced machine learning models and data-driven reasoning systems to extract actionable insights, anticipate system failures, and support real-time operational decisions. Current research shows considerable progress in areas such as predictive maintenance, anomaly detection, and adaptive control, where AI models enhance accuracy, responsiveness, and system reliability. However, several challenges remain, including severe data imbalance, sensor degradation, dynamic operating conditions, limited edge-level computation, and concerns regarding transparency and trust in automated decisions. Addressing these limitations requires scalable AI architectures, interpretable models, and efficient fusion of multivariate sensor signals to support robust decision pipelines. Emerging approaches such as edge-cloud collaborative intelligence, reinforcement-driven industrial control, and federated analytics demonstrate increasing potential to elevate situational awareness and autonomous responses in complex IIoT networks. By synthesizing current developments, technological gaps, and practical constraints, the discussion highlights how AI-enabled decision-making continues to evolve as a central component for building intelligent, efficient, and resilient industrial ecosystems.

Keywords: Artificial Intelligence, Industrial IoT, Edge-Fog-Cloud Computing, Federated Learning, Explainable AI, Decision Making.

1 INTRODUCTION

The physical world is transformed into being digitized and make everything connected. An explosion of smart devices and technologies has allowed mankind to be in constant communication anywhere and anytime. The Internet of Things (IoT) is the network of physical objects devices, instruments, vehicles, home appliances, buildings and other items embedded with electronics, circuits, software, sensors and network connectivity that enables these objects to collect and exchange data [1]. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency and accuracy.

The smart use of IoT in industries, which is named Industrial IoT (IIoT) where IoT is used to develop industrial applications using various sensors and wireless devices. To cater to the high demands and infrastructural needs of industries, IoT is widely used in industry to make an industry a smart one, can be named as a smart factory [2]. This fulfils the demand of the 4th industrial revolution termed as 'Industry 4.0'. IoT and Cyber-Physical Systems (CPS) are key elements of Industry 4.0. Along with IIoT, artificial intelligence, big data, cloud computing, cyber security, system integration, simulation, augmented reality, and additive manufacturing are pillars of industry 4.0. Industry 4.0 and the Industrial Internet of Things (IIoT) are interconnected frameworks that make use of cyber–physical systems and advanced data analytics to enhance industrial operations through autonomous decision-making and real-time optimization [3][4].

AI facilitates real-time data analysis, intelligent decision-making, and predictive analytics in addition to enhancing the security of the IIoT ecosystem against substantial cyber threats. Furthermore, artificial intelligence (AI) and machine learning algorithms play a crucial role in optimizing resource allocation, ensuring grid stability and reliability, and enhancing energy usage planning. The true value of the IIoT can only be fully realized by integrating Artificial Intelligence (AI) models into embedded platforms, including microprocessors and microcontrollers, which underpin the embedded devices and systems commonly used in the industrial environment [5]. Real-time analysis of industrial data is made possible by AI in IIoT decision-making, enabling autonomous, adaptive, and predictive operations. By utilizing machine learning, deep learning, and optimization techniques across distributed industrial environments, it improves productivity, decreases downtime, and facilitates intelligent resource management.

The purpose of this paper is to provide an overview of the current framework and AI-based decision-making techniques in industrial IoT networks, including their applications, limitations, and potential. It makes an attempt to identify problems before outlining potential avenues for further study into scalable, dependable, and real-time AI solutions for the sector.

1.1 Structure of the paper

The structure of this paper is as follows: Section 2 provides an overview of Industrial IoT networks. Section 3 explains AI fundamentals in IIoT. Section 4 presents AI-driven decision-making techniques. Section 5 reviews related literature. Section 6 concludes the study and outlines future research directions for advancing AI-enabled IIoT.

2 ESSENTIALS OF INDUSTRIAL IOT NETWORKS

The network architecture of an Industrial IoT (IIoT) is often multi-layered, namely, perception layer, network layer, middleware, and application layer, which allow easy data gathering, transmission, computing, and service providing. Interoperability and reliable connectivity through protocols such as MQTT, CoAP, Bluetooth, ZigBee, 5G, and other such well-known protocols and standards such as OPC- UA and ISO/IEC 30141 [6]. Even though IIoT systems are beneficial, their disadvantages are poor connectivity, issues related to integrating IT and OT, security vulnerability, data storage requirements, and complexity of analytics. All these are some of the issues that need to be addressed in order to achieve efficient, secure, and scalable industrial automation in the contemporary smart manufacturing industry.

2.1 IIoT Architecture and Component

A four-layer architecture that may be applied to various IIoT systems. It can accommodate the fundamental components of a three-layer IIoT architecture, while also readily expanding this four-layer architecture with additional components to depict a five-layer IIoT architecture with finer granularity. The Figure 1 shows, of a three-layer IIoT architecture, while also readily expanding this four-layer architecture.

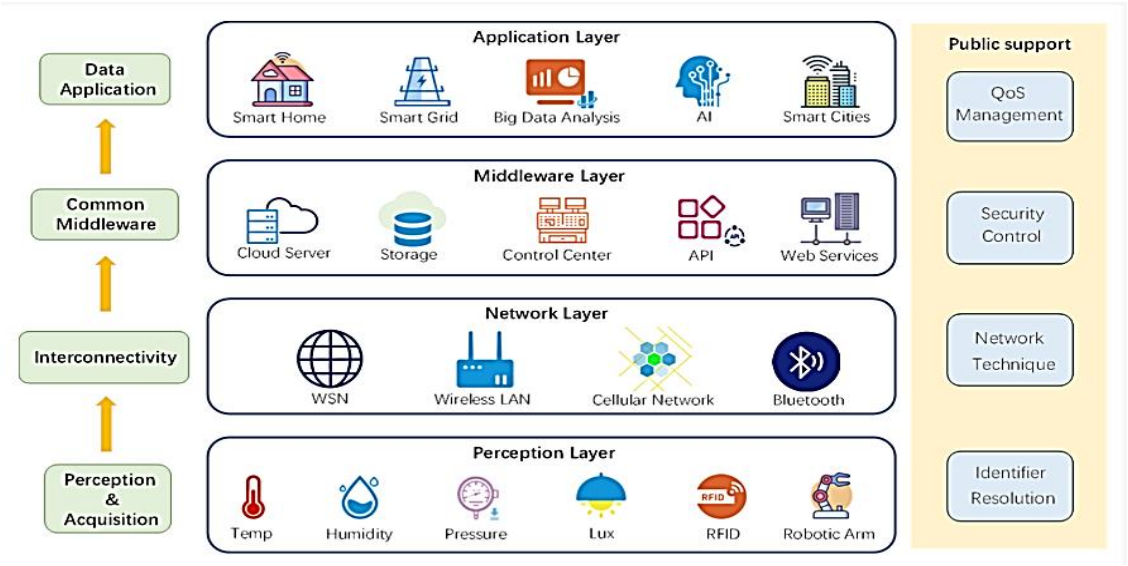

Figure 1: A Four-layer IIoT Architecture

2.1.1 Perception Layer

The perception layer, which includes a variety of sensors for collecting various kinds of human-machine collaborative production context data, is thought to be the lowest physical layer of the IIoT architecture. The perception layer is made up of sensors and actuators that acquire and interpret context data to carry out tasks (e.g., retrieve location and acceleration). A variety of IIoT applications require the perception layer. To connect the physical and cyber worlds, a variety of end devices can be employed at the perception layer. Near Field Communications (NFC), RFID, wireless sensors and actuators, RFID, and some smart devices are examples of typical end devices.

2.1.2 Network Layer

The network layer encapsulates large amounts of protocols (e.g., MQTT, COAP, ZigBee, Ethernet). For the protocols of the IIoT, it can generally be divided into two categories, namely communication protocol (e.g., Bluetooth and ZigBee) and transmission protocol (e.g., High-Speed Ethernet (HSE), Modbus TCP/IP, and ProfiNet), performing secure information sharing. Cloud computing and the Internet are the fundamental components of this layer [7]. Additionally, Internet gateway devices work in this tier by utilizing the most recent communication technologies to deliver network-connected services.

2.1.3 Middleware Layer

This third-level layer, commonly called the support layer, is presented. It offers IIoT systems database and cloud services for the application layer to use further. The middleware layer employs advanced computational techniques to evaluate, process, and store data. It can use cutting-edge technologies such as cloud computing and big data analytics to automatically analyze and compute the

information that has been acquired. As described in the previous section. Middleware has become an effective tool for researchers to achieve interoperability between systems.

2.1.4 Application Layer

The termination layer of the IIoT is another name for the application layer. By preserving data integrity, secrecy, and authentication, this layer performs as the bridge between users and applications. This layer accesses the middleware layer's data and offers multiple services to the users [8]. Additionally, it is integrated with commercial organizations to access smart applications. Using internet-capable devices such as smartphones, tablets, PCs, wearable technology, and many other smart gadgets, users can access the smart services at this layer.

2.2 Communication Protocols and Standards

These protocols are essential for IIoT which enable devices to communicate with each other and with centralized systems to ensure smooth operation across various networks and environments [9]. Below are some of the key protocols:

- **Message Queuing Telemetry Transport (MQTT):** A lightweight protocol ideal for low-bandwidth networks, commonly used in IoT applications where efficiency is critical.
- **Constrained Application Protocol (CoAP):** Designed for constrained devices and low-power networks, especially suitable for IoT applications.
- **Advanced Message Queuing Protocol (AMQP):** Used in more complex environments for reliable messaging between systems.
- **Bluetooth and Zigbee:** Protocols used for short-range communication between IoT devices, with applications in home automation and sensor networks [10].
- **5G and Low Power Wide Area Networks (LPWANs):** Key protocols for large-scale IIoT applications, offering high speed, low latency, and wide area coverage for industrial use.

Standards ensure interoperability between devices and systems in IoT/IIoT environments, which is critical for the seamless integration of new technologies and large-scale deployments [11]. Common IoT/IIoT standards are as follows:

- **International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 30141:** The international standard for IoT reference architecture, ensuring the security, privacy, and reliability of IoT systems.
- **IEEE 802.15.4:** A key standard for low-rate wireless personal area networks, widely used in IoT communication.
- **Open platform communications unified architecture (OPC-UA):** An M2M communication standard commonly used in industrial automation.
- **International Standard for the Integration of Enterprise and Control Systems (ISA-95):** A standard for the integration of enterprise and control systems, particularly relevant to IIoT applications.

2.3 Challenges Faced by Industrial IoT

The physical world is slowly transforming into digital world from ordinary world because of smart technology and devices which allows user and devices to be in constant communication with each other. It's now more efficient because of artificial intelligence, machine learning, etc [12]. This arises new challenges and opportunities for business leaders. There are few challenges that are faced by IIoT are depicted in Figure 2 & explained as follows:.

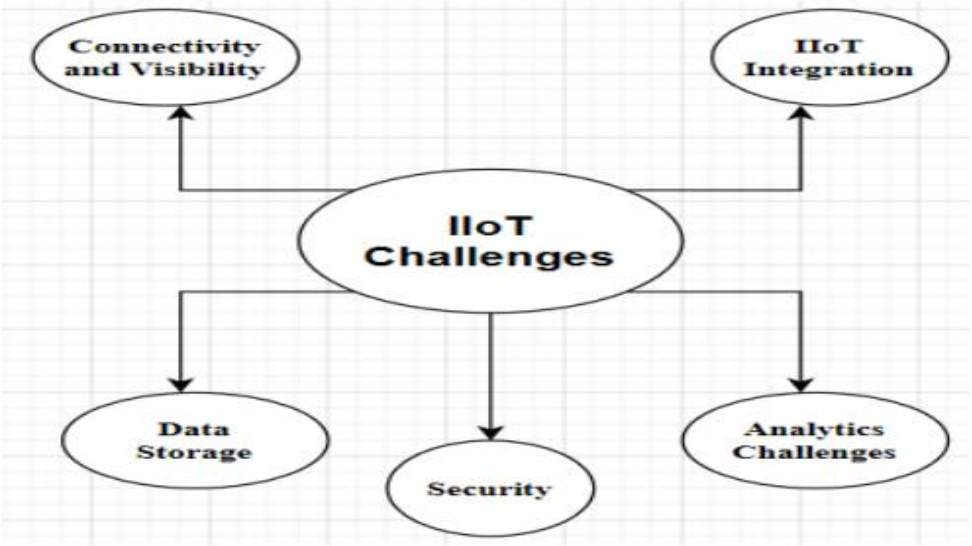

Figure 2: The Challenges in IIoT

- **Connectivity and Visibility:** Due to improper or poor connectivity the critical IIoT-implementation challenges arise. Joining of machine with IIoT is a challenging problem, and it's necessary to ensure that these machines are working at an optimal level and it's important to monitor machines to enhance the production level. Different units are responsible for the proper working of IIoT machines, and there might be a problem of coordination arises as a result of power blackouts, internet outages and physical or technical errors.
- **IIoT Integration: -** Integration of the information technology (IT) is another difficulty faced by the IIoT execution. Integration between these two technologies suffers due to essential connectivity and synchronization.
- **Security: -** As enjoy several comforts from the IoT, must also take care about safety and privacy in smart devices [13]. must give main priority to security while designing the IoT devices. Privacy of personal data and privacy of physical well-being are including in it. Security is the biggest challenge for IIoT technology team since a small or regular threat could disintegrate the whole enterprise.
- **Data Storage: -** Data storage is another major challenge for any company or enterprise. The data which was stored in past are used for the all forecasted activities. Today none of the enterprise uses an old conventional method to tackle data which mostly would be analyzing high-frequency data, observe it, and punctually thrown it away [14]. It is compulsory for any company to adopt proper plan for a secure storage of data before run IIoT in full mode.
- **Analytics Challenges:** It's necessary for Data Analytics partners to include data processing, cleansing, and representation while executing IoT architecture. Enough space for functionality factor is left surely and this factor add real-time or predictive analytics to an IoT solution simply.

3 ROLE OF ARTIFICIAL INTELLIGENCE IN IIOT

In IIoT, Artificial Intelligence (AI) uses techniques such as machine learning, deep learning, or reinforcement learning to enable intelligent decision-making and optimize decision-making through data [15]. AI implementation in IIoT utilizes layers for deployment via edge, fog, and cloud, balancing real-time latency, localized intelligence, and sizeable data processing. Edge nodes provide the ability to acquire and pre-process data, fog nodes allow for the analysis of data at the local regional level, while cloud provides a unified data set for all edge devices for optimization on a more global scale. The AI models deployed with IIoT must be able to provide real-time results, must be lightweight, and must aid in human comprehension, which can be accomplished through a combination of course-grained pruning, quantization, and knowledge distillation.

3.1 AI Paradigms Relevant to IIoT

Artificial Intelligence (AI) plays a critical role in Industrial Internet of Things (IIoT) by enabling intelligent decision-making, predictive insights, and autonomous operations [16]. Various AI paradigms, including machine learning, deep learning, and reinforcement learning, are leveraged to process massive amounts of industrial data from sensors, machines, and networks. These paradigms help optimize production, improve efficiency, and reduce downtime in complex industrial environments.

- **Machine Learning (ML):** Machine learning allows IIoT systems to automatically learn from data rather than relying on explicit programming. By analyzing historical and real-time sensor, device, and operational data [17], ML models can identify patterns, correlations, and anomalies that help in predictive maintenance, process optimization, and intelligent decision-making.
- **Supervised and Unsupervised:** ML approaches can be categorized into three main types. Supervised learning uses labeled datasets to train models for tasks such as quality inspection or fault detection [18]. Unsupervised learning identifies hidden patterns in unlabeled data, useful for clustering devices or detecting unusual behaviors.
- **Deep Learning (DL):** Deep learning extends traditional ML by employing multi-layered neural networks capable of handling large-scale, high-dimensional data. DL can process complex information from IIoT environments, including images from inspection cameras, vibration signals from machinery, and sensor fusion data. Its capability to automatically extract hierarchical features makes it ideal for applications like anomaly detection, predictive maintenance, and process automation.
- **Reinforcement Learning (RL):** Reinforcement learning is particularly suited for dynamic and uncertain IIoT environments. By continuously interacting with machines, robots, or production systems, RL agents learn optimal strategies over time. The reward-punishment mechanism enables systems to adapt to changing conditions, optimize energy consumption, reduce downtime, and improve overall operational efficiency.

3.2 Edge, Fog, and Cloud AI Deployment Models

The architecture for Cloud-Edge AI integration in IIoT follows a layered approach, combining the strengths of both cloud and edge computing. This architecture is designed to optimize real-time data processing, enhance system efficiency, and improve overall industrial automation [19]. It consists of three key players: the edge layer, the fog layer, and the cloud layer, each with distinct roles and responsibilities, as illustrated in Figure 3.

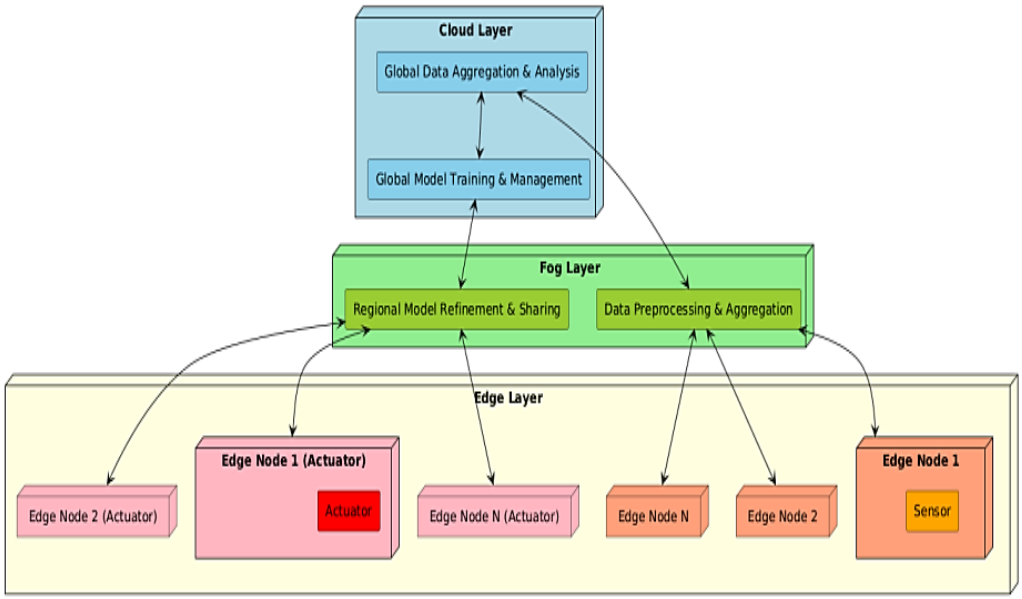

Figure 3: Cloud-Edge AI Architecture for IIoT

3.2.1 Edge Layer

The edge layer is the closest to the physical world, consisting of IIoT devices such as sensors, actuators, and embedded systems that are directly attached to industrial equipment. This layer plays a crucial role in ensuring real-time responsiveness and reducing data transmission overhead by processing data locally. At the edge, data acquisition is performed by sensors that collect raw information, such as temperature, vibration, pressure, and other operational parameters [20]. To improve data quality and minimize noise, local data pre-processing is conducted, including filtering, cleaning, and basic aggregation of sensor readings. This reduces the volume of data that needs to be transmitted to higher layers, saving bandwidth and improving efficiency.

3.2.2 Fog Layer

The fog layer serves as an intermediary between the edge and the cloud, providing additional computational and storage resources closer to the data source. This layer is typically implemented on industrial gateways, local servers, or edge clusters, offering more processing power than edge devices while maintaining lower latency compared to cloud services [21]. One of the primary responsibilities of the fog layer is data aggregation and analysis—collecting information from multiple edge nodes, identifying patterns, and performing regional-level analytics. This helps detect localized trends that may not be apparent at an individual device level.

3.2.3 Cloud Layer

The cloud layer acts as the central hub for large-scale computing, storage, and AI-driven insights. It provides a global perspective of the entire IIoT ecosystem by aggregating data from multiple industrial sites and performing comprehensive analytics [22]. One of its key functions is global data aggregation and analysis, where data collected from thousands of edge and fog nodes is combined to generate insights at an organizational level. This enables companies to monitor overall production efficiency, detect long-term trends, and make data-driven decisions for optimizing operations.

3.3 AI Model Requirements for IIoT

In the case of Industrial IoT, AI models are required to be adjusted to the limits of industrial processes and be highly reliable. Real-time is necessary because most applications of IIoT demand real-time responses daily, including anomaly detection, predictive maintenance and process control, to avoid production downtimes that could lead to quality or safety issues [23]. The low weight is also essential, as most of the IIoT devices, especially edge-based ones, have a weak processing capacity, memory, and energy provisions.

The model pruning, quantization, and knowledge distillation are the techniques that are commonly used to decrease the number of parameters and ensure the level of accuracy. Lastly, interpretability, i.e., being able to make sense of AI decisions, is essential in the industrial context where operators and engineers need to comprehend the rationale of AI decisions in order to be grounded, support trouble shooting, and optimal legal compliance [24]. A trade-off between these three needs allows the implementation of AI systems that can be technically effective and operationally reliable in practice when it comes to IIoT.

4 TECHNIQUES FOR DECISION MAKING IN IIOT

The ultimate objective of integrating AI-enabled smart sensors in IIoT is to facilitate accurate and timely data-driven decision-making. This requires the framework to provide meaningful insights into the operational status of industrial processes, enabling predictive

maintenance, process optimization, and anomaly detection. [25]. To ensure reliable data-driven decision-making, the framework should integrate advanced AI techniques, including machine learning (ML) and deep learning (DL), for processing and analyzing sensor data [26]. ML models can be used for predictive analytics, such as forecasting equipment failures and optimizing resource utilization.

4.1 Deep Learning Integration for Intelligent Decision-Making in IIoT

Deep Learning is considered to be one of the most powerful techniques in the domain of artificial intelligence (AI). The integration of DL methods in smart industries can upgrade the smart manufacturing process into a highly optimized environment by information processing through its multi-layer architecture. DL approaches are very helpful due to their inherited learning capabilities, underlying patterns identification, and smart decision-making. The biggest advantage of DL over conventional ML techniques is automatic feature learning. With this option, there is no need to implement a separate algorithm for feature learning [27]. The deployment of DL techniques can be very effective to perform the types of aforementioned analysis in smart industries.

4.2 Federated Learning for privacy-preserving decision-making

Federated Learning (FL) is a distributed machine learning model that trains local models on the user side and aggregates them with a central manager. FL allows devices to collaboratively train shared models without having to exchange their local private data. FL model training is divided into three phases. First, data are locally collected and trained. Second, the local model is uploaded and aggregated. Finally, the aggregation forms a global model, which is then distributed to local devices [28]. By allowing AI models to be trained cooperatively across dispersed devices without exchanging raw data, federated learning facilitates privacy-preserving IIoT decision-making. This method lowers the risks associated with data exposure while utilizing a variety of real-time industrial datasets to enhance model accuracy and flexibility.

4.3 Explainable AI (XAI) for Transparent Decisions in Industry

Critical processes like production optimization, equipment maintenance, and safety control are frequently impacted by decisions made in industrial IoT environments [29]. Even though AI models, especially deep learning, can produce highly accurate results, it can be difficult to comprehend how decisions are made because of their "black-box" nature. This is addressed by Explainable AI (XAI), which gives managers, engineers, and operators interpretable insights into AI model outputs so they can validate and trust automated decisions. In the IIoT, where stakeholders must validate decision logic prior to execution, XAI is especially crucial for regulatory compliance, fault diagnosis, and risk mitigation. By revealing the logic behind predictions, methods like feature attribution, model-agnostic explainers (like LIME and SHAP), and visualization tools contribute to the transparency of AI systems.

5 LITERATURE REVIEW

This section presents a literature review on AI-driven decision-making in Industrial IoT networks, covering IIoT sensor integration with cloud analytics, distributed TinyML frameworks, agent-based disaster prediction systems, hybrid decision-making models, NF-based communication methods, blockchain applications, and secure IIoT data transmission, highlighting advancements, challenges, and future research directions.

Khan et al. (2025) Industrial Internet of Things (IIoT) networks, essential to modern manufacturing, logistics, and critical infrastructure, face unprecedented cybersecurity challenges. As IIoT networks expand, integrating countless interconnected devices, they are increasingly exposed to cyber threats that exploit system vulnerabilities, jeopardizing data integrity, operational continuity, and safety. Traditional security measures, while effective in standard IT environments, often lack the adaptability and real-time responsiveness needed for IIoT's unique requirements. In response, Artificial Intelligence (AI) has emerged as a transformative solution, offering enhanced detection, prediction, and response capabilities tailored to the complex IIoT landscape. This chapter explores the critical role of AI-driven approaches in advancing cybersecurity for IIoT networks [30].

Jovith et al. (2024) presents the use cases and benefits of IIoT sensor networks for gathering actionable insights and operational data from industrial machinery. These networks might benefit from cloud computing to better manage and analyze the massive amounts of data the produce. It highlights the evolution of conventional industrial landscapes into linked ecosystems that may provide insightful decision-making data. The data for users to use sensor networks to monitor equipment and improve productivity. Reducing equipment downtime by 30% and increasing operational efficiency by 20% are both made potential by combining Industrial IoT sensor networks with cloud analytics. With an 80% success rate, maintenance techniques save a ton of money and make things more efficient [31].

Yuan and Eddie Law (2024) have designed a set of function calls for enabling the distributed deployments of neural network models across multiple resource-constraint sensing devices in DTSN. It results in facilitating autonomous data analysis and decision-making while reducing reliance on Cloud services. With the popular Bluetooth technology, Bluetooth mesh networks are utilized for inter-device communications and support dynamic memory management without compromising model precision. Their model offers on-device model training, fast deployment, and provides inferences at an IoT gateway node. The experiment results indicate that the DTSN achieves high accuracy in both regression and classification tasks. It demonstrates the feasibility of training and inference on embedded devices. [32].

Chekati, Riahi and Moussa, (2024) introduces the SADM-Smart Object framework, a cutting-edge, agent-based conceptual and methodological IoT framework designed for self-adaptation and decision-making, specifically applied to the context of natural flood disasters. The primary objective of this framework is to monitor key climate indicators such as rainfall, humidity, temperature, pressure, and water levels and discern their temporal correlations to enhance flood prediction accuracy. It offers a strong layered architecture complemented by efficient tools for constructing IoT systems, integrating machine learning classifiers for data classification, and agent-based approaches for decision-making [33].

Cherif and Frikha (2023) aims to investigate the significance of IoT systems in various domains, focusing specifically on the industrial application, emphasizing the pivotal role of reliable and efficient device connectivity within such systems. To address the challenges posed by uncertainty and ambiguity in real-life scenarios, proposed the integration of rough set theory with multi-criteria decision-making approaches to evaluate and classify IoT devices in the industrial domain. The utilization of the proposed hybrid multi-criteria group decision-making approach allows to effectively model and handle the uncertainty arising from expert assessments [34].

Gunasekaran et al. (2023) intends to create an NF-based communication system for IIoT platforms to leverage those benefits. The proposed model includes smart decision-making procedures to deal with communication issues. Compared with the many methods already in use, the suggested mechanism's functional viability in the automated system is found to be optimal. Outcomes from simulations reveal that the suggested method has improved the accuracy and communication reliability of the IIoT platforms in comparison with the previous methods. Aside from these, the suggested model keeps the throughput of the local automation unit at 96.03% and the throughput of the production hall at 95.58% on average while maintaining the lowest average PLR of about 26.48% [35] .

Table 1 presents a summary of the literature review, highlighting each study's focus, approach, key findings, challenges, and proposed future directions.

TABLE I. SUMMARY OF RESEARCH GAPS IN AI-BASED DECISION-MAKING FOR INDUSTRIAL IOT (IIOT) SYSTEMS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Khan et al. (2025)	Cybersecurity challenges in Industrial IoT (IIoT) networks	AI-driven security approaches for IIoT environments	Demonstrates that AI enhances detection, prediction, and dynamic response for IIoT cyber threats; highlights limitations of traditional security in real-time IIoT settings	Difficulty integrating AI models into resource-constrained IIoT devices; high data heterogeneity; real-time adaptation issues	Develop lightweight AI algorithms for edge-based threat detection; explore federated learning for secure distributed analytics; enhance real-time anomaly detection systems
Jovith et al. (2024)	Use cases and benefits of IIoT sensor networks integrated with cloud analytics	IIoT sensor networks combined with cloud-based data analysis	Significant improvements in productivity and reduced downtime (30%); operational efficiency increased by 20%; maintenance techniques achieve 80% success rate	High dependency on cloud platforms; latency and bandwidth limitations; security/privacy concerns in cloud-based IoT	Move toward hybrid edge-cloud analytics; explore privacy-preserving data processing; develop autonomous maintenance models
Yuan & Eddie Law (2024)	Distributed neural network deployment in Distributed Tactical Sensor Networks (DTSN)	On-device model training using Bluetooth mesh networks for distributed inference	Achieves high accuracy in regression/classification tasks with reduced reliance on cloud services; supports dynamic memory management	Limited computational resources on sensing nodes; communication constraints in mesh networks; energy consumption issues	Develop ultra-efficient neural architectures; optimize distributed training strategies; improve mesh communication protocols for scalability
Chekati, Riahi & Moussa (2024)	Agent-based IoT framework for natural flood disaster monitoring	SADM-SmartObject: layered architecture with ML-based classification and agent-driven decision-making	Effective in monitoring climate indicators and improving flood prediction accuracy; strong conceptual framework for IoT-based decision systems	Lack of real-world deployment validation; data noise and environmental unpredictability; integration complexity with diverse sensors	Advance real-world pilot studies; incorporate deep learning for improved prediction; expand framework to multi-hazard disaster management

Cherif & Frikha (2023)	Evaluating and classifying industrial IoT devices under uncertainty	Hybrid Rough Set Theory + Multi-Criteria Decision-Making (MCDM)	Effectively models uncertainty in device classification; improves assessment accuracy in industrial IoT systems	Limited scalability for large-scale IoT networks; computational complexity of hybrid models; reliance on expert input	Develop automated uncertainty-aware evaluation tools; enhance scalability with big-data methods; integrate AI-driven decision support
Gunasekaran et al., (2023)	NF-based communication model for IIoT platforms	Smart decision-making communication architecture improving reliability and throughput	Achieves ~96% throughput and improves communication reliability; reduces packet loss ratio to ~26.48%	PLR still relatively high; limited adaptability under extreme network stress; lacks hardware-level validation	Further optimize reliability mechanisms; integrate AI-based network optimization; validate model via real industrial testbeds

6 CONCLUSION AND FUTURE WORK

The combined forces of IIoT connectivity and AI-based decision-making are increasingly defining the next generation of industrial automation, offering enhanced precision, predictive insight, and operational intelligence. Yet, real industrial settings reveal persistent challenges related to fluctuating sensor quality, unstable data distributions, and the difficulty of validating decisions produced by complex AI models. Strengthening decision reliability requires models that operate effectively under uncertainty, adapt to shifting environments, and provide transparent reasoning that engineers can trust. Future directions point toward more advanced edge-AI pipelines, where local processing supports fast, autonomous decisions without relying heavily on centralized nodes. Reinforcement learning, adaptive rule-based agents, and digital twin-guided analytics are expected to play greater roles in enabling systems that learn continuously from operational feedback. Expanding research on trustworthy AI, particularly explain ability and robust decision verification, will help reduce the risks associated with automated industrial actions. Furthermore, federated and distributed learning approaches offer pathways for training intelligent models across multiple industrial sites while preserving data privacy and respecting operational constraints. Collaborative efforts across AI researchers, control engineers, and industry practitioners will be essential for transitioning from experimental prototypes to fully dependable, scalable, and ethically aligned IIoT decision-making solutions.

REFERENCES

[1] S. Munirathinam, “Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT),” in *Advances in Computers*, 1st ed., vol. 117, no. 1, Elsevier Inc., 2020, pp. 129–164. doi: 10.1016/bs.adcom.2019.10.010.

[2] S. Deshpande and R. M. Jogdand, “A Survey on Internet of Things (IoT), Industrial IoT (IIoT) and Industry 4.0,” *Int. J. Comput. Appl.*, vol. 175, no. 27, pp. 20–27, Oct. 2020, doi: 10.5120/ijca2020920790.

[3] V. Prajapati, “Improving Fault Detection Accuracy in Semiconductor Manufacturing with Machine Learning Approaches,” *J. Glob. Res. Electron. Commun.*, vol. 1, no. 1, pp. 20–25, 2025.

[4] M. I. Joha, M. M. Rahman, M. S. Nazim, and Y. M. Jang, “A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application,” *Sensors*, vol. 24, no. 23, 2024, doi: 10.3390/s24237440.

[5] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, “Toward Edge-Based Deep Learning in Industrial Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4329–4341, 2020, doi: 10.1109/JIOT.2019.2963635.

[6] O. Peter, A. Pradhan, and C. Mbohwa, “Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies,” *Procedia Comput. Sci.*, vol. 217, pp. 856–865, 2023.

[7] V. Shah, “Networking Challenges in IoT to Deployment of TCP / IP to 6LoWPAN for Next Gen Network System,” *KOS J. Sci. Eng.*, vol. 1, no. 1, pp. 1–8, 2024.

[8] J. Leng *et al.*, “Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions,” *Machines*, vol. 10, no. 10, 2022, doi: 10.3390/machines10100858.

[9] S. Thangavel, A. Kotiyal, A. Thomas, H. Patil, S. Kulkarni, and N. L, “Robust Authentication Protocols for IoT Devices in High-Density Networks,” in *2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC)*, 2024, pp. 1–7. doi: 10.1109/ICDSCNC62492.2024.10939350.

[10] G. Sarraf, “Resilient Communication Protocols for Industrial IoT : Securing Cyber- Physical-Systems at Scale,” *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 694–702, 2021, doi: 10.14741/ijcet/v.11.6.14.

[11] F. Qiu *et al.*, “A Review on Integrating IoT, IIoT, and Industry 4.0: A Pathway to Smart Manufacturing and Digital Transformation,” *IET Inf. Secur.*, vol. 2025, no. 1, 2025, doi: 10.1049/ise2/9275962.

[12] H. Jaidka, N. Sharma, and R. Singh, “Evolution of IoT to IIoT: Applications & Challenges,” *SSRN Electron. J.*, 2020.

[13] K. Seetharaman, “Incorporating the Internet of Things (IoT) for Smart Cities: Applications, Challenges, and Emerging Trends,” *Asian J. Comput. Sci. Eng.*, vol. 08, no. 01, pp. 8–14, 2023, doi: 10.22377/ajcse.v8i01.199.

[14] S. F. Tan and A. Samsudin, “Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey,” *Sensors*, vol. 21, no. 19, 2021, doi: 10.3390/s21196647.

[15] R. Q. Majumder, "Machine Learning for Predictive Analytics : Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, 2025.

[16] S. Garg, "Next-Gen Smart City Operations with AIOps & IoT : A Comprehensive look at Optimizing Urban Infrastructure," *J. Adv. Dev. Res.*, vol. 12, no. 1, 2021, doi: 10.5281/zenodo.15364012.

[17] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[18] G. Czeczot, I. Rojek, D. Mikołajewski, and B. Sangho, "AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes," *Electronics*, vol. 12, no. 18, 2023, doi: 10.3390/electronics12183800.

[19] R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, pp. 503–514, May 2023, doi: 10.48175/IJARSCT-11979B.

[20] Y. Wu, "Cloud-edge orchestration for the Internet of Things: Architecture and AI-powered data processing," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12792–12805, 2020.

[21] V. Kumbhar, A. Shende, P. Tamhankar, Y. Raut, and A. Mangore, "A State-of-the-Art 360° Run-Down of Cloud, Edge, Dew, and Fog Computing," in *Modelling of Virtual Worlds Using the Internet of Things*, 2024, pp. 133–173. doi: 10.1201/9781003480181-6.

[22] S. Johnson, "Cloud-Edge AI Integration for Real-Time Data Processing in Industrial Internet of Things (IIoT)," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 2, no. 3, pp. 9–16, 2021, doi: 10.63282/3050-9416.IJAIBDCMS-V2I3P102.

[23] S. Amrale, "Anomaly Identification in Real-Time for Predictive Analytics in IoT Sensor Networks using Deep," *Int. J. Curr. Eng. Technol.*, vol. 14, no. 6, pp. 526–532, 2024, doi: https://doi.org/10.14741/ijcet/v.14.6.15.

[24] P. Dini, L. Diana, A. Elhanashi, and S. Saponara, "Overview of AI-Models and Tools in Embedded IIoT Applications," *Electronics*, vol. 13, no. 12, 2024, doi: 10.3390/electronics13122322.

[25] M. Kovacs, "AI-Enabled Smart Sensors for Industrial IoT: A Secure and Scalable Framework for Data-Driven Decision Making," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 2, no. 4, pp. 20–33, 2021, doi: 10.63282/3050-9416.IJAIBDCMS-V2I4P103.

[26] S. Dodda, N. Kamuni, P. Nutalapati, and J. R. Vummadi, "Intelligent Data Processing for IoT Real-Time Analytics and Predictive Modeling," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 649–654. doi: 10.1109/ICoDSA67155.2025.11157424.

[27] S. Latif *et al.*, "Deep Learning for the Industrial Internet of Things (IIoT): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions," *Sensors*, vol. 21, no. 22, 2021, doi: 10.3390/s21227518.

[28] F. Hongbin and Z. Zhi, "Privacy-Preserving Data Aggregation Scheme Based on Federated Learning for IIoT," *Mathematics*, vol. 11, no. 1, 2023, doi: 10.3390/math11010214.

[29] P. Dimple, "Explainable Artificial Intelligence (XAI) for industry applications : Enhancing transparency , trust , and informed decision-making in business operation Dimple Patil," no. November, 2024.

[30] Z. U. Khan, S. Taj, F. Khan, T. Jamil, A. Muhammad, and J. Khan, "AI Driven Cybersecurity for Industrial IoT Networks," in *Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defenses*, 2025, pp. 55–90. doi: 10.4018/979-8-3373-0583-7.ch003.

[31] A. A. Jovith, C. S. Ranganathan, S. Priya, R. Vijayakumar, R. Kohila, and S. Prakash, "Industrial IoT Sensor Networks and Cloud Analytics for Monitoring Equipment Insights and Operational Data," in *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, 2024, pp. 1356–1361. doi: 10.1109/ICCSP60870.2024.10543619.

[32] Z. Yuan and K. L. Eddie Law, "Distributed TinyML on Resource-Constrained IoT Sensor Networks," in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, IEEE, Nov. 2024, pp. 457–462. doi: 10.1109/WF-IoT62078.2024.10811277.

[33] A. Chekati, M. Riahi, and F. Moussa, "Flood Disaster Management using SADM-SmartObject: An Agent-Based IoT Framework for Sensing, Data Classification, and Decision Making," in *2024 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2024, pp. 1–7. doi: 10.1109/ICT-DM62768.2024.10798957.

[34] M. R. Cherif and H. M. Frikha, "IoT Device Connectivity Selection Using a Hybrid Multi-Criteria Group Decision-Making Approach," in *2023 International Conference on Decision Aid Sciences and Applications (DASA)*, 2023, pp. 436–440. doi: 10.1109/DASA59624.2023.10286610.

[35] K. Gunasekaran, V. V. Kumar, A. C. Kaladevi, T. R. Mahesh, C. R. Bhat, and K. Venkatesan, "Smart Decision-Making and Communication Strategy in Industrial Internet of Things," *IEEE Access*, vol. 11, pp. 28222–28235, 2023, doi: 10.1109/ACCESS.2023.3258407.

