IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques

Ruchi Patel
Independent Researcher
rpnilkanth@gmail.com

Abstract: *The IIoT is revolutionizing contemporary industry by facilitating intelligent decision-making and real-time data sharing through networked systems and devices. An in-depth examination of the communication protocols and edge computing architectures vital to IIoT applications is provided in this study. Based on delay, it assesses MQTT, CoAP, HTTP, DDS, and AMQP, which are important protocols, bandwidth efficiency, reliability, and security to determine their suitability for diverse industrial scenarios. Additionally, it examines the integration of edge computing to offload processing from centralized cloud systems, thereby reducing latency and improving scalability. The study also explores enablers such as Automated Guided Vehicles (AGVs), Rule-Based Path Allocation (RBPA), and RFID, along with critical aspects including routing, task scheduling, data storage, and cybersecurity in edge-enabled IIoT networks. Their findings underscore the importance of protocol selection and edge orchestration in building resilient, interoperable, and efficient IIoT infrastructures. This study concludes with discussions on open challenges and future directions for standardization and intelligent protocol adaptation in edge-centric IIoT ecosystems.*

Keywords: Industrial Internet of Things, Message Queuing Telemetry Transport, Automated Guided Vehicle, Robot-Based Process Automation, Communication Protocols, MQTT, CoAP, DDS, AMQP, AGV, Task Scheduling.

I. INTRODUCTION

The IoT is a dynamic network that enables cost-effective, scalable, and reliable ecosystems for diverse domains, including smart cities, consumer devices, industrial systems, vehicular networks, multimedia applications, and 5G mobile systems. From a communications perspective, the IoT platform typically leverages TCP/IP-based networks and standardized communication protocols to interconnect devices and ensure seamless information exchange [1]. These protocols include AMQP 1.0, MQTT, CoAP, XMPP, and lightweight data formats such as JSON.

In the IoT ecosystem, a wide range of heterogeneous devices with unique identifiers communicate across various transmission mediums to enable dynamic, real-time information interaction [2][3]. As a result of IoT technology being used in the industrial sector, of the IIoT, a new paradigm focused on enhancing system-level interoperability, resource optimization, and autonomous process execution.

IIoT serves as the technological foundation for Industry 4.0, Smart Manufacturing, and Smart Factories, where M2M communication, distributed intelligence, and flexible automation are prioritized [4]. In this decentralized industrial landscape, systems are expected to handle mission-critical data transmission with low latency, high reliability, robust security, and deterministic behavior. Technologies such as IEEE 802.11ah have recently gained traction in enabling M2M communication in IIoT edge scenarios, due to their energy efficiency and long-range capabilities.

Nevertheless, industrial communication infrastructures still rely heavily on proprietary and vendor-specific protocols, especially in SCADA-like systems, which results in closed-loop architectures and hinders interoperability [5][6]. The integration of modern Surpassing these constraints relies heavily on communication protocols used at the edge of industrial networks, particularly as edge devices need to facilitate secure connection with centralized systems, local

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

decision-making as well as real-time data analysis.

To meet the stringent communication requirements of IIoT environments, particularly at the edge, optimizing communication protocols is essential. This involves addressing trade-offs between bandwidth efficiency, latency, computational overhead, power consumption, and data security [7][8]. Several recent efforts have focused on developing lightweight protocols, cross-layer optimization strategies, AI-based protocol selection, and adaptive middleware architectures that can dynamically adjust to industrial workload conditions.

A. Structure of the Paper

The structure of the document that follows is as follows: Section II discusses Edge computing for industrial IoT, and Section III provides the communication protocols for IOT. Section IV provides a cutting-edge edge computing technology in IoT. Section V provides the Literature Review on IoT Edge Networks. At last, Section VI serves as the paper's conclusion.

II. EDGE COMPUTING FOR INDUSTRIAL IOT

In IIOT Edge Computing serves a vital role, as this fast processing and informative and automatic decision-making assist with the continuous flow of the production line, while cloud and enterprise applications are mainly used for dictating procedures and long-periods of time monitoring & learning [9][10]. The goal of designing an industrial robot is to create a versatile administrator with the ability to reprogram its actions in order to transport various goods, objects, and equipment. It may change similarly to the errand, which also receives important data and moves intelligently as a result.

B. Automated Guided Vehicle

In the traditional industrial machinery, such as AGVs and industrial robots, has traditionally adhered to a predetermined set of rules. These devices can transition to a digital tool during the procedure [11][12][13]. One practical option for managing the movement of various objects is the Automatic Guided Vehicle, which is both user-friendly and widely used. Particularly in big and medium-sized businesses, it requires direction when dealing with situations like crucial automation on the factory floor [14][15]. In order to handle these unforeseen situations, the AGV must receive extremely careful instructions, such as a format change for different scenarios.

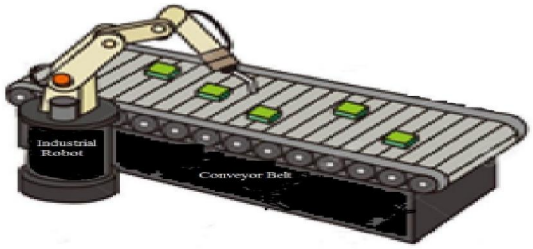

Fig. 1. Autonomous Robots

Therefore, this work offers a fresh approach for the robots depicted in Figure 1, specifically for AGV, to ensure its ongoing adaptability in complex situations.

C. Intelligent AGV and RBPA

The deployment of industrial robots and automated guided vehicles in a shop floor setting presents a few challenges. For the most part, robot-guided vehicles have been utilized for internal transit and assembly, as well as for the handling of materials and items. Although this could be the best case scenario, in reality, there are a number of automated switchovers, and certain processes require human intervention [16][17][18]. Computerized working methods will increase the effectiveness and quality, and RBPA offers innovative solutions for all kinds of organizations (Figure 2).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

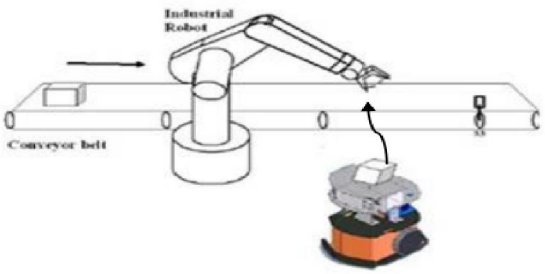

Fig. 2. Integration of AGV and RBPA

An "Autonomous Robot" or programming is organized using the advanced technique known as RBPA to transform current applications for managing the product. From a business standpoint, it is altering their thought process.

Therefore, by eliminating repeated operations, it offers remarkable enhancements in precision, processing time, and heightened efficiency. An active RFID-enabled AGV is essential to their suggested project [19][20]. RFID is used for product identification, control over movement and guidance. To convey data, it employs radio frequency waves with a certain frequency. Thus, this study's primary focus is on the planning procedure for an RFID-enabled AGV solution inside the Self-Configurable IIoT framework.

III. COMMUNICATION PROTOCOLS FOR INTERNET OF THINGS

Communications and information technology, or ICT, is predicted to revolutionize the way that information is transferred between people, things, and other people. People may connect with smart gadgets, share information, and make decisions for them. "Connectivity for anything" is the name given to this revolutionary technology. Anywhere, at any moment, it can connect. There are significant limitations despite the vast number of smart devices in the IoT ecosystem [21][22]. Among these limitations include processing capacity, storage space, low power life, and radio range. IoT communication protocols are often divided into two categories, as seen in Figure 3: (1) short-range networks and (2) LPWAN.

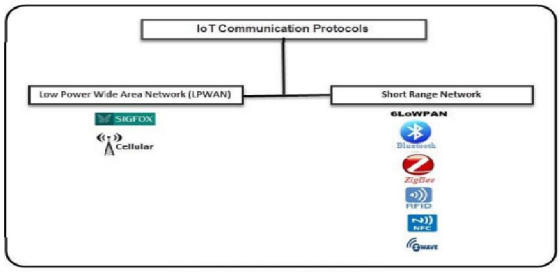

Fig. 3. IoT Communication Protocols

A request/reply interaction paradigm is provided by REST HTTP and CoAP, while MQTT and AMQP, and DDS implement a publish/subscribe approach. For message delivery, the MQTT, AMQP, and QoS functionality provided by CoAP protocols is quite limited. MQTT and AMQP provide three distinct QoS levels, but only two CoAPs allow the delivery of request and reply messages. The underlying transport protocols of REST HTTP and XMPP provide quality of service (QoS) [23]. However, DDS offers a thorough set of QoS guidelines.

A. Hypertext Transport Protocol (HTTP)

This protocol, which is used daily by web developers, is the protocol that works best with the current network infrastructure and serves as the foundation for the client-server architecture of the Web [24]. As seen in Figure 4, HTTP/1.1 is now the most used version of this protocol [25][26]. A client sends an HTTP request message to a server, which replies with a response message that, if the request was granted, contains the resource that was requested. This process is known as request/response messaging.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

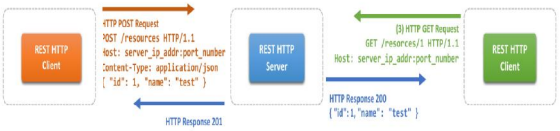

Fig. 4. REST HTTP Interaction Model

REST is a method for building web services that adheres to a specific architectural style to specify how various components interact, and has recently been linked to HTTP. Since RESTful Web services are so popular, a lot of effort has been made to combine REST and HTTP in order to incorporate incorporating this design into IoT-based solutions [27][28].

B. Constrained Application Protocol (CoAP)

It was created by the Core working group of the IETF to be utilized in devices with limited processing power. Its usage of the tried-and-true REST architecture is one of its most distinctive features, much like HTTP. Similar to REST HTTP, CoAP supports the request/response paradigm with this functionality, particularly in contexts with constraints. Since CoAP is regarded as a lightweight protocol, it has a lower overhead than many other protocols since all methods, headers, and status codes are encoded in binary [29][30]. Additionally, it uses a simpler UDP transport protocol rather than TCP, which lowers overhead even more.

C. Message Queue Telemetry Transport Protocol (MQTT)

One of the publish-subscribe model-based lightweight communications protocols, like MQTT, is appropriate for devices with little bandwidth and high latency, as well as devices operating under less-than-optimal network connection conditions. For the IoT, IBM released, as seen in Figure 5, MQTT and OASIS accepted its most recent version, MQTT v3.1. It is often suggested as the preferable communication method for the Internet of Things because to its ease of use and reduced message header size when compared to other messaging protocols.

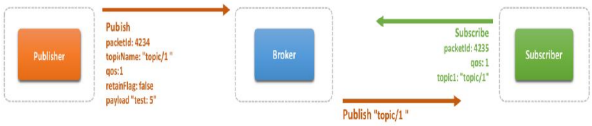

Fig. 5. MQTT Interaction Model

MQTT is reliable because it uses the TCP transport protocol to function. MQTT is one of the most used protocols. Its smaller header and much reduced power consumption make it a viable solution in constrained settings compared to other dependable protocols like HTTP.

D. Data Distribution Service (DDS)

DDS, according to the OMG, is a publish-subscribe interaction paradigm-based real-time data-centric interoperability standard. Since DDS is peer-to-peer and decentralized, it is independent of the broker component, in contrast to some other publish-subscribe protocols. Through peer-to-peer communication over the data bus, DDS allows publishers and subscribers to share data asynchronously according to their interests. Because there isn't in addition to lowering the possibility of a single point of failure for the whole system; therefore, the absence of a broker increases system reliability.

Even if no subscribers are interested, a publisher can still disseminate data since the two communication sides are not connected. As the publishers don't ask who uses their data, the consumption of the data is essentially anonymous. Consequently, DDS makes it possible for an architecture in which all participating nodes have a consistent understanding of the data value [31].

E. Advanced Message Queueing Protocol (AMQP)

A standard protocol that follows the publish-subscribe model of OASIS is AMQP. Regardless of the underlying designs

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 19, May 2023 Impact Factor: 7.301

of various systems and applications, its objective is to increase their interoperability. Its original purpose was to provide a non-proprietary method that might handle a lot of message exchanges that could happen in a system quickly for business communications. Because it enables message interchange across systems with different languages built into them, this AMQP interoperability feature is important and might be particularly helpful in heterogeneous systems.

Similar to MQTT, AMQP offers three distinct QoS levels and relies on TCP for dependable transmission [32]. Lastly, supplementary security methods are offered by the AMQP protocol, which uses Data security measures, including using SASL for authentication and the TLS protocol for encryption. Despite all of its advantages, AMQP's main drawback in IoT-based ecosystems is seen it is a somewhat heavy protocol due to its comparatively high power, processing, and memory requirements. This protocol works best in areas of the system that have higher processing capacity and are not constrained by latency or bandwidth.

IV. STATE OF THE ART OF EDGE COMPUTING IN IOT

Data processing, networking, and sensor technologies are used by IIoT edge computing to connect many components, resulting in various breakthroughs in a number of areas that significantly impact edge computing performance [6][9]. For example, the routing strategy will have a direct impact on the delay performance, and data gathered by many Moving sensors between the Far-Edge Layer and the Cloud Application Layer, Mid-Edge Layer, and Far-Edge Layer is required[33]. Task scheduling is the process of allocating activities to be completed on various devices in order to maximize idle resources and increase computing efficiency.

The effectiveness of scheduling plans has an impact on how efficiently tasks are completed. Additionally, the timeliness and accuracy of the decision are directly tied to data storage and analytics, the systematism and extensibility of Standardization have a direct influence on IIoT edge computing technologies, and edge secure techniques and algorithms have a direct impact on the dependability of edge networks or edge systems. As a result, this section provides a thorough examination of the aforementioned advancements.

A. Routing

In the IoT, extensive Sensor networks that collect enormous amounts of real-time data and have complex topological topologies are used to improve the intelligence of process control and the flexibility of industrial operations. By using edge computing in the IIoT, request-response times can be shortened by processing preliminary sensory data close to the sensor nodes [34]. However, the cost and latency may be further reduced by effective and reliable routing techniques. In the industrial sector, edge computing in IIoT requires research on routing.

The edge nodes' location and energy are the primary design factors for several standard routing systems, which are often appropriate when IIoT edge nodes are energy-constrained and immobile [35]. The N-SEP, for instance, takes into account all of the sensor node characteristics in the fog environment, including the base station's distance, the network's heterogeneity, the energy left, the cluster head distance, etc.

Furthermore, certain traditional routing strategies are used to investigate how to create routing pathways and enhance routing stability when edge IIoT nodes are very mobile. Typically, these routing algorithms may be used in situations where the nodes include smart manufacturing robots, mobile users, and automobiles. Using the IGR protocol, for example, the source vehicle chooses the next junction based on a scoring function that considers the intersection's density and the vehicle's position. The data packet is then forwarded from this junction to the next junction using enhanced greedy routing.

B. Task Scheduling

The top design of resources and data is the subject of task scheduling. This entails choosing how resources are allocated and used, as well as how data should be sent throughout the network [36]. The undervalued processing power may be combined with the many sensors, Access points, switches, routers, base stations, and gateways are used in IIoT-enabled industrial processes.

The associated data compute, storage, and forwarding capabilities vary due to the vast variances in hardware setups and software functionalities. Effectively managing the problems includes integrating compute outputs, minimizing energy

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

usage, decreasing latency, and guaranteeing load balancing while managing many edge computing nodes and efficient task distribution.

C. Data Storage and Analytics

Big data is without a doubt at the heart of IIoT. The major sources of industrial big data include enterprise external data produced by numerous devices and time-consuming business procedures, equipment and object data, and production and operational business data. Large data's "4V characteristics" in general Industrial big data is therefore valuable, varied, accelerated, and large in volume. It also contains a number of unique features, including as closed-loop, precision, and real-time. Research on the distributed processing and storing of industrial big data is necessary for edge computing in the IIoT.

D. Security

The IIoT can benefit from the reduction of transmitted data volume through the use of edge computing, but traditional security protection techniques are unable to meet edge computing's protection requirements because it is impossible to properly account for security issues at the beginning of the design. Furthermore, the threats to data, networks, and applications have risen as a result of the integration of several technologies [33].

Effective edge IIoT network protection is provided by many network attack detection and defines technologies. The LDNAD method detects critical IIoT device assaults in the fog using ML techniques [37]. Edge network security is improved by precisely detecting and addressing network assaults. The fog-based HD-IDS deploys IDS across several network levels to defend power grid smart meters from fake data injection attacks.

E. Standardization

The natural fusion of edge computing, IoT, and industrial Internet technologies is known as IIoT edge computing. It entails the intricate application and integration of system platforms, communication, hardware, and software. Establishing standards is a prerequisite for the widespread adoption, use, and IIoT support for edge computing.

The only organization now is the IIC, which publishes white papers about IIoT edge computing. These articles outline the benefits of edge computing in addition to offering helpful advice discussing the framework and components required to use edge computing in the IIoT. It highlights important use-case issues, outlines the edge computing architecture's potential, and focuses on model deployment and implementation strategies for edge computing in diverse horizontal processes.

F. Comparison matrix

A number of technical factors must be considered during the creation and implementation of IIoT systems in order to guarantee dependable, efficient, and scalable performance. These parameters include bandwidth, reliability, latency, scalability, energy efficiency, and QoS support. Each plays a pivotal role in determining how well an IIoT network performs under specific operational constraints and application requirements. Table I presents a comparative analysis of these parameters, highlighting their respective pros, cons, and importance within the IIoT context.

1. Bandwidth

Application developers take into account IoT device constraints, bandwidth restrictions, energy use, etc., under a variety of unfavourable circumstances. Selecting the communication protocol to be utilised for data transmission or reception is a crucial topic that requires attention [38]. However, a lack of bandwidth can limit the speeds at which data can be transmitted, which can influence the overall efficiency of the network and the capacity of IoT networks to handle high-throughput applications.

2. Reliability

However, a system's or product's performance over a given period of time is referred to as reliability. This distinction between the two words is crucial, particularly when it comes to ensuring that a system or device will continue to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

operate at a sufficient level over time [39]. Essentially, it can assess IoT quality, but this won't provide us with any guarantees on the deployment's ongoing performance.

3. Latency

The term "latency" describes the interval of time between a message's transmission by the sender and its reception by the recipient [5]. There should be a limit on all forms of delays, including processing, propagation, transmission, and computing, as some IIoT applications are time-sensitive.

4. Scalability

A network that allows for the addition of new devices or services without impairing network performance is known as a scalable IoT low-power network. Given that there are billions of resource-constrained devices in the present deployment of IoT low-power networks [40], the scalability criterion must be met to prevent subpar network performance.

5. Energy efficiency

One area where IIoT will continue to support sustainability projects is energy efficiency. Wireless sensors are included in contemporary IoT systems to collect data for process monitoring and operation management across many applications [41]. Energy efficiency must be taken into account while developing IoT devices in order to ensure their long-term performance.

6. Quality of service (QoS) support

The evaluation of a service's entire performance to gauge user satisfaction is known as QoS. These metrics—packet loss, latency, bandwidth, and network end-to-end delay—are used to assess its performance [42]. In specifics, the kind of application determines the QoS level in IoT low-power networks. For instance, some Internet of Things applications, like smart metering, can withstand delays, but not others, like forest fire detection. Therefore, it is crucial to take the QoS requirement into account while constructing the network in order to prevent having bad network performance.

Table 1: Comparison Matrix of Key IIoT Network Parameters

Parameter	Pros	Cons	Importance in IIoT
Bandwidth	• Enables efficient data transmission • Supports streaming and data-intensive applications	• Limited by low-power protocols • Can restrict high-throughput communication • Protocol selection is complex	Critical for ensuring sufficient data flow, especially in multimedia, real-time analytics, and industrial automation
Reliability	• Ensures system performance over time • Facilitates fault-tolerant design	• Quality doesn't guarantee continued success • Susceptible to failures or degradation over time	Fundamental for continuous, dependable operation of IIoT devices in harsh or remote industrial environments
Latency	• Enables near-instantaneous response • Essential for control and feedback loops	• Affected by delays in processing, transmission, and propagation	Crucial for real-time applications like robotics, automated manufacturing, and emergency response
Scalability	• Allows addition of new devices/services without degrading performance	• Managing billions of devices is complex • Risk of poor performance in dense deployments	Important for supporting future growth and device expansion in smart factories, cities, and infrastructure
Energy	• Increases battery life	• May reduce processing	Essential for long-term

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 19, May 2023 Impact Factor: 7.301

Efficiency	• Reduces maintenance cost • Enhances sustainability	capability • Trade-offs with performance and speed	deployment, especially in battery-powered or remote environments
QoS Support	• Enables service differentiation • Ensures performance for critical apps (e.g., fire detection)	• Requires accurate traffic classification • May increase system complexity	Vital for meeting application-specific needs, prioritizing critical traffic, and maintaining user satisfaction

V. LITERATURE REVIEW

The efficiency, energy consumption, data integrity, and applicability for a range of applications within the dynamic industrial IoT and smart infrastructure environment are highlighted in this literature review, which examines many IoT communication protocols.

Bakhtiari et al. (2022) IIoT Recent years have seen a rigorous development of technology that is heading towards Industry 4.0's ambitious goal is network automation. But there are still major challenges in developing a dependable IIoT ecosystem for various applications; these include contentious issues with security, battery life, and bandwidth. In contrast to sensors and actuators, which are downstream devices, an item upstream is a cloud. Within the broader context of the IIoT, the majority of the problems are related to edge computing [43].

Kaskatiiski and Boyanov (2021) evaluate and contrast several widely used IoT data transmission protocols utilizing organized, semi-structured, and unstructured data. In their daily lives, IoT is already evident in wearable technology, industrial controls, weather monitoring stations, agricultural systems, and consumer gadgets. The bandwidth and energy consumption of these devices increase significantly as their numbers rise, even if the information transmitted via IoT may be quite small. Therefore, it's critical to ensure that the devices involved communicate as efficiently as possible [37].

Nikolov, Nakov and Gotseva (2021) explained and contrasted between the LwM2M and MQTT protocols for Internet of Things devices. They explain their features, fundamentals, software implementation, range of applications, and best cases. Selecting the best IoT communication protocol for use is a really difficult task. Specifics, application goals, and concepts of IoT protocols are used to compare them. Selecting the right IoT communication protocol depends on the application [44].

Reilly et al. (2019) advanced energy distribution systems and smart cities are two instances of IoT-rich ecosystems. The vital information about urban infrastructure that keeps their contemporary cities running is sent by these systems. IoT devices nowadays don't have communication protocols that prioritize data integrity. In the absence of data integrity, these systems run the possibility of using compromised data to activate urban landscapes. Cyber-physical assaults can be carried out by attackers using this IoT connectivity weakness. They created a distributed, scalable, integrity-first, Ethereum-based Internet of Things communication protocol. Their light client ensures data transmission integrity for systems that require it most[45].

Petija et al. (2019) provide, summary of communication protocols that meet the IoT systems' QoS criteria. The IPFIX protocol has been described, along with its architecture, headers, messages, and communication model. A description of the Tiny IPFIX implementation-based IoT infrastructure monitoring architecture has been made available, as well as the Tiny IPFIX transformation mechanism that makes use of mediation, template management procedures, and application scenarios. Since the IoT lacks a common protocol, the study also provides insight into communication protocols by classifying them based on the transmission range and the OSI layer on which they function [46].

Sharma and Gondhi (2018) understand the many IoT protocols that are used at different IoT protocol suite tiers and evaluate their effectiveness and dependability based on their lightweight, energy-efficient, and secure design. With its quick development and broad range of real-world applications that have changed their lives, the IoT has become incredibly popular. IoT device connectivity depends heavily on communication. IoT protocols that provide dependable, For effective IoT messaging, communication must be lightweight, secure, and free of the energy and computing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

limitations of the limited IoT devices[47].

Table II presents a comparative overview of the primary research articles on the communication protocols of industrial IoT edge networks, highlighting each

Table 2: Research on Communication Protocols in Industrial IoT Edge Networks

Reference	Focus On	Key Findings	Challenges	Limitations
Bakhtiari et al. (2022)	IIoT challenges in Industry 4.0 and edge-cloud architecture	IIoT development is crucial for industrial automation; edge computing plays a critical role	Security, battery life, bandwidth	Limited discussion on implementation strategies and metrics
Kaskatiiski and Boyanov (2021)	Comparison of IoT data communication protocols	Efficient communication is vital as IoT device numbers grow; different data types impact protocol performance	Bandwidth and energy usage with scaling devices	Lack of in-depth performance benchmarks
Nikolov, Nakov, and Gotseva (2021)	MQTT vs. LwM2M protocol comparison	Protocol suitability depends on specific IoT use cases; highlights protocol features and implementation	Complex decision-making for protocol selection	No practical experiments or real-world validation
Reilly et al. (2019)	Secure IoT communication for smart cities	Developed integrity-first communication using Ethereum blockchain for data-critical systems	Lack of data integrity in current IoT protocols; risk of cyber-physical attacks	Blockchain overhead; not appropriate for all IoT devices with limited resources
Petija et al. (2019)	QoS-based IoT communication protocols, especially IPFIX and TinyIPFIX	Proposed TinyIPFIX for monitoring IoT infrastructure; classified protocols by OSI layer and range	Lack of a universal protocol; QoS management	Limited scalability and generalization across IoT applications
Sharma and Gondhi (2018)	IoT protocol suite analysis by layer	Protocols must be secure, energy-efficient, and lightweight for constrained devices	Balancing reliability, security, and energy efficiency	No protocol completely satisfies all criteria; lacks real-time testing

VII. CONCLUSION AND FUTURE WORK

Optimizing communication protocols in IIoT edge networks is fundamental to achieving efficiency, scalability, and security in industrial automation. By analyzing widely adopted protocols, and evaluating their performance, including MQTT, CoAP, HTTP, DDS, and AMQP across key IIoT requirements, including latency, bandwidth, reliability, and security, its highlighted their suitability for various industrial use cases. Furthermore, the integration of edge computing was shown to significantly enhance real-time data processing, reduce network congestion, and improve responsiveness in dynamic manufacturing environments. Key enablers such as AGV, RBPA, and RFID systems were discussed in the context of intelligent communication and localized decision-making. In addition, it addressed essential aspects like task scheduling, data routing, storage strategies, and the pressing need for robust security mechanisms. Despite significant progress, challenges such as standardization gaps, interoperability issues, and edge resource limitations persist, necessitating further research and industry collaboration. Ultimately, a well-architected synergy between communication protocols and edge computing will be instrumental in achieving scalable, resilient, and intelligent IIoT systems. Future work should focus on developing adaptive protocol stacks, AI-driven edge orchestration, and standardized frameworks to meet the evolving demands of Industry 4.0 and beyond.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

REFERENCES

[1] S. Jaloudi, "Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study," *Futur. Internet*, vol. 11, no. 3, Mar. 2019, doi: 10.3390/fi11030066.

[2] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges," *IEEE Commun. Surv. Tutorials*, 2020, doi: 10.1109/COMST.2020.3009103.

[3] H. S. Chandu, "A Survey of Memory Controller Architectures: Design Trends and Performance Trade-offs," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 930–936, 2022.

[4] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks," *J. Crit. Rev.*, vol. 6, no. 7, 2019, doi: 10.53555/jcr.v6:i7.13156.

[5] R. Basir *et al.*, "Fog computing enabling industrial internet of things: State-of-the-art and research challenges," *Sensors (Switzerland)*. 2019. doi: 10.3390/s19214807.

[6] A. Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 396–402, 2021.

[7] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[8] 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.

[9] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[10] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.

[11] S. Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.

[12] V. Kolluri, "An Extensive Investigation into Guardians of the Digital Realm: AI-Driven Antivirus and Cyber Threat Intelligence," *Tijer–Tijer–International Res. J.*, vol. 2, no. 11, 2015.

[13] S. S. S. Neeli, "Leveraging Docker and Kubernetes for Enhanced Database Management," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, p. 5, 2022.

[14] M. De Yck, M. Versteyhe, and F. Debrouwere, "Automated Guided Vehicle Systems, State-of-the-Art Control Algorithms and Techniques," *J. Manuf. Syst.*, vol. 54, pp. 152–173, Jan. 2020, doi: 10.1016/j.jmsy.2019.12.002.

[15] A. Balasubramanian, "AI-Driven Optimization of Urban Mobility: Integrating Autonomous Vehicles with Real-Time Traffic and Infrastructure Analytics," *Int. J. Innov. Res. Creat. Technol.*, vol. 5, no. 5, pp. 1–13, 2019.

[16] S. Chandramohan and M. Senthilkumaran, "Intelligent Automatic Guided Vehicle for Smart Manufacturing Industry," in *Springer Proceedings in Materials*, 2021. doi: 10.1007/978-981-15-6267-9_39.

[17] A. Goyal, "Scaling Agile Practices with Quantum Computing for Multi-Vendor Engineering Solutions in Global Markets," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, Jun. 2022, doi: 10.14741/ijcet/v.12.6.10.

[18] A. Gogineni, "Multi-Cloud Deployment with Kubernetes: Challenges, Strategies, and Performance Optimization," *Int. Sci. J. Eng. Manag.*, vol. 1, no. 02, 2022.

[19] S. Chandramohan and M. Senthilkumaran, "A Self Configurable Edge Computing for Industrial IoT," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.b3868.129219.

[20] G. Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.

[21] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*, 2017. doi:

10.1109/ICITECH.2017.8079928.

[22] P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," *J Adv Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.

[23] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," *J. Adv. Dev. Res.*, vol. 11, no. 1, 2020.

[24] V. S. Thokala, "A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications," *IJRAR*, vol. 8, no. 4, pp. 383–389, 2021.

[25] D. D. Rao, A. A. Waoo, M. P. Singh, and F. Paul, "Breaking Down Barriers: Scalability and Performance Issues in Blockchain-Based Identity Platforms Achieving Scalable and High-Performance Blockchain-Based Identity Systems," 2021.

[26] A. Gogineni, "Novel Scheduling Algorithms for Efficient Deployment of Mapreduce Applications in Heterogeneous Computing," *Int. Res. J. Eng. Technol.*, vol. 4, no. 11, 2017.

[27] T. Bressoud and D. White, "The HyperText Transfer Protocol," in *Introduction to Data Systems*, 2020. doi: 10.1007/978-3-030-54371-6_20.

[28] A. Gogineni, "Observability Driven Incident Management for Cloud-native Application Reliability," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 9, no. 2, 2021.

[29] F. A. Alhaidari and E. J. Alqahtani, "Securing Communication Between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey," *J. Commun.*, pp. 14–30, Jan. 2020, doi: 10.12720/jcm.15.1.14-30.

[30] M. Shah and A. Gogineni, "Distributed Query Optimization for Petabyte-Scale Databases," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 10, pp. 223–231, 2022.

[31] M. J. Michaud, T. Dean, and S. P. Leblanc, "Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems," in *MALWARE 2018 - Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software*, 2018. doi: 10.1109/MALWARE.2018.8659368.

[32] A. Prajapati, "AMQP and beyond," in *2021 International Conference on Smart Applications, Communications and Networking, SmartNets 2021*, 2021. doi: 10.1109/SmartNets50376.2021.9555419.

[33] S. Murri, "Data Security Environments Challenges and Solutions in Big Data," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 565–574, 2022.

[34] N. Patel, "Sustainable Smart Cities : Leveraging IoT and Data Analytics for Energy Efficiency and Urban Development," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 3, 2021.

[35] J. Marietta and B. C. Mohan, "A Review on Routing in Internet of Things," *Wirel. Pers. Commun.*, vol. 111, no. 1, pp. 209–233, Mar. 2020, doi: 10.1007/s11277-019-06853-6.

[36] A. R. Arunarani, D. Manjula, and V. Sugumaran, "Task scheduling techniques in cloud computing: A literature survey," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2018.09.014.

[37] S. U. Amin and M. S. Hossain, "Edge Intelligence and Internet of Things in Healthcare: A Survey," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2020.3045115.

[38] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digit. Commun. Networks*, 2022, doi: 10.1016/j.dcan.2022.03.013.

[39] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "IoT reliability: a review leading to 5 key research directions," *CCF Transactions on Pervasive Computing and Interaction*. 2020. doi: 10.1007/s42486-020-00037-z.

[40] M. Aboubakar, M. Kellil, and P. Roux, "A review of IoT network management: Current status and perspectives," *Journal of King Saud University - Computer and Information Sciences*. 2022. doi: 10.1016/j.jksuci.2021.03.006.

[41] E. Zanaj, G. Caso, L. De Nardis, A. Mohammadpour, Ö. Alay, and M. G. Di Benedetto, "Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey," *Technologies*. 2021. doi: 10.3390/technologies9010022.

[42] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, "Connectivity Technologies for IoT," in *Demystifying*

ISSN: 2581-9429
Volume 4, Issue 19, May 2023
Impact Factor: 7.301

Internet of Things Security, 2020. doi: 10.1007/978-1-4842-2896-8_5.

[43] M. Bakhtiari, Y. Wei, H. Nishi, K. Fung Tsang, N. Aljuhaishi, and M. Alahmad, "Optimum Configuration of Edge Computing Protocols for Industrial Internet-of-Thing Applications," in *IECON Proceedings (Industrial Electronics Conference)*, 2022. doi: 10.1109/IECON49645.2022.9969057.

[44] N. Nikolov, O. Nakov, and D. Gotseva, "Research of MQTT versus LwM2M IoT communication protocols for IoT," in *2021 56th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, IEEE, Jun. 2021, pp. 45–48. doi: 10.1109/ICEST52640.2021.9483477.

[45] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "An IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client," in *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*, IEEE, May 2019, pp. 53–56. doi: 10.1109/SERP4IoT.2019.00016.

[46] R. Petija, P. Fecil'ak, F. Jakab, and M. Michalko, "Critical Analysis of Communication Protocols to Support the Quality of Services in IoT-based Infrastructures," in *2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, IEEE, Nov. 2019, pp. 612–617. doi: 10.1109/ICETA48886.2019.9039989.

[47] C. Sharma and N. K. Gondhi, "Communication Protocol Stack for Constrained IoT Systems," in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, IEEE, Feb. 2018, pp. 1–6. doi: 10.1109/IoT-SIU.2018.8519904.