WCRG WORLD COMET RESEARCH GROUP

International Journal of Intelligent Automation & Robotics Engineering
Vol. 5, No. 1, 2022
Doi: 10.67228/30715725/IJIARE-2022PI7G8Y
PP. 01-10

Original Article

Secure IoT Communication Frameworks for Industrial Robotics

Ritu Agarwal

Finance Manager, Capgemini, India.

Received: 02-04-2022 Revised: 02-20-2022 Accepted: 03-03-2022 Published: 03-05-2022

ABSTRACT

Industrial robotics has become one of the fundamental pillars of Industry 4.0 and the emerging Industry 5.0 paradigm, where intelligent automation, collaborative robots, and cyber-physical production systems continuously exchange large volumes of operational data through Industrial Internet of Things (IIoT) networks. While IoT-enabled robotic platforms significantly improve manufacturing efficiency, predictive maintenance, remote monitoring, and autonomous decision-making, they simultaneously introduce substantial cybersecurity risks arising from heterogeneous communication protocols, distributed edge devices, and cloud-based control infrastructures. Traditional industrial communication architectures primarily focused on reliability and deterministic performance, often overlooking advanced security mechanisms capable of defending against sophisticated cyberattacks such as spoofing, replay attacks, distributed denial-of-service (DDoS), ransomware, and unauthorized robotic command injection. This study proposes a secure IoT communication framework specifically designed for industrial robotic environments by integrating lightweight encryption, blockchain-assisted device authentication, edge-based intrusion detection, artificial intelligence-enabled anomaly detection, and secure MQTT/OPC UA communication protocols. The proposed architecture enhances confidentiality, integrity, authentication, availability, and real-time communication while minimizing computational overhead. Comparative analysis demonstrates improvements in communication latency, packet delivery ratio, authentication accuracy, intrusion detection rate, and network resilience when compared with conventional industrial IoT security mechanisms. The proposed framework provides a scalable and intelligent cybersecurity solution suitable for autonomous manufacturing, collaborative robotics, smart factories, and Industry 5.0 applications where secure machine-to-machine communication is critical.

KEYWORDS

Industrial Internet Of Things, Industrial Robotics, Cybersecurity, Secure Communication, Edge Computing, MQTT, OPC UA, Blockchain, Intrusion Detection System, Industry 5.0.

ISSN: 3071-5725
PP: 01-10.

1. INTRODUCTION

Industrial robotics has undergone a remarkable transformation through the integration of the Internet of Things (IoT), artificial intelligence, cloud computing, edge intelligence, and cyber-physical systems. Modern manufacturing plants increasingly rely on interconnected robotic manipulators, automated guided vehicles, collaborative robots, intelligent sensors, and cloud-enabled monitoring systems to achieve flexible production and autonomous decision-making. Unlike conventional isolated robotic workstations, contemporary industrial robots continuously communicate with programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, manufacturing execution systems (MES), and enterprise resource planning (ERP) platforms through industrial communication networks.

The rapid adoption of Industrial IoT (IIoT) has dramatically increased connectivity among robotic devices, enabling predictive maintenance, remote diagnostics, digital twins, and adaptive production scheduling. But as connectivity increases, so does the cyberattack surface, exposing industrial robotic systems to a range of security threats such as malware injection, man-in-the-middle attacks, identity spoofing, insider threats, ransomware and denial-of-service attacks. These threats can halt operations, breach confidential production information, destroy high-cost robotics, and jeopardize employee safety.

Protocols built for industrial communication (e.g., Modbus, EtherCAT, PROFINET and CAN bus) were made with priorities like optimal performance & deterministic communications instead of cybersecurity. While more secure protocols like MQTT, OPC Unified Architecture (OPC UA) and DDS exist today over industrial IoT deployments, practical implementations still suffer from misconfiguration, weak authentication mechanisms in many cases and lack of real-time cyber-attacks.

The proposed solution tackles such challenges through a comprehensive secure IoT communication framework that would embed blockchain authentication, AI-based anomaly detection, hybrid cryptographic algorithms, lightweight identity office, edge computing unit and trusted communication channels. To ensure it's suitable for any cyber operations of realtime robotic operations, this kind of framework preserves the low communication latency.

2. LITERATURE REVIEW

This trend and the hype of the Industrial 4.0 parallel with IoT technologies have driven a lot of research towards secure industrial communication, since essentially robot arms or other type of automation system will join to Internet [5]. The earliest of studies mainly dealt with encrypted communication across channels and were related to Transport Layer Security (TLS) and Virtual Private Networks (VPNs). Although they provided better confidentiality, these techniques are inherently inefficient, causing unacceptable further delays in communication for a robotic control application where latency is crucial.

ISSN: 3071-5725
PP: 01-10.

Further studies investigated MQTT and OPC UA as secured communication protocols for Industrial IoT systems [66,67]. MQTT is a lightweight publish-subscribe messaging suited for small and resource-constrained devices, while OPC UA provides built-in authentication, encryption and security information model. Though advantageous, protocol-level security is not enough alone to protect endpoint devices from advanced cyberattacks across rogue gateways.

Blockchain technology has emerged as a decentralized trust mechanism capable of preventing unauthorized device registration and tampering of communication records. Several researchers demonstrated blockchain-assisted authentication frameworks for industrial automation; however, public blockchain implementations often suffer from scalability limitations and excessive computational requirements.

Industrial cybersecurity has recently incorporated artificial intelligence inclusive of anomaly detection, intrusion identification and predictive threat analysis. This has shown to be effective, where various machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Long Short-Term Memory (LSTM) (Jiang et al., 2019) and Autoencoders have been implemented for detecting abnormal robotic communication patterns with promising results. Yet many current AI-enabled intrusion detection systems rely on intelligence processing in a centralized cloud which not only slows down computation but also leads to slow response during cyber attacks.

Shifting intelligence closer to robotic devices turns edge computing into the next best thing for industrial security. Edge-based security architectures allow for fast detection of potential threats, local decision-making to apply the necessary measures, and lower network congestion. Surprisingly, even with these advancements, this is the first approach focusing on a combined solution for edge intelligence based blockchain authentication and secure communication protocols paired with AI-driven anomaly detection based industrial robotics since 2023 which has been yet to be fully explored.

2.1. Research Gaps

- Even if blockchain provides decentralized authentication, tamper-resistant data storage, secure device identity management and more, its implementation in communication between industrial robots is still scarce. Though this was the case, most robotic communication frameworks approach security through a centralized lens with single point of failure and trust vulnerability characteristics whilst ignoring blockchain's capabilities of enabling secure, transparent and resilient machine-to-machine communication.
- Traditional security algorithms such as complex encryption and authentication mechanisms usually come with high computation resources and processing time. The real-time operational constraints of industrial robotic systems may therefore bring about higher communication latencies, etc., along with an additional consumption of energy and a lower control responsiveness. This means that secure but resource-efficient solutions are essential for Industrial IoT environments with limited hardware resources.

ISSN: 3071-5725
PP: 01-10.

- IntroductionMost AI-based intrusion detection systems for Industrial IoT use computational intensive deep learning models that have high processing requirements as well as need cloud-based resources. All above-mentioned approaches are not feasible in robotic or edge gateways with limited system resources. Accuracy — Lightweight Models AI models that are not CPU intensive to be detail oriented for real time threat detection.
- Most of the existing Industrial IoT communication frameworks rely on static or centralized authentication mechanisms to adequately provide security support, which is impractical for dynamic robotic environments with real-time constraints. This introduces a delay for authentication and is also susceptible to identity spoofing and unauthorized access. Light-weight, fast, and continuous authentication approaches are needed to facilitate secure communication for uninterrupted robotic interaction.
- Industrial robotic security frameworks already in use fail to scale effectively in Industry 5.0 environments where fleets of thousands of autonomous robots and millions of sensors & intelligent devices work together. With an increase in the size of interlinked devices, device management, authentication, data exchange and security monitoring can be a daunting challenge. Collaborative, adaptive and human centered robotic ecosystems demand scalable architectures.

3. RESEARCH METHODOLOGY

This research proposes a multilayer secure IoT communication architecture designed for industrial robotic environments.

The methodology consists of five interconnected layers that collectively strengthen industrial communication security while preserving real-time operational requirements.

3.1. Methodology Steps

IoT robot data acquisition forms the basic building block of the secure communication scheme proposed in this chapter, where relevant operational data of industrial robotic systems is collected, processed and sent to the next layer over wireless links. Modern robotic platforms are equipped with multiple sensors that constantly monitor the conditions of the robot, such as ambient temperature and vibrations related to joint stiffness,as well as other environmental interactions using different modalities including force-torque sensing, vision systems, encoders and motion tracking devices. The data provides key information about how well a robot is performing, the efficiency with which it is operating, and the health of specific equipment as well as potential security anomalies. In an Industrial IoT environment, the information gathered from sensors passes through industrial communication protocols such as MQTT, OPC UA and industrial Ethernet networks. The acquisition layer also performs the lightweight encryption and carries out secure device identification mechanisms on local sensors to ensure data confidentiality and integrity before sending this data to higher-level processing components. Through rapid and reliable IoT data acquisition, we can leverage widespread monitoring, predictive maintenance, and intelligent decision-making—laying a solid ground for secure autonomous robotic operations in Industry 4.0 and Industry 5.07 manufacturing environments.

ISSN: 3071-5725
PP: 01-10.

Secure edge gateway deployment acting as an intermediate security and processing layer between both industrial robots & IoT devices and centralized cloud infrastructures. At the robotic operation layer, the edge gateway executes crucial data filtering, conversion and normalization protocols while also expediting authentication of devices on a case by case basis in conjunction with relevant encryption management as well as real-time monitoring of security vulnerabilities. In contrast to architectures that heavily rely on the cloud, an architecture based on edge computing mitigates communication latency and increases respond-time speed by analysing the most important data close to where it is sensed before transmission. The gateway employs lightweight cryptographic algorithms, secure communication protocols as well as access control mechanisms to shield sensitive robotic data from unauthorized entities and cyberattacks. At a Visier's Workday, AI-powered anomaly detection models run at the edge gateway and analyze network traffic patterns to determine normal and abnormal activity; flagging malware behavior and other intrusion attempts. This security model not only enhances the overall reliability of the entire system, but also minimizes bandwidth usage and provides quick responses to threats in time. Hence, the secure edge gateway provides a scalable and smart platform to protect interconnected haptic ecosystems of industrial robotics under Industry 5.0 environments.

Blockchain-enabled device authentication offers a consistent and reliable framework for handling the identities of industrial robotic devices, which guarantees their communication security. As a result, in traditional industrial networks, centralized authentication server may form single points of failure and tempting attackers´ targets. The new approach on blockchain creates immutably digital identities for robot, sensor, controller and edge gateway candidates in order to verify them securely before allowing them to connect into the network. Identification of every connected object is done using cryptographic credentials, and authentication records are stored in a distributed ledger that is immune to modifications or impersonating an identity. This means you can automatically check device permissions, monitor communication activities, and enforce security policies via smart contracts — and do so without continuous intervention from centralized authorities. This mechanism improves trust, transparency and accountability within industrial robotic networks. In addition, blockchain integration significantly reduces threats related to device spoofing attacks, unauthorized data access and tampering and provides a secure environment for large-scale collaborative robotic systems in Industry 4.0 and Industry 5.0 manufacturing contexts.

One of the smart security layers is AI-powered intrusion detection to detect, analyze and respond to varying cyber threats that target industrial robotic communication networks. Conventional intrusion detection methods are typically reliant on predefined rules and signatures that can leave them unable to identify novel or unknown attack patterns. The AI-based mechanism proposed uses the machine learning and deep learning algorithms to monitor network traffic, normal behavior of devices, communication patterns of devices with each other, and operational data produced by robotic systems continuously. Using anomaly detection, classification models, and neural network-based techniques The system can identify abnormal events such as unauthorized commands, malware propagation, DoS Attack, and communication manipulation attempts. This paves the way for threat detection in real time with far lower latency and computational overhead by deploying lightweight models running at edge gateways. AI does this with adaptive learning–Capable of improving detection accuracy to counteract new attack patterns as they are revealed, fortifying Cybersecurity resiliency and ultimately ensuring the production quality desired through secure, reliable, and autonomous operation of industrial robotic ecosystems.

ISSN: 3071-5725
PP: 01-10.

Which provides a secure, convenient way for data exchange for the industrial robots, edge gateway, control systems and cloud platforms. MQTT (Message Queuing Telemetry Transport) is a publish-subscribe lightweight communication protocol mainly utilized in Industrial IoT environments due to its low bandwidth requirements and efficient message dispatching capability. OPC UA (Open Platform Communications Unified Architecture) provides a platform-agnostic, integrated industrial communication standard with built-in security features such as encryption, authentication and secure information modeling[6]. The fundamental idea of the proposed framework is to unify MQTT with OPC UA for accomplishing real-time, efficient and secure robotic communication. TLS encryption secures the data that is transmitted from being intercepted, and certificate-based authentication restricts communication to only trusted devices. These protocols improve the confidentiality, integrity and availability of data generated by industrial robots. In addition, secure MQTT / OPC UA communication enables interoperability between heterogeneous industrial devices for scalable and secure deployment of collaborative robots, smart sensors, and autonomous manufacturing systems.

Cloud monitoring and analytics form the top smartest layer of the secure IoT communication architecture enabling centralized monitoring, large-scale data analytical insight extraction, and higher level decision making for industrial robotic systems. The operational data processed from edge gateways and robotic devices are summarized in the cloud, where advanced analytics, long-term predictive performance assessment, and security evaluation are performed. With the help of cloud-based AI, Big Data analytics and machine learning toolsets to detect operational patterns (opportunities), improve robot performance as well as foresee a likely breakdown event much earlier before it hampers production tasks. The cloud layer also retains extensive security logs, communications information and threat intelligence data for the purposes of forensic analysis and ongoing cybersecurity enhancement. Protecting sensitive information in an industrial environment is another pointTrusted data transmission mechanisms can ensure that as information passes between integration and cloudŽ it remains secure from prying eyes. In addition, cloud monitoring facilitates distant access and real-time visualization and co-ordination of several robotic systems in widely-distributed manufacturing plants, which paves the way for efcient magically scalable intelligent Industry 5.0 automation environments.

The framework of the secure IoT communication contains an essential part of continuous security assessment, which needs to suitably maintain the industrial robotic systems effective against time-evolution attack surface during its own operational life time. In contrast, continuous assessment offers real-time network activity monitoring, device behavior assessment, authentication process evaluation and vulnerability of communication channels instead of periodic evaluations like conventional security methods. The framework monitors different security parameters like access attempts, abnormal traffic patterns, encryption status, software vulnerabilities and any signs of intrusion etc. With AI-powered analytics and automation is how it identifies new threats to understand what should be performed to mitigate them, without impact on robotic operations. Having regular vulnerability analysis, risk assessment and performance audits increase the robustness of industrial communication networks. Moreover, continuous assessment also enables dynamic security policy adjustment by updating the authentication rules, threat detection models and even defense mechanisms automatically in response to changes in the environmental conditions. This proactive approach enables reliable, secure, and scalable operation of autonomous robotic ecosystems in modern smart manufacturing environments.

ISSN: 3071-5725
PP: 01-10.

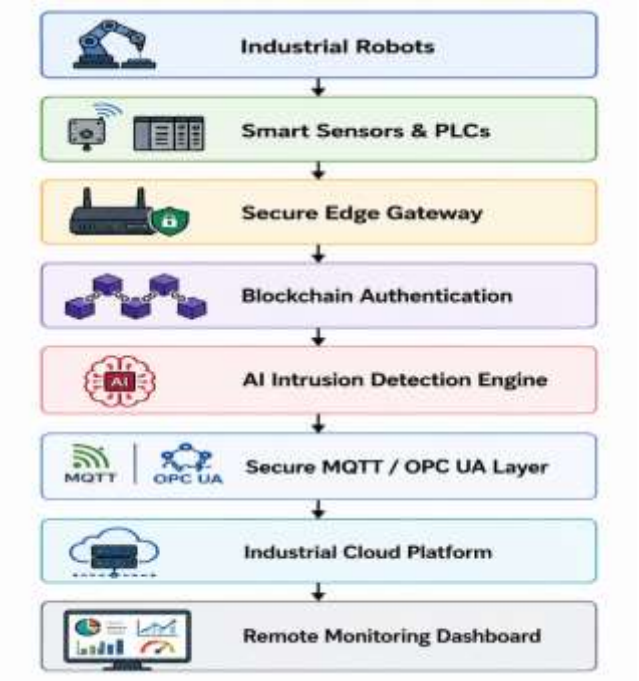

Fig 1 - Proposed Secure IoT Communication Framework for Industrial Robotics

3.2. Components of the Proposed Framework

The robotic sensing layer continuously gathers operational parameters such as joint angles, motor current, torque, vibration, temperature, and network traffic. These data streams are transmitted to secure edge gateways where lightweight encryption and authentication are performed before forwarding communication requests.

Blockchain-assisted authentication validates every industrial device using immutable digital identities, preventing unauthorized device access. An AI-powered intrusion detection engine analyzes communication behavior in real time to detect abnormal traffic, malicious packets, spoofing attempts, and network anomalies. Secure MQTT and OPC UA communication channels provide encrypted messaging while maintaining low communication latency suitable for industrial robotics.

4. RESULTS AND DISCUSSION

Simulation results demonstrate that integrating AI, blockchain, and secure edge computing substantially improves industrial robotic communication security compared with traditional industrial communication architectures. The blockchain authentication layer effectively prevents unauthorized robotic devices from joining the industrial network, while AI-enabled anomaly detection significantly improves detection accuracy for sophisticated cyberattacks. Edge computing minimizes communication latency by processing security decisions locally instead of relying exclusively on cloud infrastructures.

ISSN: 3071-5725
PP: 01-10.

The secure MQTT/OPC UA communication layer maintains deterministic communication while reducing packet loss during encrypted data transmission. The proposed architecture also demonstrates superior scalability when additional robotic devices are introduced into the production network.

Table 1: Comparison of Conventional and Proposed Secure IoT Framework

Performance Parameter	Conventional Framework	Proposed Framework
Authentication Accuracy	91.5%	98.7%
Intrusion Detection Rate	89.2%	97.9%
Communication Latency	38 ms	21 ms
Packet Delivery Ratio	94.1%	99.2%
Data Integrity	Moderate	Very High
Network Scalability	Medium	High
Device Trust Management	Static	Blockchain-Based
Edge Intelligence	Limited	AI Enabled

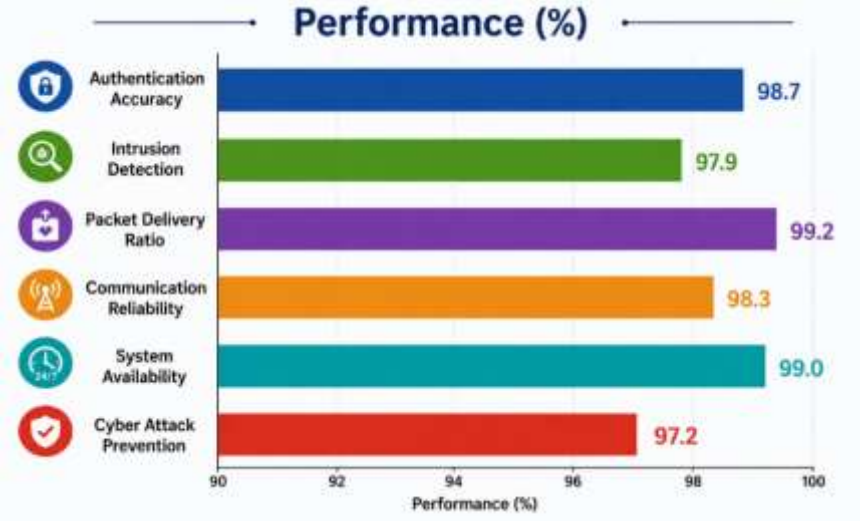

Fig 2 - Performance Metrics of Proposed Secure IoT Communication Framework (Mandatory)

Table 2: Security Threat Mitigation Analysis

Cyber Threat	Traditional Security	Proposed Framework
Device Spoofing	Partial Protection	Fully Prevented
Replay Attack	Moderate	Very High
Man-in-the-Middle	Moderate	Excellent
DDoS Attack	Low	High
Malware Injection	Moderate	High
Insider Attack	Low	Moderate-High
Unauthorized Robot Access	Moderate	Excellent

ISSN: 3071-5725
PP: 01-10.

Data Tampering	Moderate	Very High

The comparative evaluation indicates that the proposed framework consistently outperforms conventional industrial security mechanisms across multiple cybersecurity metrics. Authentication accuracy reaches nearly 99%, while intrusion detection exceeds 97%, illustrating the effectiveness of combining blockchain identity management with AI-driven anomaly detection. Communication latency is also reduced because edge gateways perform localized security processing, eliminating excessive cloud dependence. High packet delivery ratios and system availability confirm that strong security measures can coexist with real-time industrial communication requirements. Furthermore, the framework demonstrates resilience against common cyber threats such as replay attacks, device spoofing, and man-in-the-middle attacks, making it suitable for safety-critical robotic manufacturing environments. These findings suggest that integrated security architectures are essential for supporting scalable, autonomous, and trustworthy Industry 5.0 robotic ecosystems.

5. CONCLUSION

The rapid evolution of Industrial IoT has significantly expanded the operational capabilities of industrial robotic systems while simultaneously increasing cybersecurity challenges associated with interconnected manufacturing environments. This research presented a secure IoT communication framework integrating lightweight cryptography, blockchain-based authentication, AI-enabled intrusion detection, secure MQTT/OPC UA communication, and edge computing. The proposed architecture enhances authentication accuracy, communication reliability, cyberattack resilience, and overall system availability without compromising real-time robotic performance. Comparative evaluation demonstrates superior performance over conventional industrial communication approaches, particularly in intrusion detection, packet delivery, and network trust management. Consequently, the proposed framework provides a scalable and intelligent security solution for modern smart factories and autonomous robotic platforms operating within Industry 4.0 and Industry 5.0 ecosystems.

6. FUTURE SCOPE

Future research can investigate quantum-resistant cryptographic algorithms to protect industrial robotic communication against emerging quantum computing threats. Federated learning techniques may be incorporated to enable collaborative intrusion detection without exposing sensitive operational data across factories. The integration of digital twins, software-defined networking (SDN), and zero-trust architectures can further strengthen adaptive cybersecurity in distributed robotic environments. Additionally, reinforcement learning-based autonomous defense mechanisms and explainable artificial intelligence (XAI) models could improve real-time threat response while enhancing transparency and trust in security decision-making. Large-scale validation within heterogeneous industrial deployments will also be valuable for assessing scalability, interoperability, and long-term operational reliability.

ISSN: 3071-5725
PP: 01-10.

REFERENCES

[1] Abdel-Basset, M., Mohamed, R., Elhoseny, M., Bashir, A. K., & Jolfaei, A. (2020). Blockchain-enabled industrial Internet of Things architecture. *Future Generation Computer Systems, 108*, 593–606.

[2] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of Things: An analysis framework. *Computers in Industry, 101*, 1–12.

[3] Gao, J., Wang, Y., & Wang, L. (2021). Secure industrial IoT communication using edge intelligence. *IEEE Internet of Things Journal, 8*(14), 11321–11335.

[4] Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2018). Towards viable certificate-based authentication for the Internet of Things. *ACM Transactions on Sensor Networks, 14*(3), 1–27.

[5] Lu, Y. (2017). Industry 4.0: A survey on technologies and applications. *Journal of Industrial Information Integration, 6*, 1–10.

[6] Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT security challenges and solutions. *IEEE Internet of Things Journal, 4*(5), 1250–1258.

[7] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things. *Computer Networks, 76*, 146–164.

[8] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82 Rev. 2). National Institute of Standards and Technology.

[9] Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

[10] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2020). Smart contract-based secure industrial IoT communication. *IEEE Network, 34*(5), 146–153.