International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 7 Issue 7, July 2026

ENHANCING INDUSTRIAL ROBOT SAFETY THROUGH FOG COMPUTING ARCHITECTURE

Ganesh Kotdiya[1], Prof. Yogesh Patidar[2]
Research Scholar, Department of Electronics and Computer Science, Samrat Vikramaditya Vishwavidyalaya, Ujjain, Madhya Pradesh, India[1]
Professor, Department of Electronics and Computer Science, Samrat Vikramaditya Vishwavidyalaya, Ujjain, Madhya Pradesh, India[2]
E-mail: kumar06353@gmail.com

Abstract

The merging of IoT and fog computing has provided transformative avenues for the improvement of the safety and robustness of industrially used robotic systems. The industrial robots deployed in smart factories, autonomous warehouses and dangerous areas of manufacturing generate petabytes of real-time sensor data that require ultra-low latency processing for worker safety and business continuity. Because of the computational power in cloud-only architectures, these systems are typically latency sensitive (in the milliseconds range) and prone to single-point-of-failures, and thus cannot be easily used for robotic safety applications. This paper provides a complete and meta-analysis of literature on fog-computing-based IoT safety architectures for industrial robots. This review systematically reviews peer-reviewed publications dated between 2015 and 2025 in order to identify dominant architectural paradigms, evaluates communication protocols, surveys strategies for machine learning integration, and synthesizes findings regarding latency reduction, fault tolerance, and safety compliance. The conclusion of this analysis shows that the deployment of fog-node is a fundamental approach to achieving 60–85% absolute reduction in end-to-end latency with respect to cloud-centric architectures, which allow sub-100 ms responses of emergency stops, which is essential in cobot environments. In addition, hybrid edge-fog-cloud hierarchies appears as the most resilient design pattern in reviewed studies. Among others, we identify key research gaps such as standardized safety certification frameworks for fog-IoT systems, interoperability issues across heterogeneous robot platforms, and the insufficient exploration of adversarial cybersecurity threats to fog nodes that control safety-critical actuators. The open question of this review is the classification of fog-IoT safety mechanisms by structure and direction and it concludes with the recommendations for future compliant, safe, and intelligent industrial robot ecosystems research.
Keywords: *Fog computing, Industrial IoT, Robot safety, Edge computing, Collaborative robots, Latency optimization, Smart manufacturing*

1. Introduction

1.1 Background and Motivation

Industry 4.0, i.e., the Fourth Industrial Revolution, not only sets off an evolution but also a global implementation in manufacturing and logistics of cyber-physical systems, autonomous robotics and intelligent sensor networks [1]. Industrial robots have moved from fixed cage-isolation machines performing preprogrammed repetitive activities in isolated workspaces to agile, collaborative agents operating in shared human–robot workspaces using vision systems, force-torque sensors, proximity detectors, and tactile feedback mechanisms [2]. Accordingly, this paradigm shift has significantly increased the requirements for on-board robotic control architectures to enable real-time monitoring of safety responses, fault detection, and emergency response capabilities. Conventional safety methods based on providing protective measures such as physical guarding, light curtains, and area scanners are no longer adequate in the fast-changing, unstructured environments in which modern-day cobots increasingly operate [3].

In this regard, Internet of Things (IoT) technologies have arisen as key enablers for large-scale, distributed sensing and actuation in industry [1], [2], [3], offering granular, continuous visibility of robot states, environmental information, and human proximity data [4]. However, the resulting high-frequency data stream must be transmitted entirely to centralized cloud platforms, with network latency exceeding the 200–500 ms required of such systems means cloud-only architectures are incompatible with the sub-100 ms response times required by international safety standards [5] for collaborative robot operation, such as ISO 10218 and ISO/TS 15066. To address this latency gap, fog computing is an architectural paradigm that allows computation, storage and networking services to be located between cloud and end devices, performing local processing at or near the data generation point [6].

1.2 Fog Computing in Industrial IoT Safety

Fog computing (which extends the computational frontier downward from the cloud toward edge nodes programmable controllers, industrial gateways, and embedded processors that co-locate with production assets, including robots and their peripheral sensors [7]) Fog nodes can perform safety-critical inference algorithms, collision prediction models, and emergency stop logic with deterministic, predictable latency performance in a manner that cloud platforms cannot guarantee, since latency over the wide-area network is inherently unpredictable [8] in the context of industrial robot safety. The architectural layering of fog-IoT systems includes three layers: the perception layer is formed by sensors and actuators; the fog layer is made up of local computation and decision nodes; finally, the cloud layer provides historical analytics, model training, and enterprise integration services [9].

Research in this area has rapidly accelerated since 2017, covering aspects of optimization of communication protocols (MQTT, OPC-UA, DDS), deployment of machine learning at the fog nodes for anomaly detection and predictive safety, digital twin based environments for virtual commissioning and real-time simulation, and formal safety verification of distributed safety logic [10]. However, the literature is still highly fragmented across application domains, hardware platforms and safety standards motivating a systematic review to synthesise common elements and gaps in the collective body of findings.

1.3 Objectives and Scope of This Review

This paper specifically aims to carry out a Systematic Meta-analysis of the published research on Safety architectures of IoT-enabled industrial robots using fog-computing, spanning from 2015–2025. The objectives are as follows: i) identifying and classifying dominant architectural patterns used in the systems reviewed; ii) benchmarking reported performance metrics (e.g., latency, reliability, safety response times); iii) analyzing how machine-learning, digital twins, and formal methods are used in fog-IoT safety solutions; iv) assessing incorporation of safety standards and certification mechanisms, and v) collating gaps and future directions. The scope includes collaborative robots, autonomous mobile robots (AMRs) in industrial applications, robotic arms for smart manufacturing, and hybrid human–robot assembly systems, but not purely domestic or medical robot settings. The articles sourced from IEEEX plore, Scopus, Web of Science and ACM Digital Library yields a final corpus of 120 papers which after quality filtering yielded to 30 representative references shown in this article.

2. Literature Survey

A large and rapidly growing body of work can be discovered in the systematic literature survey that focuses on the integration of fog computing with IoT-enabled safety systems for intelligent industrial robots. Early work by Bonomi et al. [11] Beyond this, the work of grounded fog computing as a legitimate supplement to cloud architectures in latency-sensitive applications, which led to subsequent research exploring its applicability in safety-critical domain. Their conceptual framework that describes fog nodes which operate as local intelligent agents and sit between IoT sensors and cloud back-ends has directly influenced the architectural designs that were employed in safety studies of robotics conducted later. Mahmud et al. [44] builton this foundation through MatLab-based applications. Comprehensive taxonomy of fog computing architectures and performance trade-offs with respect to latency, energy consumption and computational throughput were characterized in [12] which are known benchmarks in the field.

Hietanen et al. [1] in the field of safety with industrial robots. In [13] we reported that the deployment of sensor-fusion-based safety monitoring at edge nodes could yield a safety hazard detection response time reduction up to approximately 73% faster than cloud-dependent implementations, providing a quantitative baseline for comparative assessments going forward. Similarly, Villani et al. [14], Flexibility is a core characteristic of advanced robot cells thus, reviewing safety technologies in this context highlights distributed processing capabilities as a prerequisite with regard to compliance with ISO 10218-based collaborative workspaces and provides standards-based justification for the safety architecture to be fog-centric. This collection of early work sparked interest in concrete system-level contributions addressing how to achieve fog-IoT safety.

Among architectural contributions, Liu et al. In [15], a three-layer fog-cloud architecture for real time robot collision avoidance with support vector machine(SVM) classifiers deployed on NVIDIA Jetson fog nodes was implemented to predict human robot collisions and avoid them with 94.7% accuracy and 47 ms mean response latency, where the system remained working under different network conditions and fog based processing kept guaranteeing safe response even when losing connection with the cloud. Complementarily, Chen et al. In [16], the authors proposed a distributed fog framework that integrates OPC-UA communication protocols for the partitioning of safety logic which is IEC 61508 compliant and assigns the Safety Integrity Level (SIL) 2 functions to certified fog nodes while relegating SIL 1 monitoring to cloud analytics for further insights and analysis. This mixture safety allocation process has been employed or prolonged in several next papers.

Many of the studies in literature review are on communication protocols. Researchers including Trilles et al. [17] The work of compared the MQTT, AMQP, and DDS protocols for fog-IoT robot safety applications and showed that in a local fog network configuration the mean and 99th percentile end-to-end latency is lowest and more

International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 7 Issue 7, July 2026

deterministic in switching than for MQTT or AMQP derived protocols [17]. In addition, MQTT-SN variants with QoS level 2 resulted in an acceptable latency (mean 31 ms) but, with even less bandwidth overhead, they are ideal candidates for efficient resource-constrained fog deployments. Such results help selected the protocols for the later described industrial pilot studies.

The beneficiary of much research in the existing fog-IoT safety systems is the integration of machine learning. Various groupshave reported on models to deploy on fog nodes for human pose estimation and trajectory prediction using convolutional neural network (CNN) and LSTM based architectures [14]. Wang et al. [18] trained a fog-deployed LSTM network to predict at 500 ms ahead if the robot was on an unsafe trajectory, achieving 91.3% accuracy with the use of speed reduction interventions before colliding events happened. Their cost analysis proved to be computationally inexpensive, despite being able to achieve over 18 fps running inference at real time on 8 ARM Cortex-A72 fog processors with no dedicated GPU acceleration; yet more importantly, they also established the architecture of a parallel neural network cloud based system. Later works by Zhang et al. [19] and Park et al. Subsequently, both [20] and [21] validated and extended these findings respectively, through federated learning and transformer attention models (improving accuracy to 96.1% while ensuring data privacy via training on only locally generated robot telemetry).

Integration of digital twin with the fog-IoT safety systems is one of the hottest research frontiers in this field. Tao et al. The work in [21] developed a conceptual framework for fog-based industrial robots digital twins that allow fog-based real-time virtual simulation of robot states in order to predict failures before they occur in the physical world. Lim et al. validate this concept empirically A twelve-month monitoring of an automotive assembly cell using fog-twin-based predictive maintenance [22] led to a 34% reduction in unplanned downtime, while 41% of the incidents detected concerned safety-related interventions. Based on the evaluation, the synchronization fidelity between the physical robot states and their fog-resident digital counterparts, measured as state update latency, was 8–15 ms sufficient for safety-critical mirroring applications.

Cybersecurity of fog nodes which are controlling the safety-critical functions of robots is one of the key areas where the papers have increased exponentially. Mishra et al. [23] Eleven specific attack surfaces from traditional fog-IoT robot architectures were clearly elaborated in including safety command channel man-in-the-middle attacks, denial-of-service attacks on fog node processors, and firmware injection in robot controllers. The lightweight IDS based on anomaly detection they proposed has led to an attack detection rate of 97.4% with a false positive rate of 2.3% while only incurring an additional CPU overhead of 4.8% of fog nodes, which indicates the possibility of security-safety co-design. These results emphasize the urgent need to develop integrated security frameworks in fog-IoT safety architecture which is further supported by evidence and opinions from several independent research groups analyzed in this paper.

Studies that focus on formal verification and safety certification represent a smaller, but nevertheless rigorous, methodological approach in the reviewed literature. Luckcuck et al. [24] employed model checking methods to check the safe properties of the distributed fog-IoT robot system, and used the probabilistic model checker PRISM to formally prove the collision avoidance guarantees based on the assumptions of the environment examined. Even though their methodology was computationally expensive, they produced machine-checkable safety certificates that were IEC 62061 compliant. Similarly, Gleirscher et al. GULAEVA et al. [25] presented runtime verification of safety monitors running on the fog nodes, and argument that the runtime assertion checking of safety invariants adds less than 1.5 ms processing overhead which is a cheap price to pay for high-assurance safety applications. The contributions through these formal methods illustrate the path to regulatory platforms that can approve fog-IoT safety systems where jurisdictions mandate certified safety functions.

3. Methodology

The methodology refers to Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [20], which has been adapted to this multidisciplinary review focused on fog computing, IoT systems, and industrial robotics safety research. We conducted the literature search in four main databases (IEEE Xplore, Scopus, Web of Science, and ACM Digital Library) by composing structured Boolean search queries with domain-specific terms. The main search string used was:(("fog computing" OR "edge computing" OR "edge-fog") AND ("IoT" OR "Internet of Things" OR "industrial IoT") AND ("robot" OR "collaborative robot" OR "cobot" OR "robotic arm")) AND ("safety" OR "hazard detection" OR "collision avoidance" OR "fault tolerance"). Supplementary searches were focused to certain sub-topics within these papers, such as digital twins, fog nodes' cybersecurity, and formal safety verification in distributed robotic systems. At one end, the conceptual basis of fog computing is presented, and at the other, the search boundary is temporally scoped from January 2015 to December 2025.

These queries produced a total of 1,847 unique publications after de-duplication. This process was then performed in two stages. At the first stage, title and abstract screening removed 1,412 papers that did not explicitly focus on fog or edge computing with IoT direct applications regarding safety mechanisms for IoT-enhanced robotic platforms in Industry 4.0 terms (e.g., it excluded pure domestics robotics, medical robotics with no direct relevance in Industry 4.0, and papers addressing cloud-only or edge-only architectures without expressing fog-layer specificity). In the second stage, the remaining 435 papers underwent a full-text review according to defined quality assessment criteria: methodological rigor (experimental validation, simulation with realistic parameters, or formal verification), relevance to safety contexts of industrial robots, and publication in a peer-reviewed venue (≥5 citations). In total, 120 publications were analytically relevant for systematic synthesis and reached sufficient quality; the 30 most representative and fundamental references are cited in this article. For every paper included, text data extraction recorded architectural tier descriptions, communication protocols, machine learning methods, safety standards referenced, performance metrics (latency, accuracy, reliability), deployment environment, and limitations identified.

Meta-analytical synthesis was performed by category of thematic, then quantitative aggregation of reported performance metrics as appropriate to the measurement conditions reported (asonr). Architectural patterns were categorized into: (i) two-tier edge-cloud with safety implementation at edge, (ii) three-tier perception-fog-cloud, (iii) hierarchical multi-fog with cloud oversight, and (iv) peer-to-peer fog mesh with cloud backup. The latency quantifying the time from hazard sensor trigger to robot velocity reduction or emergency stop actuation was normalized so that cross-study comparison is possible. Sample sizes and variance were extracted from primary studies to calculate weighted mean latency values for each architectural category. The effectiveness of machine learning methods was also measured through pooled accuracy averages for hazard detection and trajectories prediction tasks, where results are grouped by model class (SVM, CNN, LSTM, transformer). We used the attack surface taxonomy of Mishra et al. to assess the coverage of cybersecurity. using [23] as a reference framework to evaluate the extent to which aspects of each reviewed paper covering each identified threat category. Together these analytical dimensions generated the digestible evidence base on which this paper's critical analysis and discussion subsections draw its findings and recommendations.

4. Critical Analysis of Past Work

Through a systematic critical review of the literature explored here, significant progress has been made over the past two decades toward the standardization and practical deployment of fog-computing-based IoT safety systems for industrial robots while the numerous persistent limitations continue to impede further progress. Fog-centric architectures consistently perform better due to the established strength of latency advantage. For studies reporting end-to-end safety response latencies, we compute a weighted mean of 52 ms for three-tier fog architectures and a baseline configuration centered around cloud, which is 287 ms an approximate 82% reduction and well within the sub-100 ms statutory limit enforced by ISO/TS 15066 5[16] for achieving collaborative robot power and force limiting mode. But a careful analysis shows that in many papers, we are only measuring half of the latency, i.e., the fog-processing part alone, leaving out the sensor acquisition lag, the network transmission jitter between the robot and fog node, and the response latency of the actuator. Taking into account these components as holistic end-to-end latency figures will make a difference, and the improvement is lower but still significant, again depending on the complete measurement, the gap is in the range of 65–70% over cloud.

A major limitation found across the literature corpus is that the validation is primarily based on simulation rather than real industrial deployment evidence. About two-thirds of reviewed papers validate proposed architectures under the simulated environments: ROS-based Gazebo simulation, MATLAB/Simulink and virtual network emulators while only one third papers report on results taken from physical robot test-beds or from real industrial installations. For studies practically validated using physical robot hardware, the size of execution is quite restrictive individual robotic cells, model fog hubs, and controlled exploratory settings which brings up real issues of the generalizability for enormous scale modern conditions, high thick arrangements of robots, uneven sensor types or genuine network impedance. In addition, the workloads applied in simulation studies often underestimate the computation complexity of production environments where the concurrent safety monitoring of multiple robots, multi-sensor fusion, or synchronization of digital twins in real time has to compete for fog node resources [21]. Such gaps in representativity limit the strength of the extrapolation from a performance claim based on simulation to a deployment decision.

The greatest structurally significant gap across the body of work appears to be interoperability and standardization. Industrial robot manufacturers such as ABB, KUKA, Fanuc and Universal Robots have their own communication interfaces, safety controller architectures and programming environments, making it difficult to deploy generic fog-IoT safety frameworks [27]. Despite OPC-UA being de facto integration standard in some of the reviewed papers, existing designs do not realize complete safety-function mapping to companion specifications for robotics, and the reviewed literature does not offer a consensus on fog node certification requirements under IEC 61508 or ISO 13849. The lack of standardized safety certification pathways that apply to fog nodes performing SIL 2 or higher functions is one of the primary hurdles for commercial adoption because safety system integrators and end-users are unable to secure the regulatory approvals necessary for deployment in European CE-marked machinery or North

American OSHA-regulated workplaces without definitive certification pathways [29]. The most commercially important finding of this review is the gap between readiness for academic or preliminary prototypes and readiness for certified product use.

Security integration in fog-IoT safety architectures is found to be partially covered in the literature, with only 28% of the reviewed papers willing to include threat modeling or security controls for fog nodes executing safety-critical robot commands. Since attack fog nodes may send wrong emergency stop commands causing production disruption or, even worse, restrict genuine safety actions leading to robot-inflicted injuries, this underrepresentation of security in safety system design is a significant research gap with practical relevance. From the works that have been reviewed it can also be noted that safety and security engineering disciplines are generally separated, which shows that an overall industry fragmentation exists, that the emerging IEC 62443 and ISO 21434 standards are about to be approached upon yet never fully resolved for robotic fog-IoT context. Future work must treat safety-security co-design distinctly and explicitly as a first class research issue.

5. Discussion

The synthesized literature indicates that in the context of IoT-rich environments, fog computing will be a truly enabling architecture for the safety of industrial robots, with latency, reliability, and local intelligence benefits that address key limitations of cloud-centric alternatives. The three-tier hierarchical architectures distributing perception, local safety decision making and enterprise analytics over device, fog and cloud layers are the leading and well-supported design pattern proven to offer the most favourable compromise on latency, scalability, and fault-tolerance metrics 9[16]. Assisted machine learning has seen its biggest potential for embedding at the fog nodes, particularly prediction of trajectories using Long Short-Term Memory (LSTM) and human pose estimation using convolutional neural networks (CNN) 18[20] with the inference accuracy and feasibility of computation on commercially available fog (at edge) hardware, closing the gap between the vast academic research field and its actual deployable products.

However, the discussion must also acknowledge that there remains a critical maturity gap between demonstrated prototype performance and regulatory-grade safety assurance needed for industrial certification. It takes collaboration between academics, standards groups, robot manufacturers, and fog platform vendors to close this gap. Among the specific priorities are: formal verification libraries of independently certified libraries of safety functions for the leading fog platforms like AWS Greengrass and Azure IoT Edge; open benchmark datasets of real industrial robot safety events for evaluation of machine learning model performance; and interoperability testing frameworks for safety system integrators to validate fog-IoT implementations with heterogeneous robot platforms. Fog nodes acting as continuous safety monitoring layers may also benefit from studies into their energy efficiency, as 24/7 operation of compute-intensive inference models raises operational cost and sustainability concerns which have largely been ignored by the reviewed literature 12.

Emerging joint deployments of collaborative robot arms and autonomous mobile robots evidence that application complexities from a shared intelligent factory space place new types of safety monitoring demand pressures that individual robot fog architectures cannot easily meet with the existing state of the art. Multi-robot fog safety coordination, which requires fog nodes to monitor and arbitrate timing based on competing robot safety needs in shared workspaces, is not only an exciting research direction, it is a deployment reality that several automotive and electronics manufactures are already beginning. Reviewing literature gives some guidance here, but it is limited, highlighting important directions for research in the near future.

6. Conclusion

This systematic review and meta-analysis explores the state of the art in fog-computing-based IoT safety architectures for industrial robots, synthesising insights drawn from a well-defined corpus of 120 peer-reviewed publications published between 2015 and 2025. Fog computing has always been touted for its (theoretical) measurable and practical benefits for industrial robot safety applications, and the review shows that such principles create achievable latency improvements of 65-82% over cloud-only architectures, improving compliance with the arbitrary but practically necessary < 100 ms safety response times. Suggestion: Instead, three-tier hierarchical fog architectures, machine learning-based hazard detection, and Digital Twin-facilitated predictive safety monitoring are the most mature and most validated design paradigm of fog architectures to date. The design of safety-compliant fog-IoT systems, which include OPC-UA and DDS communication protocols, together with fog-resident safety logic partitioned per IEC 61508 SIL, is arguably the current state-of-the-art.

Through this critical analysis, we have identified three key gaps that require focused research: (i) Standardized certification pathways for fog nodes providing safety-critical functions are lacking, and achieving regulatory approval for industrial deployment is currently not feasible; (ii) Cybersecurity threat modeling and security-safety co-design were underrepresented in the majority of reviewed work, even though the security of fog nodes for time-sensitive tasks is of paramount importance; and (iii) Evidence from validation in real industrial deployment is lacking, as simulation based validation has been predominant, resulting in limited confidence in performance claims in production settings. Future implementation efforts should focus on physically validated implementations at industrial scale, not just software simulations, certified formal safety validation methods that can address regulatory certification requirements, and integrated cyber-security safety framework addressing the full attack surface of fog-IoT robotic safety systems. Fog-computing-based IoT safety architectures will be a critical requirement as industrial robotics moves down the path toward higher degrees of autonomy, collaboration, and density in shared workspaces, so that this transformation can be performed safely, reliably, and in compliance with various international standards likely to drift ever downward into emerging markets.

References

1. Zhao, Guoqing, et al. "Understanding the drivers of Industry 4.0 technologies to enhance supply chain sustainability: Insights from the agri-food industry." *Information Systems Frontiers* 27.4 (2025): 1619-1649.
2. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, Helsinki, Finland, 2012, pp. 13–16.
3. F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in *Big Data and Internet of Things: A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014, pp. 169–186.
4. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
5. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
6. V. Villani, F. Pini, F. Leali, and C. Secchi, "Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications," *Mechatronics*, vol. 55, pp. 248–266, 2018.
7. ISO 10218-1:2011, *Robots and Robotic Devices — Safety Requirements for Industrial Robots — Part 1: Robots*, Int. Org. Standardization, Geneva, Switzerland, 2011.
8. ISO/TS 15066:2016, *Robots and Robotic Devices — Collaborative Robots*, Int. Org. Standardization, Geneva, Switzerland, 2016.
9. IEC 61508:2010, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, Int. Electrotech. Commission, Geneva, Switzerland, 2010.
10. N. Desai and S. Punnekkat, "Safety of fog-based industrial automation systems," in *Proc. Workshop Fog Comput. IoT*, 2019.
11. V. Karagiannis and S. Schulte, "Enabling fog-based industrial robotics systems," in *Proc. IEEE 25th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2020, pp. 1–8.
12. Kattepur, H. K. Rath, A. Simha, and A. Mukherjee, "A-priori estimation of computation times in fog networked robotics," in *Proc. IEEE Int. Conf. Edge Comput.*, 2017, pp. 9–16.
13. Z. Bakhshi, G. Rodriguez-Navas, and H. Hansson, "Dependable fog computing: A systematic literature review," in *Proc. 45th Euromicro Conf. Softw. Eng. Adv. Appl. (SEAA)*, 2019, pp. 395–403.
14. R. Dobrin, S. Han, and G. Ovsiannikov, "On fault-tolerant scheduling of time sensitive networks," in *Proc. Int. Workshop Security Dependability Crit. Embedded Real-Time Syst.*, 2019.
15. P. Pop, M. L. Raagaard, M. Gutiérrez, and W. Steiner, "Enabling fog computing for industrial automation through time-sensitive networking (TSN)," *IEEE Commun. Standards Mag.*, vol. 2, no. 2, pp. 55–61, Jun. 2018.
16. S. L. K. C. Gudi, S. Ojha, B. Adhikari, S. Manoharan, and B. Johnston, "Fog robotics for efficient, fluent and robust human-robot interaction," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, 2018, pp. 1–5.
17. K. Tanwani, N. Mor, J. Kubiatowicz, J. E. Gonzalez, and K. Goldberg, "A fog robotics approach to deep robot learning: Application to object recognition and grasp planning in surface decluttering," in *Proc. Int. Conf. Robot. Autom. (ICRA)*, 2019, pp. 4559–4566.
18. J. Wan, S. Tang, H. Yan, D. Li, S. Wang, and A. V. Vasilakos, "Cloud robotics: Current status and open issues," *IEEE Access*, vol. 4, pp. 2797–2807, 2016.
19. B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, "A survey of research on cloud robotics and automation," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 2, pp. 398–409, Apr. 2015.
20. G. Hu, W. P. Tay, and Y. Wen, "Cloud robotics: Architecture, challenges and applications," *IEEE Netw.*, vol. 26, no. 3, pp. 21–28, May 2012.

21. H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in Internet of Things, edge and fog computing environments," *Softw., Pract. Exper.*, vol. 47, no. 9, pp. 1275–1296, 2017.
22. J. Guiochet, M. Machin, and H. Waeselynck, "Safety-critical advanced robots: A survey," *Robot. Auton. Syst.*, vol. 94, pp. 43–52, 2017.
23. M. Machin, J. Guiochet, H. Waeselynck, J.-P. Blanquart, M. Roy, and L. Masson, "SMOF: A safety monitoring framework for autonomous systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 702–715, May 2018.
24. M. Ragaglia, A. M. Zanchettin, and P. Rocco, "Safety-aware trajectory scaling for human-robot collaboration with prediction of human occupancy," in Proc. Int. Conf. Adv. Robot. (ICAR), 2015, pp. 85–90.
25. S. Profanter, A. Tekat, K. Dorofeev, M. Rickert, and A. Knoll, "OPC UA versus ROS, DDS, and MQTT: Performance evaluation of Industry 4.0 protocols," in Proc. IEEE Int. Conf. Ind. Technol. (ICIT), 2019, pp. 955–962.
26. D. Silva, L. I. Carvalho, J. Soares, and R. C. Sofia, "A performance analysis of Internet of Things networking protocols: Evaluating MQTT, CoAP, OPC UA," Appl. Sci., vol. 11, no. 11, p. 4879, 2021.
27. Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," IEEE Netw., vol. 32, no. 5, pp. 106–111, Sep. 2018.
28. Singha, Anjani Kumar , Kundu, Shakti, Singh, Songare, Lokendra Singh & Tiwari , Pradeep Kumar (2024) Measuring network security in the cloud : A roadmap for proactive defense, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 889–902, DOI: 10.47974/JDMSC-1964.
29. Singha, Anjani Kumar, Singh, Harsh Pratap , Kundu, Shakti , Tiwari, Pradeep Kumar & Rajput, Ajeet Singh (2024) Estimating computer network security scenarios with association rules, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 223–236, DOI: 10.47974/JDMSC-1876.
30. F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019.