GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

ISSN 2545-4803 on line
DOI: 10.46763/BJAMI

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI)

YEAR 2025 VOLUME 8, Number 2

AIMS AND SCOPE:
BJAMI publishes original research articles in the areas of applied mathematics and informatics.

Topics:
1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS
(BJAMI), Vol 8

ISSN 2545-4803 on line
Vol. 8, No. 2, Year 2025

EDITORIAL BOARD

TABLE OF C O N T E N TS

Balkan Journal of Applied Mathematics and Informatics Online ISSN 2545-4803
Volume 8 Number 2 Year 2025 UDC: 004.891.056:[007.52:004.771]

SECURITY CHALLENGES AND SOLUTIONS IN ROBOTIC AND INTERNET OF ROBOTIC THINGS (IoRT) SYSTEMS: A SCOPING REVIEW

VESNA HRISTOVSKA, ALEKSANDAR VELINOV, NATASA KOCESKA

Abstract. Robotic systems and the Internet of Robotic Things (IoRT) are rapidly expanding into domains such as healthcare, industry, logistics, and smart environments, bringing significant benefits but also exposing new security challenges. Because robots exchange data, interact with cloud and edge platforms and operate autonomously, cyber incidents can cause information breaches and physical harm. This scoping review maps current research on IoRT security by analyzing studies published in the last five years. Using PRISMA methodology, the review identifies the main threats affecting IoRT systems-ranging from adversarial manipulation and data leakage to insecure wireless communication and vulnerabilities in learning-based components. The literature examined shows that most solutions focus on protecting data confidentiality, ensuring integrity of robotic behavior, and applying cryptographic or AI-driven defense mechanisms, while protocol-level security remains notably underexplored. Overall, the review reveals a growing yet fragmented field and highlights the need for a more systematic evaluation of communication protocols and robust, trustworthy AI methods to secure increasingly autonomous robotic systems.

1. Introduction

The Internet of Robotic Things (IoRT) represents an emerging paradigm that integrates robotics, the Internet of Things, Artificial Intelligence (AI), and cloud–edge computing into a unified, interconnected ecosystem. Within this ecosystem, robots are equipped not only with advanced sensing and actuation capabilities but also with the ability to communicate, coordinate and learn from distributed data sources. This convergence enables autonomous decision-making, adaptive behavior and collaborative operation across diverse environments, ranging from industrial automation and healthcare to smart cities and logistics [1]. By leveraging real-time data exchange and computational resources distributed across the network, IoRT systems enhance the efficiency, flexibility and scalability of robotic applications, while also introducing new challenges related to security, interoperability and system reliability [23].

The integration of robotic devices with the internet, sensor networks and intelligent computational platforms creates a highly complex environment in which every vulnerability can have multiple consequences. A compromised robot can pose significant risks because it directly interacts with both digital systems and the physical environment. It can perform unexpected or dangerous movements, cause collisions or equipment damage, manipulate objects incorrectly, execute incorrect tasks, unauthorized video/audio surveillance, collecting confidential data etc. Moreover, IoRT environments depend on diverse communication protocols, cloud infrastructures and

edge-computing and fog-computing architectures, collectively producing multilayered attack surfaces and amplifying the challenges associated with securing such systems [2].

Scientific literature offers numerous IoT security solutions, but when it comes to robots and IoRT, the knowledge is still fragmented. Some papers focus on visual and biometric data privacy [13][24], others examine cryptographic and secure transmission mechanisms [3][9], some analyze vulnerabilities of industrial robotic and Industrial Control Systems (ICS) platforms [8][16][17], while others address AI-based attack detection and machine-learning–driven security[5][6].

A comprehensive insight is lacking – one that would unite the most studied aspects of security and highlight the remaining open challenges.

Our research aims to overcome this gap, systematically collecting, categorizing, and analyzing relevant papers in five years. Focused on security of robotic and IoRT systems, this review seeks to identify areas that are well-explored, as well as those where sufficient empirical or theoretical support is lacking-particularly in the areas of cybersecurity of autonomous robots, trusted communication architectures, and AI-based protection mechanisms in IoRT ecosystems.

2. Methods

The scoping review follows the PRISMA methodology through which a substantial body of relevant scientific literature was systematically identified and examined. Fig. 1 shows the main stages of the research methodology. In developing the study design, the research questions were first defined, followed by the establishment of eligibility criteria, the formulation of a comprehensive search strategy and the specification of procedures for data collection and analysis.

2.1. Scope and research questions

The aim of this scoping review is to identify, categorize and synthesize scientific studies that examine the security aspects of robotic systems and the Internet of Robotic Things (IoRT). It is becoming increasingly important to recognize that the integration of robots with cloud platforms, wireless networks, sensing infrastructures and other autonomous environments exposes them to a broad range of cybersecurity threats. For this reason, this review includes studies that explore how security is defined, implemented, challenged or compromised within robotic and IoRT settings.

Our focus is on papers published in the last five years that cover research addressing both software and hardware based security mechanisms, communication infrastructures,

vulnerabilities arising from networked robotic behavior, as well as security techniques enhanced through artificial intelligence. The purpose of the analysis is to determine which aspects of IoRT security are most frequently discussed, which methods have been proposed to mitigate risks and where significant gaps remain.

This scoping review was guided by the following research questions:

- RQ1: What security aspects are most frequently addressed in robotic and IoRT systems?
- RQ2: Which communication protocols are used in IoRT systems, and how secure are they?
- RQ3: What types of attacks and vulnerabilities have been identified in IoRT systems?
- RQ4: What countermeasures and technical solutions are used to improve the security of IoRT systems?
- RQ5: Is artificial intelligence used to support or enhance the security of IoRT systems?

2.2. Eligibility criteria

The selection of relevant studies for our research included the following inclusion criteria: (1) Only articles and conference papers were considered; Studies published within the last five years (2020-2025); (2) Publications written in English language; (3) Research papers that explicitly addressed security, privacy or protection mechanisms in robotic or Internet of Robotic Things (IoRT) systems.

The exclusion criteria included: (1) Review articles, survey papers, book chapters and thesis documents; (2) Studies not related to IoRT or robotic systems, or papers where IoRT/robotics is mentioned only sporadically without emphasizing security; (3) Publications that discussed IoRT or robotics in general but did not address cybersecurity, privacy, vulnerabilities or protection mechanisms; (4) Studies conducted in informal, non-technical, or non-scientific contexts that did not provide rigorous analysis or technical contributions.

2.3. Sources and search strategy

The literature search was carried out systematically across three major scientific databases: IEEE Xplore**,** Scopus**,** and Web of Science, in order to ensure a comprehensive coverage of publications relevant to IoRT security. The search process was restricted to works published within the last five years (2020–2025), written in English, and limited to journal articles and conference papers. A structured keyword-based query was applied during the electronic search phase, using the following search

expression: *(Security AND Robot AND* (*IoRT OR "Internet of Robotic Things" OR "Internet of Robotics Things")).*

The combined search across the selected databases initially yielded 103 publications**,** distributed as follows: 46 records from Scopus**,** 27 from IEEE Xplore**,** and 30 from Web of Science**.** After removing 47 duplicates**,** the final dataset consisted of 56 unique publications that met the initial search parameters.

2.4. Selection of studies

After generating the initial pool of publications retrieved through the database search, the next phase involved screening of titles and abstracts to determine which studies were suitable for further examination.

During this stage, 7 publications were excluded based on abstract review because they did not sufficiently address IoRT security or were outside the defined scope. Additionally, 14 studies were removed due to lack of open-access availability, preventing full-text evaluation. The remaining 35 publications were retrieved and subject to detailed full text analysis.

15 studies were excluded because they did not meet the inclusion criteria. The final selection includes 20 articles that met all inclusion criteria and were used in the final analysis.

The complete selection and exclusion process conducted according to PRISMA methodology is illustrated in Figure 1**.**

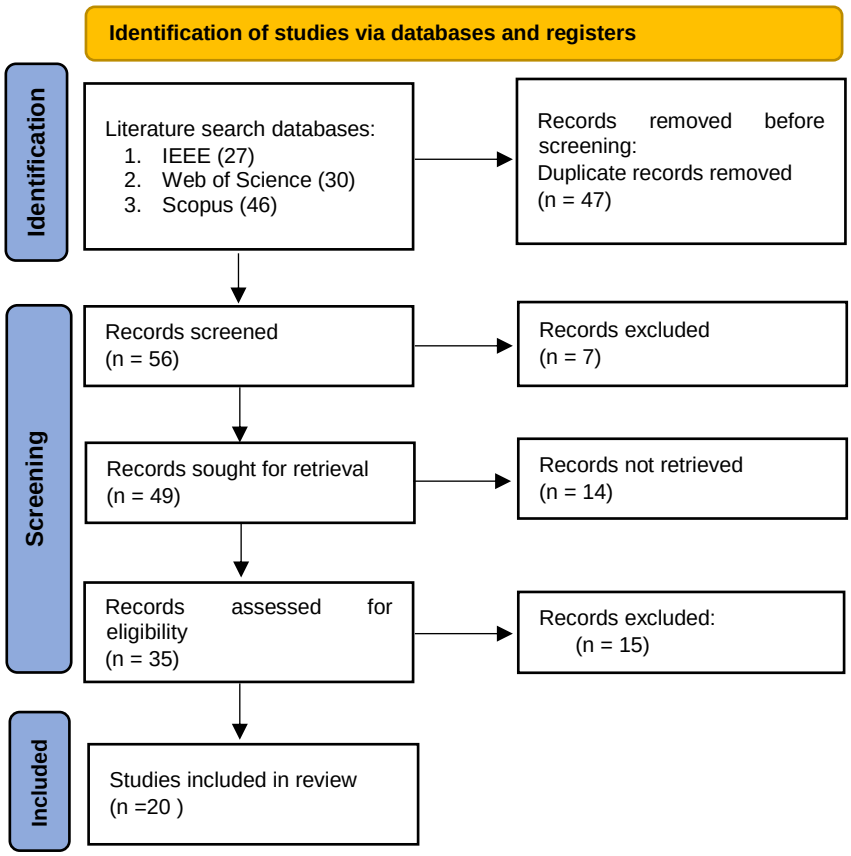

Figure 1. PRISMA flow diagram for literature search

3. Results

The final set of 20 studies that investigate security challenges, mechanisms and vulnerabilities in robotic and IoRT systems is summarized in Table 1 in the Appendix. These studies were further analyzed in detail and systematically organized according to their relevance to our research questions.

4. Discussion

When examining the security aspects emphasized across the reviewed literature, several distinct security themes emerge. A substantial group of papers focuses on data confidentiality and privacy protection, proposing methods that prevent leakage of

sensitive data. This includes studies [3][22][12][14] and [8], all of which concentrate on encrypting data, filtering private information, or safeguarding communication channels.

A second cluster of studies is centered on system integrity and trustworthy operation, particularly in learning-enabled IoRT environments. Papers [7][17] and [16] highlight risks such as data poisoning, unauthorized behavior modification, integrity attacks and weaknesses in hardware logic or control systems.

Another strong segment of the literature examines AI/ML robustness and AI-driven security, reflecting the growing dependence of IoRT systems on intelligent decision-making. Studies [6][5][19], and [13] address adversarial ML threats, anomaly detection, spoofing resistance and AI-based security monitoring.

As the discussion shifts toward communication protocols, it becomes evident that only a small subset of the reviewed papers directly addresses IoRT communication technologies or evaluates their security properties.

A small group of papers mentions TLS-protected TCP/IP channels as part of their system design, including [4][5] and [18], which describes encrypted client–server communication for robot control. Other studies reference standard IP-based networking or Wi-Fi connectivity, such as [6][7] and [19] where data transmission is discussed in the context of wireless channels but without specifying IoRT-focused protocols.

Several papers outline cloud–edge or cloud–robot communication flows, including [3][10] and [13]. In these studies, communication is presented as part of a distributed IoRT architecture, yet the exact protocols that support this communication remain unspecified. A separate group of studies refers to blockchain-based data exchange [9], where blockchain acts more as a secure medium for data sharing rather than a communication protocol in the classical sense.

Finally, a number of conceptual IoRT papers - including [20] and [21] mention broader communication technologies like Wi-Fi, 4G/5G, ZigBee, or satellite links, but do not analyze their protocol-level security or implementation details.

Despite these references, none of the reviewed studies offers a dedicated evaluation of communication protocols or their security properties. Protocols appear only as supporting elements within broader architecture rather than as objects of study. As a result, although communication mechanisms are mentioned across the corpus, no paper examines how secure these protocols are, which highlights a clear and persistent research gap in IoRT protocol-level security.

Across the reviewed literature, cybersecurity threats in IoRT systems fall into several recognizable categories. A large group of papers focuses on AI- and data-level vulnerabilities, identifying risks such as model poisoning, adversarial manipulation and data inference. This includes [6][5] and [7], all of which highlight how learning-enabled components can become attack surfaces. Another cluster of studies emphasizes communication and network threats, particularly in unprotected wireless environments [4]. Studies [12][13][14][17] and [19] describe risks such as eavesdropping, spoofing, and data interception. A third group focuses on physical and operational vulnerabilities, including incorrect robot behavior, sensor tampering, or unsafe coordination, as discussed in [21] and [20]. Together, these studies show that IoRT vulnerabilities span the cyber, physical and AI layers, underscoring the complex attack surface of interconnected robotic ecosystems.

The countermeasures proposed in the reviewed studies can be grouped into a few major categories. A significant portion of the literature focuses on cryptographic and privacy-preserving techniques, introducing lightweight encryption, privacy filtering or secure transformation of visual data [3] and [22]. Another strong cluster centers on AI- and ML-based detection systems, where anomaly detection, behavioral monitoring and adversarial learning defenses are proposed [6][5] and [13]. In [7] federated learning integrity protection, using moving-target defense or trust-based aggregation is introduced. Finally, there is one paper that emphasizes system-level or architectural defense, focusing on secure-by-design principles, validation frameworks and lifecycle risk management [17]. All these articles illustrate the wideness of technical strategies being applied in contemporary IoRT security research.

Artificial intelligence is widely used in the analyzed studies, either as a key security mechanism or as a technology whose security-related weaknesses need to be addressed. Several papers use AI for security enhancement, proposing ML-based intrusion detection, anomaly recognition, behavioral modeling and adversarial filtering [6][13][5], and [22]. In these studies, AI models help identify cyber-attacks, protect sensitive visual information, or evaluate system behavior. At the same time, another group of papers emphasizes that AI introduces new vulnerabilities, particularly when robots rely on learning-based decision-making, examples include [7] and [5], which discuss poisoning, manipulation and adversarial perturbations. Additionally, conceptual IoRT works use AI primarily for perception or autonomy but do not apply it to cybersecurity [18] and [19]. Overall, the analysis shows that AI can play a dual role in IoRT ecosystems-serving as a primary defense mechanism but also as a significant attack surface.

5. Conclusion

This scoping review examined recent work on the security of robotic and IoRT systems demonstrating the rapid progress in this field, but also the uneven development. Most studies focus on safeguarding data confidentiality and maintaining reliable robot behavior, usually through cryptographic methods, privacy-preserving techniques, or AI-based detection mechanisms.

At the same time, communication security is addressed only superficially: protocols are mentioned within system architectures but are rarely evaluated or tested, leaving important questions about their resilience unanswered. AI is widely used as a security tool, yet it also introduces new vulnerabilities that current research has only begun to explore. Overall, the review highlights an emerging research area with substantial potential but also several critical gaps. Future work should focus on systematic evaluation of IoRT communication protocols, real-world testing of attack scenarios and development of trustworthy and transparent AI methods tailored specifically to robotic systems. As IoRT technologies continue to integrate into sensitive environments such as healthcare, industry, and critical infrastructure, establishing a robust and holistic security foundation becomes essential for ensuring safe and reliable operation.

References

[1] Simoens, P., Dragone, M., & Saffiotti, A. (2018). The Internet of Robotic Things: A review of concept, added value and applications. *International journal of advanced robotic systems*, *15*(1), 1729881418759424.

[2] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.

[3] Öztürk, G., Çimen, M. E., Çavuşoğlu, Ü., Eldoğan, O., & Karayel, D. (2025). Secure and Efficient Data Encryption for Internet of Robotic Things via Chaos-Based Ascon. *Applied Sciences*, *15*(19), 10641.

[4] Mărieș, M., & Tătar, M. O. (2025). OT Control and Integration of Mobile Robotic Networks. *Electronics*, *14*(13), 2531.

[5] Karim, H., Gupta, D., & Sitharaman, S. (2025). Securing llm workloads with nist ai rmf in the internet of robotic things. *IEEE Access*.

[6] Raza, A., Memon, S., Nizamani, M. A., Dhomeja, L. D., Memon, N., & Charan, K. (2024). Machine Learning Techniques for Cyber Security in Internet of Robotic Things. *VFAST Transactions on Software Engineering*, *12*(3), 01-10.

[7] Zhou, Z., Xu, C., Yang, S., Zhang, X., Li, H., Huang, S., & Muntean, G. M. (2024). Safeguarding privacy and integrity of federated learning in heterogeneous cross-silo iort environments: A moving target defense approach. *IEEE Network*, *38*(3), 25-32.

[8] Gueye, T., Iqbal, A., Wang, Y., Mushtaq, R. T., & Petra, M. I. (2024). Bridging the cybersecurity gap: A comprehensive analysis of threats to power systems, water storage, and gas network industrial control and automation systems. *Electronics*, *13*(5), 837.

[9] Bilal, H., Ahmed, F., Aslam, M. S., Li, Q., Hou, J., & Yin, B. (2024). A blockchain-enabled approach for privacy-protected data sharing in internet of robotic things networks. *Humcent Comput Inf Sci*, *14*(1), 71.

[10] Echikr, A., Yachir, A., Kerrache, C. A., Oudjida, A. K., & Sahraoui, Z. (2024). Interoperable IoRT for Healthcare: Securing Intelligent Systems with Decentralized Blockchain. *Acta Informatica Pragensia*, *13*(2), 168-192.

[11] Gueye, T., Iqbal, A., Wang, Y., Mushtaq, R. T., & Bakar, M. S. A. (2023). Neuro-robotic synergy: Crafting the secure future of industries in the post pandemic era. *Electronics*, *12*(19), 4137

[12] Chang, S. H., Hsia, C. H., & Hong, W. Z. (2023). A secured internet of robotic things (IoRT) for long-term care services in a smart building. *The Journal of Supercomputing*, *79*(5), 5276-5290.

[13] Hajiabbasi, M., Akhtarkavan, E., & Majidi, B. (2023). Cyber-physical customer management for internet of robotic things-enabled banking. *Ieee Access*, *11*, 34062-34079.

[14] Alamer, A., & Basudan, S. (2022). Security and privacy of network transmitted system in the Internet of Robotic Things. *Journal of Supercomputing*, *78*(16).

[15] Alamer, A. (2022). A secure anonymous tracing fog-assisted method for the Internet of Robotic Things. *Library Hi Tech*, *40*(4), 1081-1103.

[16] Kokovin, V. A., Sytin, A. N., & Skvortsov, V. V. (2022, May). Methods for increasing the cybersecurity of FNC devices on the FPGA-based platform in network communications. In *2022 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)* (pp. 825-830). IEEE.

[17] Dutta, V., & Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. *Electronics*, *10*(22), 2850.

[18] Johansson, T. M., Dalaklis, D., & Pastra, A. (2021). Maritime robotics and autonomous systems operations: Exploring pathways for overcoming international techno-regulatory data barriers. *Journal of Marine Science and Engineering*, *9*(6), 594.

[19] Antenucci, A., Brancati, A., Mazzaro, S., Bastianelli, G., Rovella, R., Massa, A., & Matta, W. (2021, January). An Industrial Distributed Network of Intelligent Robotic Security Guards Based on the Internet of Robotic Things Paradigm. In *2021 International Conference on Computer, Control and Robotics (ICCCR)* (pp. 9-13). IEEE.

[20] Samara, G., Hussein, A., Matarneh, I. A., Alrefai, M., & Al-Safarini, M. Y. (2021, December). Internet of robotic things: Current technologies and applications. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

[21] Romeo, L., Petitti, A., Marani, R., & Milella, A. (2020, June). Internet of robotic things in industry 4.0: Applications, issues and challenges. In *2020 7th International Conference on Control, Decision and Information Technologies (CoDIT)* (Vol. 1, pp. 177-182). IEEE.

[22] Alsulaimawi, Z. (2020, May). A privacy filter framework for internet of robotic things applications. In *2020 IEEE Security and Privacy Workshops (SPW)* (pp. 262-267). IEEE.

[23] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243.

Appendix

Table 1: *Research results*

Ref. num.	RQ1	RQ2	RQ3	RQ4	RQ5
[3]	Confidentiality, integrity and authentication of messages (AEAD tags)	Communication mechanisms (MQTT and ROS2 (DDS) with Ascon-based encryption) but without protocol-level analysis.	Cyber attacks	Lightweight AEAD encryption (Ascon-128) and chaos-based PRNG for keys/nonces, authentication tags, secure message validation, and integrating the crypto layer into MQTT/ROS2 communication	No
[4]	Data authentication, confidentiality, integrity, network isolation and auditability.	TLS-secured IP communication	Network-based attacks, Message integrity & authentication attacks, Application-level attacks	TLS (HTTPS / WSS) for encrypted channel and hash-based signature authentication.	No
[5]	AI/ML security, cyber-physical security, communication security and data integrity and reliability.	TLS-secured IP communication	AI-model attacks, Communication & network attacks, sensor & physical-layer attacks, System & configuration weaknesses	Cryptographic protections, AI security mechanism, access control & authentication, sensor security, network protection and risk mitigation through NIST AI RMF.	Yes
[6]	Cyber and physical security of robotic systems &authentication	IP/WiFi networking without protocol analysis.	Cyber-attacks and physical attacks.	Machine learning techniques for attack detection and additional security measures: firewalls.	Yes
[7]	Data privacy, model integrity and heterogeneity-induced vulnerabilities.	IP-based client–server communication no protocol specified..	Poisoning attacks, Byzantine behaviors , privacy leakage attacks and heterogeneity-driven vulnerabilities	FedMTD and combining: hierarchical cross-silo training and cluster-specific sample-level differential privacy.	Yes
[8]	Ensuring confidentiality and integrity and mitigating the risks of cyber-attacks that can impact physical processes	Modbus / Modbus TCP and Synchrophasor PMU–PDC communication (IEEE C37.118)	Cyber-attacks against ICS environments including: network intrusions, malware infections, unauthorized access, and manipulation of critical physical processes.	Data-driven countermeasures	Yes
[9]	Data privacy and data integrity and tamper resistance.	Blockchain-based channels for data exchange.	Confidentiality, integrity, collision, search/keyword attacks and Server-side attacks	Cryptographic access control, Searchable encryption, Blockchain integrity mechanisms, Smart-contract verification, Secure computation offloading	No

Ref. num.	RQ1	RQ2	RQ3	RQ4	RQ5
[10]	Confidentiality and integrity.	Communication mechanisms (oneM2M, MQTT) but without protocol-level analysis.	Confidentiality, integrity, authentication, centralization risk, insecure communication	Blockchain, ECDSA, smart contracts, oneM2M security, encrypted data	No
[11]	Protection of industrial control systems for sectors such as power plants and water reservoirs.	Mentions communication mechanisms but without protocol-level analysis.	ICS cyberattacks, malware, network intrusion, DDoS-style disruptions, unauthorized access, data tampering	Neural-network intrusion detection, multi-model ML/DL defenses, secure password/patching policies, anti-malware tools, physical ICS safeguards	Yes.
[12]	Confidentiality, integrity and authentication.	MQTT, CoAP, REST over HTTP	Confidentiality risks, integrity threats, authentication weaknesses, insecure IoT/IoMT communication	AES-based encrypted transmission, two-step device authentication, random-key server validation, unique device IDs/PUF.	No
[13]	Privacy of biometric and customer data and secure transmission and storage.	IPFS (Interplanetary File System) as the main communication protocol.	Document fraud, biometric forgery, data tampering, privacy leakage, insecure transmission	Blockchain, deep-biometric KYC, AES/RSA encryption, watermarking, privacy-preserving video masking	Yes
[14]	Confidentiality and integrity.	Communication mechanisms at the cryptographic layer but without protocol-level analysis.	Confidentiality breaches, integrity tampering, message forgery by malicious fog nodes, identity leakage	Proxy re-signcryption, signcryption-based confidentiality, integrity verification, mutual authentication, pseudo-identity protection	No
[15]	Privacy of robot identity & location and anonymity / unlinkability	Fog Computing Network and Roadside Units as fog communication nodes	Tracing attacks, location disclosure, identity exposure by malicious fog nodes	CBF-tree tracing, salted hashing, unlinkability, privacy-preserving fog tracking	No
[16]	Confidentiality of hardware architecture and internal logic and integrity of messages between FNC devices.	Communication Protocol: IEEE Std 1355–1995 (DS-link serial communication interface)	Side-channel attacks, hardware Trojans, JTAG-based access, IP-core vulnerabilities, FPGA configuration tampering	Crypto-Identifiers (CI), TDC-based timing verification, FPGA hardware protection, lossless-compression integrity check	No
[17]	Authenticity and confidentiality.	Communication mechanisms Publish–Subscribe communication model (ROS / ROS2) but without protocol-level analysis.	Information faults, system failures, data eavesdropping, message, tampering, manipulation, network delays, unauthorized access, controller hijacking	Robotic security design methodology (RSDM) and security-by-design engineering principles.	No
[18]	Information security and control system security.	TLS-secured IP communication	Data security gaps, data governance weaknesses, regulatory inconsistencies, confidentiality risks, cyber-risk exposure	Harmonized standards, clear data-ownership rules, secure data storage/transfer, improved governance, liability frameworks	Yes

Ref. num.	RQ1	RQ2	RQ3	RQ4	RQ5
[19]	Identity security and health-related security	General IP/WiFi networking without protocol analysis.	Biometric spoofing / identity fraud and unauthorized access to restricted areas.	Multimodal biometric authentication and thermal scanning and illness detection.	Yes
[20]	Confidentiality, integrity and authentication.	TLS-secured IP communication	Communication attacks (eavesdropping and hijacking).	Encrypted communication and strong authentication mechanisms.	No
[21]	Insecure communication and authentication problems	General IP/WiFi networking without protocol analysis	Communication vulnerability and authentication vulnerabilities	Secure communication channels, authentication strengthening, data-protection mechanisms, multi-source threat analysis	No
[22]	Privacy protection and data confidentiality	LAN/Internet data transmission; security depends on privacy filtering, no protocol choice	Inference attacks, privacy leakage, re-identification, sensitive-data exposure	Privacy filter (PF) autoencoder and adversarial training	Yes

Vesna Hristovska
Faculty of Computer Science,
Goce Delcev University,
Stip, North Macedonia
E-mail address: vesna.hristovska@ugd.edu.mk

Aleksandar Velinov
Faculty of Computer Science,
Goce Delcev University,
Stip, North Macedonia
E-mail address: aleksandar.velinov@ugd.edu.mk

Natasa Koceska
Faculty of Computer Science,
Goce Delcev University,
Stip, North Macedonia
E-mail address: natasa.koceska@ugd.edu.mk