EasyChair Preprint

№ 9792

Robotics Cyber Security Issues

Hadi Dastan Elikhchi and Thaier Hamid

February 28, 2023

Robotics cyber security issues

First Author Hadi Dastan Elikhchi and Second Author Dr Thaier Hamid

University of Bolton
Greater Manchester, England
t.hamid@bolton.ac.uk

Abstract. Robotics Cybersecurity is a rapidly growing and developing area that draws attention from researchers and practitioners. It keeps continuously evolving with better capabilities and advancements in an environment that includes both hardware and software. In this case, a robot can be simple and small but able to increase performance and productivity. Moreover, this technology become an integral part of human lives or even expanded to Robotics automation, space projects, defense, education, and household utilities to medical.

When it comes to Robotics functionalities which is similar to computer systems running by a program that is defined to repeat task or operate. It introduces new threats and vulnerabilities. They are suffering from security issues similar to computer systems that faced for decades must be addressed to secure information and functionality in robotics systems. Therefore, when robots are compromised, which directly impacts two different areas:

Physical elements that may arise concern three key aspects; integrity, confidentiality, and availability of the robot system's operational and functional.

Virtual security and vulnerabilities can be in the provider platforms, misconfigurations, weakness inside of robot system (by design) and risks from data communications channels.

Therefore, we focus on the both physical and virtual problems in robotics systems which is rapidly growing. We also identify existing cybersecurity problems in Robotics, security gaps, weakness, cyber threats, and vulnerabilities. Finally, we provide an overview of findings with better solutions and suggest several strategies and propose direction for further advances in this area.

Keywords: Cybersecurity in Robotics, Cyber-Attacks, Privacy and Safety.

1 Introduction

Nowadays, field of robotics emerging with different technologies such as: human machine collaboration, Industrial Internet of Things (IIoT), Artificial Intelligence (AI) and Machine Learning (ML) to provide better services and at the same time increase performance and productivities [1]. In addition, most of the robots became intelligent with different capabilities, especially more benefited and offered important resources for digitization in the manufacturing industry as well.

According to International Federation of Robotics (IFR) current market value for robots increased by 30% to US$ 9.5 billion in 2019 and at the same time sales are increased [2]. Moreover, most of the robot's system are used into different environments (non-manufacturing) such as professional robots, transportation sectors, hospitals, homes. In this case, some critical requirements must be implemented like overlook cybersecurity factors during the production phases and during the design. Furthermore, some of Robotic applications exposed to cybersecurity vulnerabilities like medical robots, entertainment robots, autonomous cars, educational robots, etc.

These, weaknesses and vulnerabilities in robotic systems opens new research paths. One of the research projects [3], focuses on the design of a distributed robotic system software architecture and on the development of applications framework concept may be implemented to reduce risks. In this case, the key issues that require to be considered during design and add extra protections. Additionally, end users are expecting better security and functionally. At the same time Robotics application architectures should design and develop user friendly interface, by considering standard requirement and key factors like fast prototyping and quick implementations of robotics system [4].

The other research area that is crucial for IoT cyber-security robots, that application-controls machine, should be well designed (trusted) and tested against attacks. Moreover, this is the point developers of robot systems should be aware of weakness and vulnerabilities in system components also, robot programming frameworks.

In general, most of the robots' project s implement their own connections like cloud connectivity's designed with simple encryption systems or even plain text, and robot system designers do not pay enough attention to details of protection systems against any attacks [5]. Nowadays, most of the robotics system functions through internet connectivity's and relying on the connected sensors to collect data and effectors also, they are considered to be cyber physical systems [6]. When a robot connects to internet or external network may revolutionize many areas such as space engineering, civil, military, agriculture, manufacturing, healthcare, and transport. Many cyber-attacks on cyber physical systems have been identified and categorized [7]. For example, cyber-attacks classification presented in Fig. 1. These cyber-attacks classifications are: system, object and vector (attackers acquires access to network or systems) and each one of and each one consequence of a physical system cyber-attack includes the following:

- Attacks can lead to personal injuries or death
- Attacks can lead to data losses or fanatical damages
- Attacks can lead to environmental damage or physical damage to system.

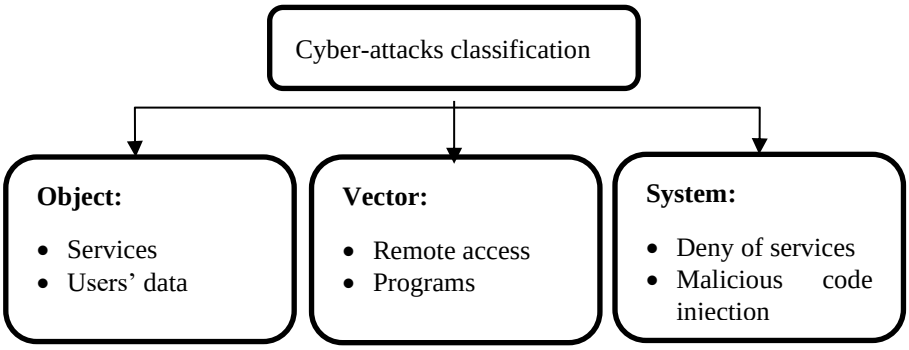

Fig. 1. Example of Cyber-attacks classification.

Therefore, it is important to understand, identify and apply for mitigations in the robotics systems to reduce security gaps, threats, and potential risks. Most critical challenges in robotics fields are related to cyber security risks which is looming over the dawn of yet immature industry and require adapting with capable safety measurements and adding extra security layers [8].

This paper aims to research, collect relevant information, review, and analysis robotics security issues, identify security gaps and vulnerabilities. Section 2, review and analysis all the selected sources. In section 3, highlights key findings related to cybersecurity of robot's system, based on the classified information's. Section 4 present overall conclusion with suggestions to overcome the problems.

2 literature review

2.1 Robotic Systems & Cybersecurity issues

Robotic systems are complex [9], thus their functionalities still pesos big security issues. Therefore, requires more attention to robotic cyber security issues to reduce risks and attacks. In this case by considering all key elements (hardware and software design) to secure robotic systems functions, none of works focused on the detection of an attack on a robot system or connectivity protocols [10]. There are many papers regarding detection and prevention, and some of studies specifically focused on the securing components using IDS and IPS. The table 1 shows some of the selected, recent papers that considered implementation of cyber-security into robotic systems.

Table 1. Some of selected recent studies on implementation of cyber-security in robotic systems.

paper	Function and attacks	Method and Purpose
[11]	Integrity, DoS	ML, detection
[12]	Confidentiality, Security audit	Prevention
[13]	Integrity, Access control	ML, detection
[14]	Integrity, Sensor spoofing	Reaction
[15]	integrity, hidden attacks	Penetration testing

In the two papers [11], and [12] are concerned robot cyber-security and analyzed data integrity and confidentiality. In the [13], authors presented study related to cyber-security in robotic systems, in the event of Sensor spoofing by using reaction method. Moreover, in the [14], work presented an analysis of access control by using machine learning detection system and behavior of robotic system. However, the paper does not address the key issues in robotic systems such as users' data, confidentiality, etc. In the [15], work highlights key performance of robot system functions and applies for hidden attacks to detect vulnerabilities. The author's analysis of research papers from the past few years, and focuses on physical and virtual cyber security in robotic systems also, this literature presents a comparison, highlights key issues in design and shows some of crucial gaps in robotics system may provide access to a considerable amount of data.

Nowadays rapidly increasing power of advanced technology like: Robots had enormous impact on society, operations, manufacturing also, significantly increased their level of functionalities [16]. At the same time Robotics used to consider as "the art of system integration." Therefore, most of Robots offers a wide range of different capabilities, functionalities with usage options of machine to perform tasks by automation. In general, a robot can provide simple functions via designed tools and technology used such as:

User interface: this is the environment that allows user to set or command the system to function and enable option to take control of operable functions through visible framework [17].

Sensor: it allows robot to detect, identify, send, or receive signals and measure environments condition of machine that surround. In this case, Robot sensor converts monitored signals/physical. For example: light intensity, motion, and temperature into electrical signals. These kinds of signals are transmitted to the receiver through provided technology like wireless or wired.

Connectivity: when it comes to Robot port connectivity allows to take control of the entire system [18], and access system files through different options (see Fig 1) like Wireless Fidelity (WIFI), Universal Serial Bus (USB) ports or even Registered Jack (RJ-45), etc.

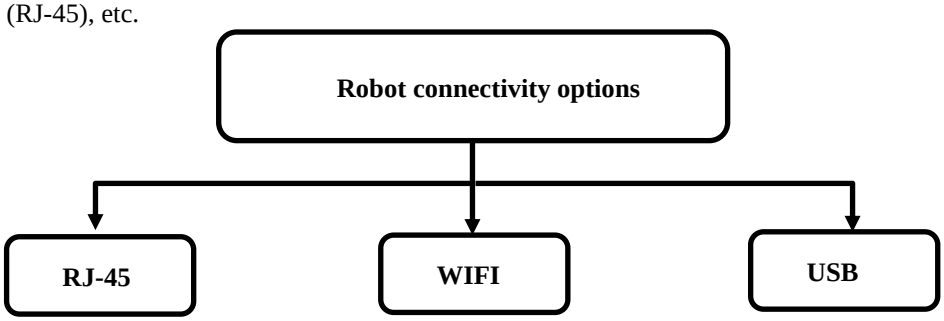

Fig. 2. Example of Robot port connectivity's options.

The majority of robots are provided with abilities to act, process, and sense the environment around them [19]. This field of robotics technology benefited from a variety of disciplines via continued advancements in manufacturing techniques, sensor fabrication, material science, computer science, and mechanical engineering.

Therefore, some of Robots are only designed for specific environments and different tasks. For example, repairing, assembling, mechanical cutting, that may not suitable for medical use or may not readily adaptable to other applications. Furthermore, when it comes to Robot physical/wireless connectivity's (data communications) it is important to classify and consider peculiar aspects of robotic systems with CIA triad data security [20] such as:

Availability: this section ensuring authorized user able to access resources into reliable manner. The inability to reach out to data can cause by a hack, attack, or malicious actions like Distributed Denial of Service attacks or even by a diester like fire. In addition, any failures of hardware or software can comprise availability too.

Integrity: it is the other key element which may undermine the security of robotic machines with a violation of their integrity, which implies the possible deletion or modification of stored data. This is a big risk to robots that constantly expose, it can be manageable via Intrusion Detection and prevention systems.

Confidentiality: it is offering to keep control of the access data and ensures who are authorized have access to specific assets also, able to avoid unauthorized disclosure. In this case, the robot's data can be violated in many ways such as man-in-the-middle attacks [21]. Robotic system requires to have additional protection layers [22] such as:

- Integrity: Robotic controllers should be minimizing the impact of potential risks and any incidents that can involve with physical parts. For example, by avoiding collisions.
- Safety: Robot system should be able to offer information's availability to users and operators. This section of requirement enabling human operators to make decisions based on the safety or even perform emergency procedures when required.
- Accuracy: any robot requires to send actuators commands and functions.
- Security and privacy: any robot require to provide necessary Security and privacy by following (Data protection act, ISO standards, policy and guidance) [23].

2.2 Cyber Threats

Cyber security and potential physical attacks on robot's result in massive risks to properties and life [24]. In general, mechanical components of robots such as: wheels, gears, motors, grippers which enables robot's machine to operate, lift and grab items, can pose serious cyber threats when controlled by any malicious attackers to robot's system. Robot's data Communications via ports, connectivity's network links, allows attackers to take advantages and exploit vulnerabilities in the systems [25]. This is including robotic platforms vulnerabilities, misconfigurations, use of insecure protocols, denial of service (DoS) attacks, malware, etc. For example, the following **Error! Reference source not found.** shows recent attacks associated with physical attacks and cyber security issues [26].

Table 2. Examples of physical security attacks and cyber security issues in robot's systems.

Location	Investigation	Event
Japan, Tokyo	Robotic system misconfigured	Robot by using AI and detected frogs for trucks [27].
UK, Cambridge	Developers made 3D image to fool robot which attacked by Robot	Robot by using AI and attacked to 3D [28].
US, shopping mall	Robot platform misconfigured and attackers exploited vulnerabilities	Floor cleaning robot (Toddler run over) [29].
US, military	Malware into robot system	Soldiers shot dead by robot [30].

3 Key Findings (weakness and security gaps)

Robotics issues are not only limited to one area, but so many factors that can impact or even lead into exploiting security gap, vulnerability to attack robotics platforms, applications, and entire system functionalities. Therefore, this paper aim is to identify

security gap, vulnerability, and potential risks. This is including detection of weakness, classifying into various categories, and overcome the problems [31].

These findings are based on the gathered information's form researches and investigations of robotics system. Moreover, the following are the top twelve weakness and security issues that detected during reviews from selected resources such as:

- Lack of collaboration: when it comes to configurations that require having a cloud-based account it is clear, there is a lack of collaboration between humans and machines with limited functions [32]. It can impact performance, and activities or even lead to misconfigurations.
- Lack of patches: this is increasing chance of being hacked or advanced attacks. For example: rootkit, remote access to sensitive data [33].
- Lack of advanced intrusion detection system: it is a major security issue, especially when it comes to IDS which mostly depending on the signature, behavior, and anomaly, rather than advanced technology like AI based IDS [34].
- Lack of AI or ML based designs: this can affect functional and operational of robotic system especially when it comes to assigning for a task [35]. In this case, robot system performance and accuracy being affected and limited.
- Lack of advanced security features (by design): this kind of weakness can lead into attacking system, accessing robotic system's architecture also, it will attackers to scan and exploit security gaps [36]. For example, attackers can modify data or inject malicious data.
- Lack of advanced safety feature (by design): it is very risky and it has been proven in the many different real cases of incidents threatening towards users' life's, financial losses, and remarkable number of casualties [37].
- Lack of self-assessing functions: this is leaving robot machine to prone to the possibility of flooding attacks [38]. Therefore, inability to self-assessing, react and retrieve on time reduce further functions degradation in its performance. Self-assessing is necessary to make sure that robot machine able to detect disruptions, can sense faults and at the same time able to reconfigure from backup resources.
- Lack of integrity in the robot system: it is due to the using very weak message authentication protocols and encryption system which can be easily compromised also, manipulate stored, in transit data by attackers to reach out robotic sensitive data too [39].
- Lack of privacy in the robot system: this kind of weakness can be resulted in exposure of entire network in organization and at the same time can affect the reputation.
- Lack of confidentiality in the robot system: it is due to the using of weak algorithms which can be broken and it leads exposure of robotic system and interception of sensitive data [40].
- Lack of advanced configurations: when it comes to robot application included insecure features and setting (Weak default configurations). This type of weakness allows attackers to easily take control of robot functionalities or even disable users' accessibility into system. Hackers or attackers exploiting these weak features that operate at the hardware or software of robot systems [41]. For example; hackers using default passwords to access systems before user manage to change it.

- Security gaps in robot connectivity options (WIFI): these kinds of security gap in access points allow attackers to sniff out and obtain password [42]. It is clear the lack strong encryption system and publicly accessibly of WIFI can make robotic systems are more vulnerable.

4 Conclusion

This paper reviewed the literature by concerning the following topics: the technologies used, current status of cybersecurity and vulnerabilities in robotics systems. In particular, we examined, classified and discussed the current cybersecurity issues in robotics systems and it is clear, there is ongoing challenges, security gaps, vulnerabilities which put users into critical conditions. Moreover, majority of robotic systems suffering from several security weakness which is easier to exploit or deploy dangerous attacks. In addition, some of those weaknesses are extremely dangerous to users as robotic systems relies on them to set up data communications.

Finally, we realized that, in recent decades development in the robotics system and research fields shifted from industrial to intelligent robotics system. This shift established to easier integration, which are capable to provide different areas of robotic researches, such as human-robot interaction, cognitive robotics, artificial intelligence, etc. In this case, the use of ML and AI algorithms lead into new challenges and security issues. Therefore, the paper aims to bring all the relevant studies to identify and address most common vulnerabilities, threats, and risks. The gathered findings show that robotic systems requiring additional protection and detection layers which is necessary to secure operational and functional robotics automation systems.

4.1 Suggestions to improve robotics security:

There are several strategies that organizations and individuals can use to improve the security of robots and their associated systems. Some of the most effective approaches include:

Regular software updates and patches: Keeping software up-to-date with the latest security patches and bug fixes can help protect against known vulnerabilities and potential security threats.

Encryption and authentication: Encrypting sensitive data and using secure authentication methods (such as passwords or biometric authentication) can help protect against unauthorized access to a robot's systems.

Physical security measures: Physical security measures, such as enclosing robots in secure areas or using security cameras, can help prevent unauthorized access and tampering with the robot.

Network security: Securing the network that the robot operates on can help prevent unauthorized access and protect against potential attacks.

User education and training: Training users on the importance of cybersecurity and how to use robots securely can help prevent security incidents and reduce the risk of attack.

Incident response planning: Having a plan in place for responding to security incidents can help organizations quickly and effectively address security threats and minimize the impact of a breach.

Regular security audits: Regular security audits can help organizations to find potential security risks and weaknesses and take steps to address them.

It is important to note that the specific security measures used will depend on the specific robot and its associated systems, as well as the organization's specific security goals and requirements. In some cases, multiple strategies may be used in combination to provide a more comprehensive view of the robot's security posture.

References

1. Dieber B (2021) ArXiv.org e-print archive. In: Robot System Cybersecurity. https://arxiv.org/pdf/2103.05789.pdf. Accessed 10 Feb 2023
2. IFR International Federation of Robotics IFR (2019) International Federation of Robotics. In: IFR International Federation of Robotics. https://ifr.org/. Accessed 10 Feb 2023
3. Zhu Q, Rass S, Dieber B, Vilches VM (2021) Cybersecurity in robotics: Challenges, quantitative modelling, and Practice. In: Foundations and Trends® in Robotics. https://www.nowpublishers.com/article/Details/ROB-061. Accessed 10 Feb 2023
4. Khatib O, Reeves N, Haddadin S (2021) An atlas of physical human–robot interaction. In: Mechanism and Machine Theory. https://www.sciencedirect.com/science/article/abs/pii/S0094114X07000547. Accessed 10 Feb 2023
5. Chen Y (2019) Robot as a service in Cloud computing - ieee Xplore. In: Robot as a Service in Cloud Computing. https://ieeexplore.ieee.org/abstract/document/8705800. Accessed 10 Feb 2023
6. Romeo, L. *et al.* (2020) *Internet of robotic things in Smart domains: Applications and challenges*, *MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/1424-8220/20/12/3355 (Accessed: February 10, 2023).
7. Bhardwaj, A. *et al.* (2022) *Secure framework against cyber-attacks on cyber-physical Robotic Systems*, *SPIE Digital Library*. SPIE. Available at: https://www.spiedigitallibrary.org/journals/journal-of-electronic-imaging/volume-31/issue-6/061802/Secure-framework-against-cyber-attacks-on-cyber-physical-robotic-systems/10.1117/1.JEI.31.6.061802.short?SSO=1 (Accessed: February 10, 2023).
8. Fountas, S. *et al.* (2020) *Agricultural Robotics for Field Operations*, *MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/1424-8220/20/9/2672 (Accessed: February 10, 2023).
9. Tao, B., Zhao, X.W. and Ding, H. (2019) *Mobile-robotic machining for Large Complex Components: A review study - science china technological sciences*, *SpringerLink*. Science China Press. Available at: https://link.springer.com/article/10.1007/s11431-019-9510-1 (Accessed: February 10, 2023).
10. H. PETERSEN, K.I.R.S.T.I.N. (2019) *Design and development of a novel core, balance and lower - IEEE xplore*, *collective robotic construction*. Available at: https://ieeexplore.ieee.org/abstract/document/8779531 (Accessed: February 10, 2023).
11. Adhikari, S. (2021) "Integrating deep reinforced learning and robotic process assessment in Blockchain Digital Transformation for autonomous cybersecurity," *AIAA Scitech 2021 Forum*, pp. 1–3. Available at: https://doi.org/10.2514/6.2021-0662.
12. Vulpe, A. *et al.* (2021) *Enabling security services in socially assistive robot scenarios for Healthcare Applications*, *MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/1424-8220/21/20/6912 (Accessed: February 10, 2023).
13. Mrabet, H. *et al.* (2020) *A survey of IOT security based on a layered architecture of sensing and data analysis*, *MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/1424-8220/20/13/3625 (Accessed: February 10, 2023).
14. Varol, A. (2019) *An overview of Robot Operating System Forensics | IEEE Conference ...*, *Robot Operating System Forensics*. Available at: https://ieeexplore.ieee.org/document/8965649 (Accessed: February 10, 2023).
15. Yankson, B. (2021) *Security assessment for Zenbo robot using drozer and mobsf frameworks*, *Security Assessment*. Available at: https://ieeexplore.ieee.org/abstract/document/9432666/ (Accessed: February 10, 2023).

16. Malham, G.M. and Wells-Quinn, T. (2019) What should my hospital buy next? -guidelines for the acquisition and application of Imaging, navigation, and robotics for spine surgery, Journal of spine surgery (Hong Kong). U.S. National Library of Medicine. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6465454/ (Accessed: February 10, 2023).
17. Suzuki, R. *et al.* (2019) "ShapeBots: Shape-changing swarm robots," *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*, pp. 1–3. Available at: https://doi.org/10.1145/3332165.3347911.
18. Tae, K. (2020) *Transoral robotic thyroidectomy using the da vinci single-port surgical system, Gland surgery*. U.S. National Library of Medicine. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7347821/ (Accessed: February 10, 2023).
19. SHIH, B.E.N.J.A.M.I.N. (2019) *Electronic skins and machine learning for - science robotics, electronic skins and machine learning for intelligent soft robots*. Available at: https://www.science.org/doi/10.1126/scirobotics.aaz9239 (Accessed: February 14, 2023).
20. Nguyen, T. (2019) *A deep look into privacy and security of vacuum robot - CPP, Privacy and Security of Vacuum Robot*. Available at: https://www.cpp.edu/cyberfair/poster-information/documents/vacuum-robot-abstract.pdf (Accessed: February 12, 2023).
21. Portugal, D. (2019) A novel solution for Securing Robot Communications based ... - IEEE xplore, securing robot communications based on the MQTT protocol and ROS. Available at: https://ieeexplore.ieee.org/abstract/document/8700390/ (Accessed: February 10, 2023).
22. Yaacoub, J.-P.A. *et al.* (2021) "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, 21(1), pp. 115–158. Available at: https://doi.org/10.1007/s10207-021-00545-8.
23. Salvini, P., Paez-Granados, D. and Billard, A. (2021) "On the safety of mobile robots serving in Public Spaces," *ACM Transactions on Human-Robot Interaction*, 10(3), pp. 1–27. Available at: https://doi.org/10.1145/3442678.
24. Bhardwaj, A. (2021) *What can machine learning do for information security, Cyber security attacks on robotic platforms*. Available at: https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2819%2930050-9 (Accessed: February 10, 2023).
25. S. Schwarzman, L. (2020) A comparison of perioperative outcomes between single-port and multiport robot-assisted laparoscopic prostatectomy, European Urology. Elsevier. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0302283820302062 (Accessed: February 12, 2023).
26. L. J. Drews, P. (2022) *Multi-physical field analysis of a temperature sensor for ..., Detecting Data Injection Attacks in ROS Systems.* Available at: https://ieeexplore.ieee.org/abstract/document/10043811 (Accessed: February 12, 2023).
27. Jecker, N.S. and Nakazawa, E. (2022) *Bridging East-west differences in ethics guidance for AI and robotics, MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/2673-2688/3/3/45 (Accessed: February 12, 2023).
28. Bhardwaj, A. (2021) *What can machine learning do for information security? Cyber security attacks on robotic platforms*. Available at: https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2819%2930050-9 (Accessed: February 10, 2023).
29. Tan, S.R.X. and Han, J. (2020) *Spying with your robot vacuum cleaner: Proceedings of the 18th Conference on Embedded Networked Sensor Systems, ACM Conferences*. Available at: https://dl.acm.org/doi/abs/10.1145/3384419.3430781 (Accessed: February 10, 2023).
30. Payal, M. (2021) *Robotics, AI, and the IOT in Defense Systems - Wiley Online Library, Robotics, AI, and the IoT in Defense Systems*. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119711230.ch7 (Accessed: February 10, 2023).

31. Galin, R. (2019) *Automation and robotics in the context of industry 4.0: The shift to ...*, *Automation and robotics in the context of Industry*. Available at: https://iopscience.iop.org/article/10.1088/1757-899X/537/3/032073 (Accessed: February 12, 2023).
32. Arents, J. *et al.* (2021) *Human–Robot Collaboration Trends and safety aspects: A systematic review*, *MDPI*. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/2224-2708/10/3/48 (Accessed: February 12, 2023).
33. Yaacoub, J.-P.A. et al. (2021) Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations - International Journal of Information Security, SpringerLink. Springer Berlin Heidelberg. Available at: https://link.springer.com/article/10.1007/s10207-021-00545-8 (Accessed: February 12, 2023).
34. R. Teixeira, R. (2019) *Security on ROS: Analyzing and exploiting vulnerabilities ... - IEEE xplore*, *Security on ROS*. Available at: https://ieeexplore.ieee.org/abstract/document/9307107/ (Accessed: February 12, 2023).
35. O'Sullivan, S. (2019) Legal, regulatory, and ethical frameworks for- Wiley Online Library, frameworks for development of standards in artificial intelligence. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/rcs.1968 (Accessed: February 12, 2023).
36. Galambos, P. (2019) *Cloud, fog, and Mist Computing: Advanced robot applications | IEEE*, *Advanced Robot Applications*. Available at: https://ieeexplore.ieee.org/abstract/document/8960619/ (Accessed: February 12, 2023).
37. Haidegger, T. (2020) *Autonomy for surgical robots: Concepts and paradigms*, *Autonomy for Surgical Robots:* Available at: https://ieeexplore.ieee.org/abstract/document/8698847/figures (Accessed: February 12, 2023).
38. Ovejero, &A., Sierra-García, J.E. and Santos, M. (2019) *Evaluation of an interactive guide for Robotics Self-Learning*, *SpringerLink*. Springer Nature Switzerland. Available at: https://link.springer.com/chapter/10.1007/978-3-031-18409-3_21 (Accessed: February 12, 2023).
39. Ullman, D. (2020) *A multidimensional conception and measure of human-robot trust*, *Trust in Human-Robot Interaction*. Academic Press. Available at: https://www.sciencedirect.com/science/article/pii/B9780128194720000010 (Accessed: February 12, 2023).
40. Lutz, C. (2019) *The privacy implications of Social Robots: Scoping - sage journals*, *The privacy implications of social robots*. Available at: https://journals.sagepub.com/doi/abs/10.1177/2050157919843961?journalCode=mmca (Accessed: February 11, 2023).
41. Giordano, G. (2019) *Reshaping antitumor immunity with chemo ... - wiley online library*, *Autonomous Soft Robots*. Available at: https://onlinelibrary.wiley.com/doi/full/10.1002/adfm.202100437 (Accessed: February 11, 2023).
42. Grau, A. (2020) *Robots in industry: The past, present, and future - IEEE Xplore*, *Robots in Industry*. Available at: https://ieeexplore.ieee.org/document/9305203 (Accessed: February 12, 2023).