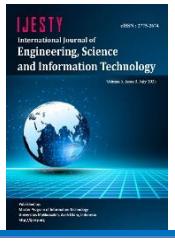
International Journal of Engineering, Science and Information Technology
Volume 5, No. 3 (2025) pp. 382-387
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i3.1059
Research Paper, Short Communication, Review, Technical Paper



Cyber Security of Robots: Integrating Safety and Security in Cognitive Social Computers

K. Parthiban[1]*, R. Kanchana[2], P S V S Sridhar[3], N. V. Krishnamoorthy[4], P.S.G. Aruna Sri[5]

[1]Department of Computer Science, N.K.R. Government Arts College for Women, Namakkal, India
[2]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India
[4]Department of Mechanical Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India
[5]Department of Internet of Things, Koneru Lakshmaiah Education Foundation, Guntur, India

**Corresponding author E-mail: rkparthiban2013@gmail.com*

The manuscript was received on 11 February 2025, revised on 18 March 2025, and accepted on 20 June 2025, date of publication 30 June 2025

Abstract

For social robots to coexist with people, they must be trustworthy and safe. This study examines the implications and relationships between cybersecurity and safety to develop more intelligent, secure, dependable autonomous robots. The initial findings are presented in this publication. Robots are used extensively in the modern world, not just in automated cars and medicine but also in industry, national security, and defence. Cyberattacks against robots and other security concerns are rising with the number of robots. We propose creating a robotic intrusion prevention system (RIPS) that employs a cutting-edge methodology to identify and stop intrusions in cyber-physical systems, including cognitive social robot systems. To mitigate cyber-physical risks, the RIPS uses system modes to specify which robotic system components limit or decrease its functioning when the system is penetrated. The RIPS detects threats at the robotic communication level. Additionally, we show that enhancements in encryption, authorisation/authentication, and physical security can considerably lower the probability of cybersecurity threats on robotic platforms. A dual regulatory framework that governs cybersecurity and physical product safety separately makes it challenging to regulate cyber-physical systems like care robots consistently and effectively. We conceive and talk about the difficulties in controlling the security of cyber-physical systems using the current dual framework, especially the absence of required certificates. Various robotic systems' security levels are examined in multiple domains to ascertain whether they need an upgrade or correction. Additionally, we outline and highlight open challenges that may emerge over the coming years.

Keywords: *Cyber-Attacks, Robotic Intrusion Prevention System, Communication Level, Cognitive Social Robot, Cybersecurity.*

1. Introduction

Robots are frequently cited as typical instances of Cyber–Physical Systems (CPS) with physical and computational capabilities. The use of robotic systems in human civilisation is expanding quickly when CPS is integrated into systems with sophisticated channels for interaction, leading to enhanced sensing abilities, efficient control, and prompt actions based on real-world characteristics [1]. Because of this, M2M communication is increasingly being examined, so CPS network security has grown in importance. Furthermore, CPSs typically involve networked robots outfitted with AI and engaging with people in public or professional contexts. Robotic applications, such as networked robots, have greatly improved the physical and mental capacities of regular human travelers or the old and crippled in recent years. Since personal and professional service robots are developing quickly, their security must be improved. Humans and autonomous robots coexist in social settings in a range of locations, including as residences, places of employment, and even essential facilities like banks and airlines. Thus, their protection and safety are crucial, especially considering that they are supposed to behave independently of humans and that their independence is growing.

Figure 1 shows two abstract communication levels. Each robot control system's local communication is the focus at the behavioural level. In this case, one or more computational nodes may have the control system installed. The phrase "communication level" refers to the global information sharing between internet archives and robot controllers or between controllers of several robot systems. Modern robotics increasingly frequently employs data and information gathered in internet clouds or operates as a multi-robot system, expanding the share of global connection [2].

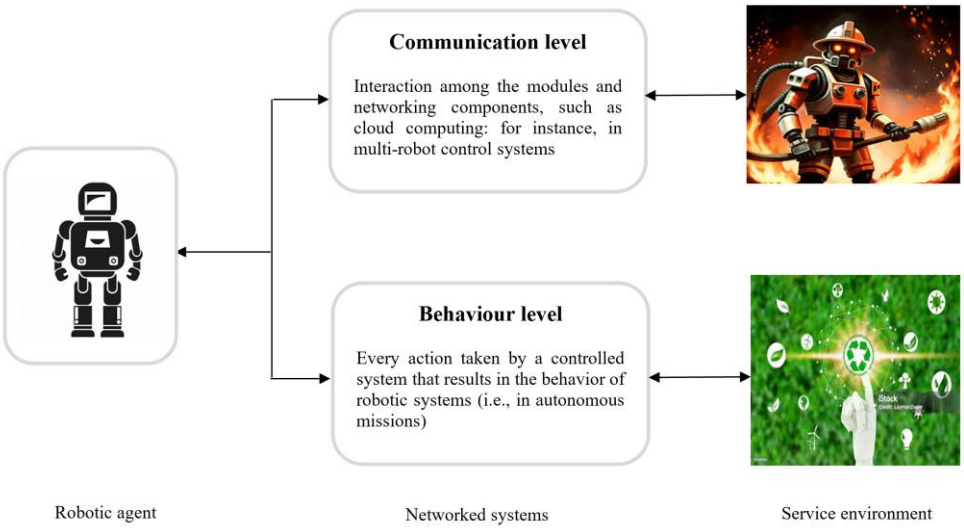


Fig 1. Two-level communications in networked robotic platforms. The interaction between system modules and networking components is the focus of the communication level. Behaviour level describes how system modules make decisions locally.

This study discusses cyberattacks unique to CPS, techniques for spotting them, and defences [3]. The following is the rest of this document. Background information and related works are presented in Section 2. The approach used for this investigation is given in Section 3. The results collected are discussed in Section 4, along with any limits, validity threats, and suggestions for further research. The work is concluded in Section 5.

2. Literature Review

The primary purpose of industrial robots is to decrease the need for human labour. Artificially intelligent robots can now complete tasks more quickly, safely, and effectively [4]. These occupations include quality control, construction, manufacturing, and transportation. Specifically, robots are being utilised to carry out risky activities in unsafe environments. Additionally, they can outperform humans in repetitive tasks with the same degree of precision. In medicine, robots have been utilised for remote therapy, virtual care, and telemedicine. Their purpose was to function as hospital, surgical, and medical robots. New medical robots can do cardiopulmonary resuscitation (CPR), and they are used to execute minor procedures precisely.

Recent academic studies offer insights into complex security issues and suggest creative solutions to support SRPS, which requires a contextual design for security [5]. Examine robot cybersecurity, describing different attack forms, effects, and defence strategies while emphasising the changing difficulties in cloud robotics, artificial intelligence, and robot forensics. By classifying risks, analysing the attack surface, and encouraging users to understand and follow security-by-design rules, the security of SRPS suggests a way to transition between architectures according to environmental conditions, improving robotic systems' versatility and failure management.

Humanoids typically integrate software and hardware from reliable supply chain partners. This trusting relationship introduces another component of a potential attack surface. These social robots will work in dynamic public areas susceptible to environmental and human influence, which raises the risk of various physical attacks, including sabotage, theft, and vandalism. Users may also be physically harmed during engagement due to malfunctions or cyberattacks [6]. When a malevolent actor controls a humanoid, it may lead to a terrorist strike; a framework that focuses on real-time monitoring and system health reconfiguration to defend collaborative robotic cyber-physical systems from cyberattacks.

The authors examined recent studies that suggested employing robotic and thermal imaging technology to detect intruders and infiltrators in frontier defence systems [7]. This study looked at both cyber and physical threats to automation, involving networks, IoT sensors, and robots. These systems integrated network links that sent photos to the command centre, IoT sensors for sound identification, and robotic motors that linked laser and infrared weaponry centre. Decisions were made to start the mitigation and detection procedures. A robotic flight control system for vehicle movement was proposed, along with several theories on alleviating traffic jams in urban areas. This technology may be able to eliminate obstacles and traffic bottlenecks.

The threat landscape and risk assessment, attack vectors and major security issues, and 5G MEC Security are some of the viewpoints from which numerous studies have examined the cybersecurity risks to 5G networks [8]. Nevertheless, there are other risks to SRPS use cases outside cybersecurity, like supply chain, public space, and social and physical hazards, which haven't gotten much attention in earlier research. Studies that did not consider the particulars of SRPS use cases served as the foundation for the 3GPP safety systems and protocols for the 5G system. Due to the large amount of environmental data that must be processed at the 5G MEC, SRPS—which are power-constrained devices—need more traffic in their uplink than Augmented Reality/Virtual Reality (AR/VR) use cases, which call for higher traffic in the downlink of a 5G network.

However, new developments in AI and cyber systems [9], such as robots and cobots, create questions such as whether these machines put workers at more risk, result in unfair treatment, or can even be used for profit. The idea of machinery is one of the first things that has evolved throughout time, as it is not yet apparent if this definition includes all of the new cyber-physical devices, such as AI agents and collaborative robots. This situation is further complicated because present standards refer to robots and robotic devices rather than machinery, and vice versa, with enacted or proposed legislation concentrating on equipment.

Unlike their autonomous counterparts, autonomous vehicles (AVs) and uncrewed aerial vehicles (UAVs), which have relatively high operational speeds, social robots will occasionally function at relatively moderate speeds or in immobile locations. Furthermore, this feature leaves the humanoids vulnerable to simple attacks like jamming and spoofing, blindness, and so forth, as well as passive attacks like reconnaissance. The human component and the AI system are additional possible targets for attacks on social humanoids [10]. Insufficient understanding of the danger actors, attack surface, and threat environment for social robots in public areas is a current issue.

Organisations and other stakeholders must also comprehend possible assault scenarios to assess and control the risks related to social robotics as a business venture. Consequently, any company continuity strategy must identify potential hazards and evaluate their effects to prevent regulatory penalties.

3. Methods

3.1. Research Paths in Cybersecurity for Robots

Developing various techniques that address every facet of service robot cybersecurity is among the most significant challenges in robot security. A highly complicated control system that is frequently dispersed over the network is typically used by service robots. It is also well-equipped with various sensors to study the surroundings. Determining the risks and weaknesses of a standard service robot control system is the first stage in designing a security system for such a robot. The creation of safe techniques and instruments should come after this stage. A preliminary study of these system hazards is shown in Figure 2 [11]. The following conclusions have been drawn from the analysis.

A low-level robot controller gives a robot application access to vital data about the robot and its surroundings [12]. Moreover, it is capable of controlling robot effectors. Consequently, authentication should be required for every request that might communicate using the low-level driver. This security measure is essential when robot apps are downloaded from a distant repository.

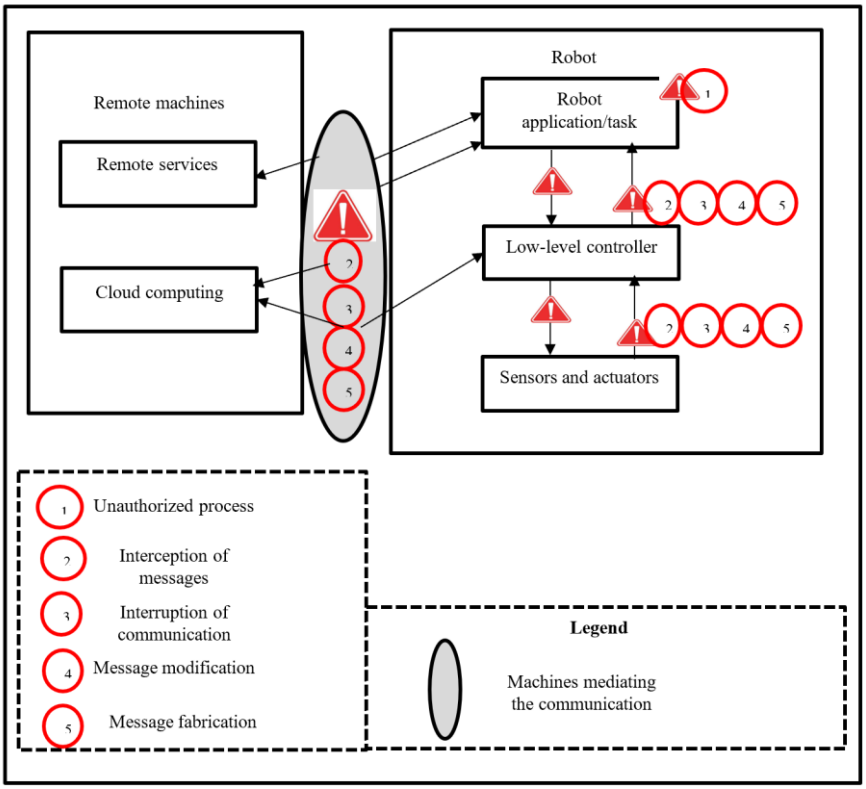


Fig 2. Examples of threats to a complex, distributed control system of a service robot

3.2. Cybersecurity in distributed robotic frameworks

The fundamental security objectives for a robotics system composed of dispersed components are as follows [13]:

1. Confidentiality: Access to the transmitted data must only be restricted to authorised principals.
2. Integrity: An unauthorised principal cannot alter the transmitted data.
3. Authentication: Only authorised principals may generate the data that is communicated.
4. Availability: The components need to be operational and delivering the relevant service.

The threat model for communication protocols typically assumes that an opponent can:

1. Behave similarly to any other network node, meaning it can send and receive messages.
2. Access to other nodes' messages. The adversary can view, alter, and delete messages from different nodes [14]. Specific attacks include taking control of the network infrastructure, such as routers or access points, or targeting the physical layers, like flooding channels with noise. All that is needed for passive attacks is observation. Active attacks, however, necessitate interference.

3.3. Types of attacks on robotic platforms

3.3.1. Physical

Hardware-based assaults are referred to as physical layer attacks. A precipitate of potential risks to CPS systems is provided. Addressing security using a single generalised model is highly challenging because of the diversity of CPS systems and components. As a result, this issue was examined from a security standpoint, beginning with the viewpoint of the CPS systems and then moving on to the CPS components. Because the material component of CPSs exposes many potential vulnerabilities and assaults, it may be helpful to be aware of potential attacker profiles to prevent them. Physical attacks can pose a serious threat to CPSs because it has been demonstrated through the classification and comparison of assailant models on CPSs that there are no widely utilised attacker models to target. A

robotic car's code-controlling microcontrollers might be the subject of hardware-based attacks, affecting battery or motor performance, providing erroneous commands, or even destroying the robot's parts. Such outcomes can be readily obtained by utilising orders that deplete the vehicle's battery or by accessing the person who operates the connection to get a complete set of compromised procedures.

3.3.2. Networking

"Network Attacks" are hostile operations carried out via distant connections without requiring direct access to physical ports, substantially increasing the attacker's range of options. Generally, sensors are among the most crucial and sensitive components of robotics regarding internet attacks, and are readily exploitable with cyberattacks. "Three forms of cyberattacks on sensor measurements were used and examined: stealthy attacks, scaling, and false data injection." Addition influenced sensor measurements in injection attacks, whereas multiplication was used in scaling assaults. Wireless methods such as NFC and Wi-Fi manage CPSs in various settings.
Every technology displayed its risk profile and known vulnerabilities linked to attacks, including data corruption, eavesdropping, and modification. Man in the Middle (MITM) tested techniques like spoofing and DoS attacks on Real Time Positioning Systems. DoS attacks were successful in interfering with the beacons' signal. Spoofing, however, altered the beacons' signal, causing mistakes and leading to an inaccurate tag location calculation.

3.3.3. Operating system

Operating system attacks exploit vulnerabilities in support software, including Linux-based operating systems or ROS, which serve as many robots' brains. According to an analysis of 176 threats taken from the machine's susceptibility database, 92.6% were primarily software-related (see figure 3), demonstrating that software in automated systems is a more serious hazard than hardware.
Ten current defence techniques are examined in an illustrative networking setup to find realistic profiles of attackers that primarily threaten ROS-based robotic systems. The outcomes for ROS 1 and ROS 2 offered helpful information and recommendations to assist subject-matter specialists in selecting the best defences for their situation against MITM and ROS node attacks. When working with active surveillance systems with multiple robots, Posting fake messages that alter velocity commands to distract a robot and sending terminating commands to control or delete any ROS node are quick and easy tasks for a hacker within the network. Node-to-node and unencrypted ROS-to-ROS interaction via unsecured ports is another ROS attack.
ROSPenTo and ROSchaos are strong tools that exploit ROS vulnerabilities and show how attackers focusing on APIs can damage ROS apps to simplify penetration testing for ROS. Another tool that can intercept, alter, and stop two ROS nodes from communicating. The tool's implementation is briefly compared to ROSspent, and it was tried on a domestic robot named Doris, demonstrating the possibility of totally impairing its functionality by losing control of its communication connection. ROSploit, a tool created specifically for this purpose, is another resource that helps researchers test exploitation for ROS.

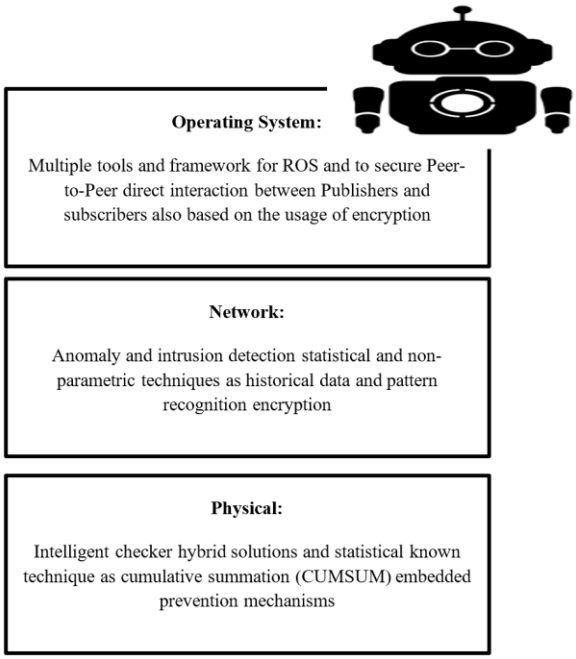


Fig 3. Main techniques adopted to protect robots

3.4. Training and creation for human-robot interaction

In addition to demonstrating complex problem-solving techniques, the robotic agent must exhibit pertinent and socially engaging behaviours to receive a sufficient HRI. Ultimately, people will engage with independent social agents who create and learn new social behaviours and adjust to novel social situations. By adopting a bottom-up embodied thinking and internal development strategy, the contributions in this section aim to achieve autonomous behaviour in robots and are at the heart of developmental robotics, bridging the gap between cognitive and social robotics. The contributions demonstrate that a wide variety of socially engaging behaviours, including attention-grabbing emotive facial expressions, trust, and theory-of-mind, can result from these biology- and psychology-inspired social robot systems.
Significantly, these viewpoints immediately contribute to new understandings in developmental psychology, such as the clinical understanding of autism spectrum disorder and the developmental mechanics of social behaviour. Collectively, these contributions shift the focus from totally top-down, scripted robotic systems—which are frequently seen in robotic systems demonstrations—to fully self-

sufficient social agents that draw inspiration from and expand upon fundamental ideas in neuroscience and psychological theory. These results offer a framework and paradigm to methodically examine unanswered concerns about human development, even as they already offer crucial insight into the creation of autonomous robotic systems. By examining the effects of preterm delivery on the formation of body schema and sensorimotor unification in the human fetal body model, for example, Kuniyoshi demonstrates the potential. These findings directly affect disorders like autism spectrum disorder, which have deficits in these mechanisms.

The artificial curiosity of an embodied physical entity can lead to self-awareness, motion detection, and infant-like exploratory activities in a non-social setting. In a social setting, however, this can lead to a range of social behaviours, including attempting to attract the attention of other agents by making eye-catching facial expressions. Importantly, these are emergent qualities of artificial curiosity within a living thing rather than preprogrammed behaviours.

4. Results and Discussion

4.1. Implementation and Experimental Results

According to others, there is no requirement to control robot cybersecurity, as the market will handle this. Indeed, it is somewhat in the best interests of robot creators, manufacturers, and consumers to ensure cybersecurity. However, given the industry's competitive challenges, producers can be motivated to prioritise a speedy market launch and only aim to safeguard their products subsequently [15]. It should come as no surprise that manufacturers prioritise developing robots that can execute a range of jobs over protecting them from all assaults, given that developing an automated system is technically extremely difficult in many aspects. Cyberattacks may not immediately impact manufacturers, and enhancing cybersecurity is expensive. Nonetheless, including cybersecurity in the technology's architecture could encourage a safer system that, in the long run, might benefit both consumers and producers.

Economic literature suggests that improving cybersecurity by implementing methods to align actors' incentives may lessen the disparities between private and societal costs and benefits. As previously stated, EU regulations should theoretically help care robot producers gain from improved safety in two ways. First, safety regulations, which increasingly include cybersecurity concerns, apply to manufacturers. First, safety regulations, which increasingly include cybersecurity concerns, apply to manufacturers. Second, robot buyers are encouraged to spend money on goods that lower liability risks and help them comply with the GDPR and possibly even the NIS Directive. Some incentives for maintaining cybersecurity are provided by both legal frameworks for safety and cybersecurity. As covered below, there is room for improvement in integrating the two frameworks.

Furthermore, practically speaking, it's unclear if buyers of robots can tell the difference between those with excellent cybersecurity and those with less-than-ideal cybersecurity. Introducing sufficient European cybersecurity certifications might lessen this knowledge gap, which would provide robot buyers with some security assurance.

4.2. Creating more explicit links between cybersecurity and safety regulation

The regulatory framework governing the safety of robotics and other connected items is disjointed and requires updating. Manufacturers are the focus of basic safety regulations, although different laws, like the GDPR, target various players, including varied roles that robot users may play. At best, there aren't many connections between these frameworks.

Robot manufacturers are responsible for ensuring the safety of their products, and they must resolve cybersecurity issues if they are severe enough to jeopardise user safety. However, the real question is how thorough and precise these cybersecurity evaluations are [15]. The MDR offers cybersecurity-focused standards that are an excellent place to start if it is decided that the robot is medical equipment. Without particular cybersecurity standards, the overall product safety framework takes effect. Generally speaking, safety is wide enough to include defence against cybersecurity threats that could have adverse safety effects. However, it is unclear if cybersecurity is given enough attention when manufacturers evaluate safety hazards without precise and unambiguous criteria.

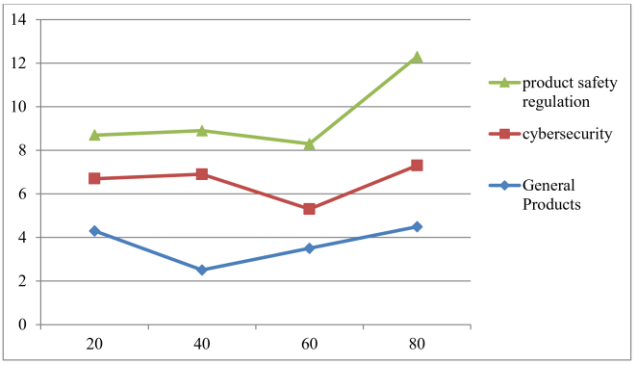


Fig 4. Increasing the connection between product safety regulations and cybersecurity

There are several ways to improve the connection between safety and cybersecurity (see Fig. 4). First, a single piece of law that covers every device that is connected (or at least ones for which risks related to cybersecurity would put users at significant risk) might handle the issue of physical and cyber security using a horizontal approach. However, it's unclear if such a substantial adjustment is necessary.

Following and building on the MDR's model, a second, vertical strategy may incorporate cybersecurity obligations more thoroughly and openly into contemporary systems, like the Toy Regulation and the RED. This strategy would concentrate on revising current, partially underway laws, such as the General Product Safety Directive amendment. In addition to potentially altering the legal text of GPSD, this strategy might also help allow for a more flexible interpretation of the current regulations (for example, expanding the concept of safety to cover cybersecurity specifically).

4.2. Forensics of robots

Cybercrime using robots is already rising in tandem with their increased use. Since hackers will increasingly target robots, forensics investigations seem like a crucial area to look into. There is currently no established approach or procedure for machine forensics, even though there are several studies regarding ROS forensics.

The interaction between ROS and the robot's parts, which contributes more data throughout this procedure, presents particular difficulties for real-time investigation.

Accurately gathering evidence from ROS presents a new problem for investigators. Additionally, ROS can store and preserve vast amounts of information that investigators find challenging to access over the network. Additionally, if researchers want a ROS gadget in their lab, the robot's size poses a new challenge. This is especially true if the robot is larger or more human-like.

The authors of a different study on ROS summarised "Robot Operating System Forensics" and discussed a few discoveries. One of the issues raised in the research is the difficulty of differentiating between the impact of software bugs and active attacks, as forensics aims to identify possible attacks and their consequences. The authors also raised issues regarding RAM acquisition in ROS systems. A study on "further detailed ROS inquiry, where they additionally utilised memory volatile forensics for ROS" was included, along with a review of papers that looked at ROS security, to address queries such as "will ROS instances be secure if they are connected to the internet?"

5. Conclusion

Patient injury could result from taking advantage of care robot security flaws. In delicate application domains like healthcare, this is particularly difficult. A number of laws that apply to different application industries, like the GDPR, the Equipment Directive, or medical devices regulation, provide standards pertinent to care robots even if there isn't a single legal framework for robot cybersecurity.

This approach aligns with the current EU institutions' efforts to reform the entire General Product Safety Directive. This tactic could change the legislation or permit a more liberal interpretation of the existing rules (for example, specifically mentioning cybersecurity-related issues). We also recommended implementing cybersecurity regulations relevant to CE marking in order to appropriately address the broader safety implications of cybercrime. In general, the increased interconnectedness of products—including robots—raises cybersecurity issues and necessitates updating the safety framework.

References

[1] V. Dutta & T. Zielińska, “Cybersecurity of robotic systems: Leading challenges and robotic system design methodology,” Electronics, vol.10, no. 22, pp. 2850, 2021.

[2] A. Botta, S. Rotbei, S. Zinno, & G.Ventre, “Cyber security of robots: A comprehensive survey”. Intelligent Systems with Applications, vol.18, no.200237, 2023.

[3] A. Moallem, (Ed.), “Smart and Intelligent Systems: The Human Elements in Artificial Intelligence, Robotics, and Cybersecurity”. CRC Press, 2021.

[4] J. P. A. Yaacoub, H. N. Noura, O. Salman, & A, “Chehab, Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations”. International Journal of Information Security, vol.21, no. (1), pp.115-158, 2022.

[5] S. Oruma, R. Colomo-Palacios, & V. Gkioulos, “Architectural views for social robots in public spaces: business, system, and security strategies”. International Journal of Information Security, vol.24 no. (1), pp.1-48, 2025.

[6] S. O. Oruma, M. Sánchez-Gordón, R. Colomo-Palacios, V. Gkioulos, & J. K Hansen, “A systematic review on social robots in public spaces: Threat landscape and attack surface”. Computers, vol.11no. (12), pp.181, 2022.

[7] E. Fosch-Villaronga, & T. Mahler, “Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots”. Computer law & security review, vol.41, no.105528, 2021.

[8] M. K. Warbhe, P. Verma, S. Gundewar, & A. Gudadhe, “A Review on the Applications of Cyber Security in IoT-Integrated Robotics”. In International Conference on ICT for Sustainable Development (pp. 347-357). Singapore: Springer Nature Singapore, 2024, August.

[9] A. G. Sreedevi, T. N. Harshitha, V. Sugumaran, & P. Shankar, “Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review”. Information Processing & Management, vol.59no. (2), pp.102888, 2022.

[10] A. Makkar, & J. H. Park, “SecureCPS: Cognitive inspired framework for detection of cyber attacks in cyber–physical systems”. Information processing & management, vol.59no. (3), pp.102914, 2022.

[11] S. O. Oruma, & S. Petrovic, S. “Security threats to 5G networks for social robots in public spaces: a survey”. IEEE Access, vol.11, no.63205-63237, 2023.

[12] A. Martinetti, P. K. Chemweno, K. Nizamis, & E. Fosch-Villaronga, “Redefining safety in light of human-robot interaction: A critical review of current standards and regulations”. Frontiers in chemical engineering, no.3, pp.666237, 2021.

[13] S. O. Oruma, M. Sánchez-Gordón, R. Colomo-Palacios, V. Gkioulos, & J. K. Hansen, “A Systematic Review on Social Robots in Public Spaces: Threat Landscape and Attack Surface”. Computers vol.2022, no.11, pp.181, 2022.

[14] H. He, J. Gray, A. Cangelosi, Q. Meng, T. M. McGinnity, & J. Mehnen, “The challenges and opportunities of human-centered AI for trustworthy robots and autonomous systems”. IEEE Transactions on Cognitive and Developmental Systems, vol.14 no. (4), pp.1398-1412, 2021.

[15] , A. G., Sreedevi, T. N. Harshitha, V. Sugumaran, & P. Shankar, (2022). “Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review”. Information Processing & Management, 59(2), 102888, 2022.

[16] S., Wolf, A. C. Burrows, M. Borowczak, M. Johnson, R. Cooley, & K. Mogenson, “Integrated outreach: Increasing engagement in computer science and cybersecurity”. Education sciences, vol.10 no. (12), pp.353. 2020.

[17] S. O. Oruma, & S. Petrovic, “Security threats to 5G networks for social robots in public spaces: a survey”. IEEE Access, 11, 63205-63237, 2023.

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

[19] M. Alowaidi, S. K. Sharma, A. AlEnizi, & S. Bhardwaj, “Integrating artificial intelligence in cyber security for cyber-physical systems”. Electronic Research Archive, 31(4), 2023.

[20] L. Monoscalco, R. Simeoni, G. Maccioni, & D. Giansanti, “Information security in medical robotics: a survey on the level of training, awareness and use of the physiotherapist”. In Healthcare (Vol. 10, No. 1, p. 159). MDPI, 2022, January.