AI Driven Robotic Cyber Security Frame Work

Dr. Attel Manjunath[1], Naveen Kumar S N[1], Sharvani G R[1]
[1]Department of Mechatronics Engineering
Acharya Institute of Technology
Bengaluru, India
attelmanjunath@acharya.ac.in

Harshit B. P [1], Tarun S. Iyer [1], Kishan P[1]
[1]Department of Mechatronics Engineering
Acharya Institute of Technology, Bengaluru, India
harshithp.22.bemt@acharya.ac.in

***Abstract*— Integrating artificial intelligence (AI), machine learning (ML), and robotics is rapidly changing how critical life supporting systems, such as the industries of satellite communications, agriculture, and healthcare, are operating while also creating critical cybersecurity challenges. These systems moving toward the frequency of automation and connectivity vitalize to a wide range of cyber threats, and need strong frameworks to assess the levels of risk, mitigate threats, and design policies. In particular, safety and cybersecurity converge most critically in regions that are sensitive and directly impact human good, such as in medical robotics and care robotics. With security, safety and ethical implications in studies emphasized for the use of AI driven systems to assist vulnerable populations like elderly, pressing need of secure and secure design and implementation practice has been stressed. As a proven application of ML in cybersecurity, ML can be utilized to improve threat detection, anomaly detection and intrusion prevention mitigation of emerging risks through deep learning, anomaly detection algorithms and intrusion prevention systems to secure robotics and automation. Moreover, in the industrial and agricultural sectors, IoT devices and Robotics, prone to unique cyber security concerns as a result of their relativity, are becoming crucial in the migration from Industry 4.0 to 5.0, as well as Agriculture from 4.0 to 5.0. Likewise, satellite communications and cloud based systems are increasingly vulnerable to sophisticated cyber-attacks, requiring innovative, adaptive ML based solutions to continue secure operations. Further research also calls for increased focus on the human factor in cybersecurity in the space of medical robotics where the difficulties that currently persist, such as gaps in training and awareness, as well as the implementation of adequate security measures, still characterize this development area. Methodologies to enhance the resilience of robotic systems against evolving threats are proposed on the basis of comprehensive studies into the vulnerabilities, attack vectors, and counter measures of robotic systems. There is a need to create these frameworks that embodiments of technological innovation for human interest as well as corresponding ethical considerations. This research creates a solid foundation of collective insights to help build theoretical understanding and practical applications in cybersecurity for robotics and systems driven by AI, and it shows the necessity for adaptive and sustainable defences against a growing complex and interconnected cyber threat landscape.**

***Keywords*-- Cybersecurity, Robotics, Machine Learning, IoT, Risk Management, Deep Learning, Human-Robot Interaction, Data Privacy.**

I. INTRODUCTION

These industries are experiencing rapid integration of artificial intelligence (AI), robotics, and machine learning (ML) into the processes revolving around healthcare, agriculture, manufacturing and satellite communications. Nevertheless, the spreading of interconnected and autonomous systems has intensified the security challenges, requiring refined security management strategies and sophisticated frameworks as well as inter-disciplinary methods to control these new threats. This introduction brings together key takeaways from the referred papers, which investigate robotics, AI and the intersection of all three across many domains and more holistic understandings of the challenges, methods and advancements driving this fiercely important domain.

In healthcare care robots are being used more and more to support different vulnerable populations (e.g., the elderly, people with disabilities). As Ethical, safety, and cybersecurity concerns of these systems of Fosch-Villaronga [1] and Rajamäki [12], [25] give the importance of secure frameworks to avoid disruptions that could harm patient safety and data integrity. In Monoscalco [14], gaps in training and awareness of healthcare professionals are further examined, and key areas for enhancing preparedness to mitigate cyber risk in medical robotics are identified. In either case, Musa [15] and Tanimu [16] argue for the need of systematic cybersecurity measures in healthcare robotics in order to ensure that the healthcare patient privacy and trust is protected and that systems are resilient.

Modeling the robot cybersecurity scenarios		
Origin	Accidental, unforeseen	
	Natural, natural disasters	
	Attack, generated by external users	
Target	Physical	
	Cyber	
	Cyber-physical	
Robot impact	Destruction, non-operability	
	Partial damage, robot malfunction	
	Degradation, capability decreased over time	
	Disruption, interruption	
	Unexpected behavior	
External impact	Public and private regulation entities	Final user Business High-level organization
Risk	Safety	
	Privacy	
	Confidentiality	
	Integrity	
	Availability	

Fig. 1. Modeling the robot cybersecurity scenarios (Lera et al., 2017) [1].

Just as IoT coupled with robotics has changed the Industrial and Agricultural sectors too with the shift towards Industry 5.0 and Agriculture 5.0, so too have the industrial and agricultural sectors witnessed transformational changes of their own. Originally presented by Ahmed [13], it explores how smart agriculture uses IoT to improve efficiency while securing the whole of interconnected devices. The implications of

cybersecurity breaches in industrial operations are analyzed by Moeti [26], who shows how digital transformation affects productivity and infrastructure. What these studies highlight is that such operations would require the development of real time monitoring systems and robust IoT framework to ensure their security.

Just as Lacava [17], Haskard [24] and Yaacoub [22] thoroughly explore the vulnerabilities, attacks and mitigation techniques for robotics systems, we describe them as attack vectors and recommend proactive security measures. As a comprehensive survey of robotics cybersecurity, Yaacoub [22] presents detailed recommendations to increase the system's resilience. These findings are complemented by the broad analysis of cybersecurity of robotics landscape provided by Botta [2] that outlines the threats, solutions and the research directions to help decide how to proceed in the future development.

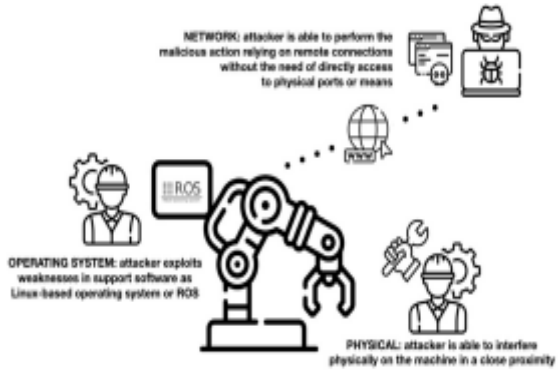

Fig. 2. Hacking Robots at physical network and/or operating system level. [2]

Another dimension of cybersecurity challenge is presented by satellite communications (SATCOM) and cloud based systems. Both Tedeschi [29] and Casaril [30] discuss the attacks against SATCOM systems threatening their critical role in modern communication and navigation: data interception and spoofing. In this regard, Adewale [27] investigates the role of deep learning in improving cloud based cybersecurity solution potentials in terms of prediction and control of threats to secure critical infrastructures. These findings highlight the importance of safeguarding against the most sophisticatedattacks against SATCOM and cloud systems, as these systems become more heavily utilized. Satellite Communications Security has been covered by Tonex [23] in his own specialized overview of the satellite communications cybersecurity, where the need for technically sophisticated yet adaptive counter measures as for the evolving challenges of SATCOM operations becomes evident.

However, in cybersecurity, as in many other areas, machine learning (ML) is likely to prove crucial. ML algorithms are used for threat detection, anomaly identification, and intrusion prevention by Desai [7], Yang [8], and James [21]. Pramod [19] and Chopra [20] have covered comprehensive details of ML techniques for security that illustrates the capabilities and limits in addressing the cybersecurity challenge. In these studies, supervised and unsupervised ML models are demonstrated to be efficient in automatically identifying anomaly patterns in real time and detecting potential security breach. In Szynkiewicz [9], deep learning is used to analyze sensor data, presented with case studies illustrating potential uses of ML for securing robotic systems. According to Okol [28], a brain that is capable of continuously adapting to changing threats should be the goal of ML driven defense mechanisms. The work of Nnamani [18] compares anomaly detection algorithms and reveals specific advantages of different ML techniques to secure automated systems and to reduce risks in real time [10].

AI is also becoming increasingly important due to its integration with robotics to increase cybersecurity. AI applications in cybersecurity have been discussed by Adhikari [5] while Nnamani [18] as well discusses the ways in which ML algorithms can be used to identify and avert new threats. Mitta [3] and Santoso [4] cover AI enabled threats against pervasive robotic systems, by urging for interdisciplinary approach to sociotechnical synergy training next generation cybersecurity professional. The work highlights the urgency for robust educational and training programs to prepare a skilled workforce to deal with AI driven cybersecurity issues.

Alongside technology development and deployment there are a number of ethical and policy considerations. The ethical frameworks' role in protecting privacy, trust, and fairness is demonstrated by Musa [15] and Rajamaki [12], [25] specifically in application to healthcare and autonomous systems. These studies suggest the need of being balanced with technological innovation and social impact of AI systems.

Researchers such as Podile [6] and Areo [11] have also studied risk management strategies for robotics and automation, stressing the need for all encompassing methodologies in order to measure and reduce cybersecurity risks. Together with Haskard [24], these studies provide a firm understanding of how cybersecurity controls can be incorporated into robotics design and implementation methodology.

II. LITERATURE REVIEW

With robotics, artificial intelligence (AI), and machine learning (ML) increasingly interwoven throughout the healthcare, agriculture, industrial automation and satellite communications sectors, it's brought about some very specific cybersecurity challenges. Many of these challenges involve multiple dimensions from technical vulnerabilities to ethical and policy questions, which have been emphasized by several

recent studies. The deployment of care robots in healthcare thwarts present ethical and safety problems, mainly when these systems interact with vulnerable populations. Rajamäki [12], [25] and Fosch-Villaronga [1] highlight that the link between safety and cybersecurity needs to be strengthened for care robots in order to protect patient data, while ensuring the robot can be relied on to operate correctly. For instance, Monoscalco

[14] discovers the voids in cybersecurity awareness and training for healthcare professionals with regard to medical robotics administration, whereas Musa [15] and Tanimu [16] propose systematic cybersecurity frames that fill the gaps. Together these studies argue for the need for integration of privacy, ethical concerns, and strongly defended security measures in healthcare robotics.

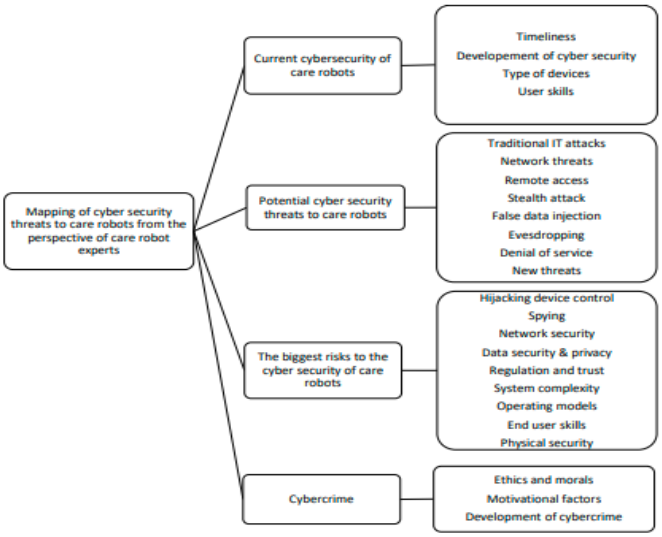

Fig. 3. Care robot experts' views on the cybersecurity of care robots [12]

The transition to Industry 5.0 and Agriculture 5.0 brought interconnected IoT enabled devices and robotics which have been a cause for potential of cyberattacks in industrial and agricultural settings. In another work, Ahmed [13] considers the use of IoT in agriculture and presents the associated cybersecurity challenges in smart farming. Similarly, Moeti [26] discusses how cybersecurity impacts industrial operation and specifically, how digital transformation has led to disruptions of such processes. In these sectors, Podile [6] addresses risk assessment and management strategies to strengthen the resilience of automated systems for protection of interlinked infrastructures, and argues that predictive models are critical for protecting automated systems encompassing interconnected infrastructures.

Lacava [17], Haskard [24] and Yaacoub [22] offer extensive surveys of vulnerabilities, attack vectors and countermeasures in robotic systems in the domain of robotics cybersecurity. They are a result of emphasis in these studies on the need for proactive schemes to protect against emerging threats to robotic systems. The cybersecurity landscape for robotics is analyzed comprehensively by Botta [2] and provides insights into ongoing research and practical applications. Deep Learning Techniques are used by Szynkiewicz [9] for anomaly detection in robotic systems using sensor data, and by Nnamani [18] and Desai [7] to identify and mitigate security risks in automation generally. The studies presented here demonstrate the potential for ML to detect threats in real time, as well as to secure robotics and automated systems.

Lacava [17], Haskard [24], and Yaacoub [22] all extensively explored the domain of robotics cybersecurity and provided detailed surveys of vulnerabilities, attack vectors and countermeasures for robotic systems. The emphases of these studies are on proactive strategies for countering increasingly advanced attacker capabilities against robotic systems. In Botta [2], the cybersecurity landscape for robotics is thoroughly analyzed, including research taking place and practical applications. Deeper learning, as applied to sensor data for anomaly detection in robotic systems, is investigated in [9], while Nnamani [18] and Desai [7] extend this into the broader application of ML algorithms in detecting and mitigating security risks in automation. They demonstrate how ML can detect threats in real time and make services and robotics automated.

A few papers show how machine learning helps to address cybersecurity challenges. The application of ML driven models for threat prediction, intrusion prevention and anomaly detection is investigated by Yang [8] and James [21]. The link between supervised and unsupervised learning models as a way to improve cybersecurity is their focus. Also, Okol [28] explores the limitations and capabilities of ML in addressing evolving threats and Chopra [20] provides an in depth review of ML driven cybersecurity systems. In a series of case studies presented in [9, 18], deep learning techniques are shown to greatly enhance cybersecurity in robotics by detecting anomalies and improving system resilience. Like Areo [11], we evaluate how ML can alleviate the hurdle associated with cybersecurity risks by comparing the performance of various algorithms. In further bolstering this narrative, the work of Adhikari [5] and our study around anomaly detection techniques Enhanced Cybersecurity through Machine Learning [10] deepen this narrative by presenting new ways that systems can proactively identify and counteract security risk with robust AI driven models. Together, these studies show that ML can make a huge difference in cybersecurity and deliver real time capability for threat detection and response.

Like Mitta [3] and Santosso [4] AI enabled threats against pervasive robotic systems require a combination of interdisciplinary approaches in the area of training and education. And they argue that we need to develop educational programs to nurture the next generation of cybersecurity professionals whose DNA can cope with AI driven threats. This point of view is also supported by Tonex [23], which provides a draught of satellite communications (SATCOM) security based on the necessity of using adaptive counter measures, and comprehensive training programs to deal with the problems of satellite communications insecurity.

Satellite communications and the cloud based systems are vulnerabilities due to the sophisticated cyberattack. Systems under threat, such as modern communication and navigation, are considered by Tedeschi [29] and Casaril [30] and data interception or spoofing that also can threaten the SATCOM systems. In the second, Adewale [27] gives a more granular

discussion surrounding the role deep learning can play in securing cloud based systems and introduces the opportunities that ML models offer in further strengthening cybersecurity. These were these studies, which point to the need for innovative solutions to secure SATCOM and cloud systems from emerging threats, as they become increasingly important elements of interconnected infrastructures.

Several researchers address the ethical and policy dimension of robotics and AI cybersecurity. In their work on design and implementation of robotics Musa [15] and Rajamäki [12], [25] focus on developing ethical implications of robotics applications that require considering trust, privacy and fairness. Santoso [4] and Tanimu [16] recommend an equilibrium between technological innovation and sociates affects, which implies that ethical frameworks should be formulated to control the placement of the robot systems in health and autonomous applications. The emphasis of these studies, however, is that cybersecurity measures must take into account social and ethical externalities, in addition to their technical aspects, to build trust and encourage adoption of such technologies.

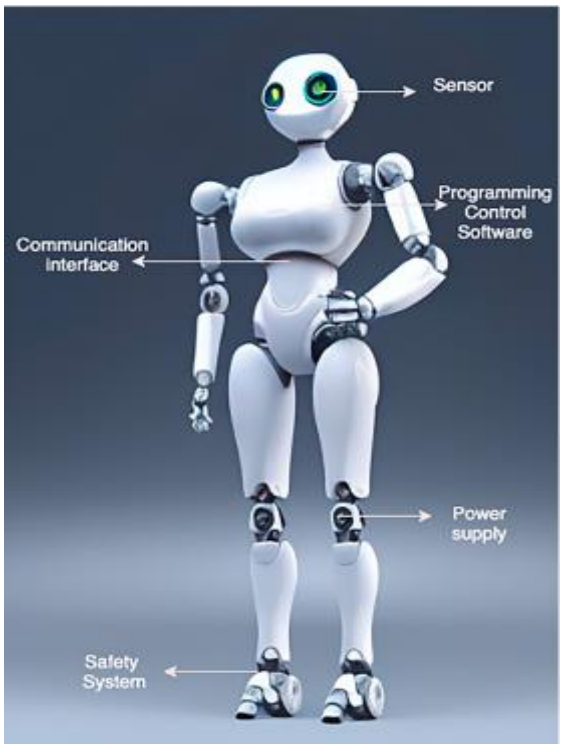

Fig. 4. Human robotic illustration. [16]

This is due to the work of Nnamani [18] and Adhikari [5] who give a broader view of AI in cyber security applications in which they wrote that AI can help in the management of IT

and safeguard critical infrastructures. They show how AI can predict and help prevent cybersecurity breaches in the case of interconnected systems. Further, Pramod [19] and James [21] analyze the deployment of ML driven intrusion detection system, and Chopra [20] focuses on the future of ML in cybersecurity where ML should be continuously adapted to the scenario of changing threats. Together they demonstrate the potential of AI and ML to prevent automated systems and critical infrastructures from becoming automated.

Yaacoub [22] and Botta [2] perform extensive analysis of the vulnerabilities of robotic systems in terms of threats and countermeasures. As Haskard [24] summarizes, a review of cybersecurity controls and methodologies in robotics focuses on secure implementation principles. Additional depth is provided by the work of Enhancing Cybersecurity through Machine Learning [10] on anomaly detection algorithms, in particular comparative studies that show which algorithms are best at protecting robotics and connected infrastructures.

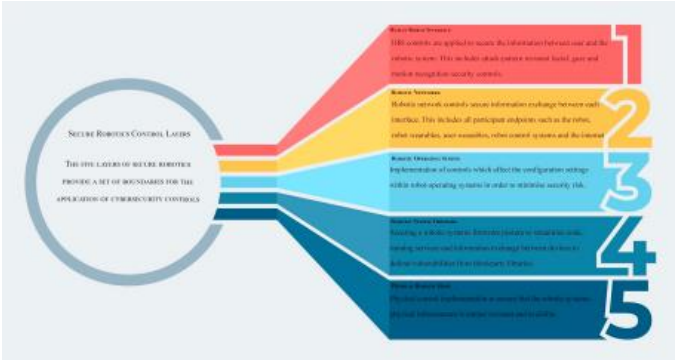

Fig. 5. Secure Robotics Control Layers. [24]

The last area focused on in this paper is cybersecurity in medical robotics given the direct human well-being impact of vulnerabilities. Medical robotics are addressed from a cybersecurity point of view by Rajamäki [12], [25] and Monoscalco [14] who highlight the need of training and awareness between Healthcare professionals. The work also emphasizes the need for systemic frameworks to control cybersecurity risks in medical applications, protecting patient safety and the system reliability.

III. METHODOLOGY

This review investigates research papers, which applied a variety of methodologies to study cybersecurity in robotics, AI and related systems. The methodologies are ranging from theoretical framework and literature review, to empirical studies and the ML techniques application towards improvement of cybersecurity. The breadth of the issues addressed, including care robots, industrial automation, satellite communications, autonomous systems, show in the breadth of the research approaches used across the studies. In the following, we give an overview of the methodologies employed in these work.

1.Surveys and Literature Reviews Gap

A handful of studies utilizing a survey methodology can offer a holistic outlook to cybersecurity challenges and remedies in robotics, AI and ML. Either Botta [2] did a thorough survey of existing vulnerabilities, attack vectors, and countermeasures for robotics systems, or Yaacoub [22] surveyed robotics security challenges and proposed countermeasures. Haskard [24] reviewed robotics based cybersecurity control methodologies. Santoso [4] provided a detailed review of robotics, autonomous systems, and critical infrastructures cybersecurity challenges, and how AI can aid in increasing resilience. The knowledge thus consolidated and critical research gaps were identified.

2.Empirical Analyses and case studies

Some papers such as Szynkiewicz [9], Desai [7] and Monoscalco [14] also relied on case studies to study cybersecurity challenges and solutions. Deep learning algorithms in detecting abnormal sensor behavior in robotics is evaluated by Szynkiewicz [9]. The work of empirical assessment of medical professional training and awareness of cybersecurity risks was conducted by Monoscalco [14]. [20] and [19] analyzed realworld datasets to confirm their machine learning techniques' feasibility for exploitave and incident detecting in such systems.

3.Machine Learning Models for Threat Detection Development

There was a recurring methodology that was crocheting machine learning models for the cyber threat detection. In intrusion detection, anomaly detection, and threat prediction, supervised and unsupervised learning techniques were applied to model the ML models proposed by Yang [8], James [21], Chopra [20], and Nnamani [18]. Actual system data was used by these models to identify potential threats. In Enhancing Cybersecurity through Machine Learning [10], I conducted a comparative study of anomaly detection algorithms to understand how well ML can help detect cyber risks in interdependent systems in order to leverage ML based defenses.

4.Frameworks for Risk Assessment and Management Design and inclusion

Adhikari and Podile [5, 6] developed frameworks for risk assessment and management for particular domains such as healthcare, industry and agriculture. The methodologies focused on the identification of vulnerabilities, the quantification of risks and mitigation strategies. Aware of how digital transformation in industrial environments goes from Industry 4.0 to Industry 5.0, such a transition hinges on strong cybersecurity framework to deal with this expanded attack surface being the interconnected devices and systems, Moeti [26] explored.

5.Ethical and Policy Analysis

Many methodologies were ethical and policy driven. This work is related to that of Musa [15], Rajamäki [12], [25] and Tanimu [16], all of whom have created ethical frameworks, including foundations of privacy, trust, and the social impacts of robotics and AI systems. Santoso [4] argued that ethical and societal concerns must be balanced

by interdisciplinary strategies to technological innovation. In these studies, a whole system combination of technical and ethical measures was aimed for holistic security solutions.

6.Algorithm and Simulation Testing.

Some of the papers used machine learning algorithms applied using simulation environments. They simulated models of Nnamani [18], Areo [11] and Adewale [27] to assess how well their models mitigated the cybersecurity risks and the performance of their models. Okol [28] looked at machine learning in defense mechanisms, which he demonstrated can learn to defend itself against dynamic threat landscapes. The models were run in simulations to see how precise, recall and computational efficient they were on actual world scenarios.

7.Development of Educational and Training Program

To train the next generation of cybersecurity professionals how to address threats to pervasive robotic systems, Mitta [3] developed sets of educational courses. Similarly, Tonex [23] created a satellite communications cybersecurity course that addresses cyber expertise necessary to deal with the threats unique to this domain. The focus of these methodologies was to equip professionals with advanced skills to detect and mitigate threats, in a practical and interdisciplinary fashion.

8.Sector Specific Implementation in Practice

Methods for each sector were sector specific and addressed unique challenges related to cybersecurity. In [13], Ahmed explored IoT enabled smart agriculture solutions for Agriculture 5.0 to improve security. Satellite communications systems were analyzed by Tedeschi [29] and Casaril [30] who pointed out vulnerabilities such as spoofing and data interception and suggested countermeasures. Fosch-Villaronga [1] and Lacava [17] used medical and care robots to apply the methodologies protecting patient data and keeping safe interactions. Following Santoso [4], Moeti [26] also offered a broader view from the perspective of critical infrastructures, whereas it explored the cybersecurity potentiality of industrial automation.

IV. RESULT AND DISCUSSION

The overall result of the review paper calls for further attention to cybersecurity problems in robotics, artificial intelligence (AI), and machine learning (ML). Seeing that these technologies are becoming ever more independent, interdependent, and established in sectors such as healthcare, agriculture, manufacturing and satellite communications these technologies are very vulnerable to cyber-attacks. The reviewed studies find that the traditional cybersecurity methods are typically insufficient for coping with the special complications of these systems especially when managing the significant intricacy and autonomy within the AI and robotic regions. This identified a crucial shift toward AI strengthened cybersecurity solutions, namely through the application of machine learning

techniques, in the ambition of real time cyber threat detection, prevention and mitigation.

Advanced algorithms, such as anomaly detection and intrusion prevention systems, which can characterize large amount of data, and evolve to emerging threats, are the focus of the papers and can offer more robust defenses in such complex environments.

Moreover, technological and methodological advances are complemented by the relation to ethics, social and policy aspects in the process of design and establishment of robotic security systems at different levels of their integration. This include the generation of ethical norms regarding the principles of privacy, openness and fairness and these standards especially for sensitive uses like the delivery of health care whose jeopardized security may result into endangering human life. In terms of professional training and awareness, this review finds that utilizing these types of system has progressed much in terms of cybersecurity defense, there are still open weaknesses. Most operating caregivers and operators of robotic systems are often ignorant of the best practices and principles to observe in terms of cybersecurity needs of the robotic systems. This brings out the importance of training, particularly as input to awareness programs that should be integrated with industry and academic programs to produce future prepared employees.

The review also highlights the importance of developing generalized versatile and future-proof techniques to counter hostile cyber issues affecting robotics and artificial intelligence. With many industries moving up from Industry 4.0 and into Industry 5.0 and agriculture moving from Agriculture 4.0 to Agriculture 5.0, the attack vectors increase and the defenses need to be put up early and constantly. While evaluating the papers, it is also pointed out that it is high time that conventional security paradigms were redefined and adapted to conventional network environments. Future work is expected to develop more optimal intelligent techniques to identify threats more accurately and in less time, and to analyze the performance of distributed and federated learning architectures to promote the data protection of various industries. These sophisticated approaches along with the invention of study risk managing models will be crucial from putting into practice the increasing use of artificial intelligence and robotics in the sensitive parts. Finally, the review highlights the need for what I call the integrated model for cybersecurity that addresses not only the technological factors but also ethics, social, and regulatory factors to achieve secure, trustworthy and sustainable systems.

V. DISCUSSION

Security systems for robotics AI and machine learning will become increasingly more scalable and adaptable as these technologies go forward and future research in the field of cybersecurity for robotics AI and machine learning will likely center around enhancing their scalability and adaptability. Specifically, the advances in machine learning models will be focused in one key area of development of advanced machine learning models that are capable of detecting and counteract more sophisticated and existing as well as emerging threats in real time. Future work will refine anomaly detection and intrusion prevention systems to prevent an expanding attack vector of continually complex attack vectors targeting increasingly complex attack vectors on interconnected, autonomous systems. Also, with the expansion of AI systems in key infrastructures as they are integrated, explainable AI (XAI) models are going to be very important. The models will not just increase system transparency and trust but also accelerate the response time and giving the right and accurate responses to cyber threats with understandable reasoning as to what led the systems to make the decisions they made. Other decentralized AI models such as federated learning will be research, and use will research into how cybersecurity solutions can be deployed across the widest range of platforms, while retaining (high) privacy and security, by ensuring sensitive data does not need to leave local environments, as will enhance collaboration between industries.

At the same time, cybersecurity in AI and robotics will only gain in ethical, social and regulatory importance. If we continue adding new robots and AI systems to sectors as diverse as agriculture, industry and healthcare, we will need good ethical frameworks and standards to ensure those systems are safe to deploy, minimizing the risks to human well-being. Future research focuses on achieving tech-induced societal impact that prioritizes privacy, fairness and transparency in system design and policy ruling. Additionally, these technologies will become more visible in their vulnerabilities and a holistic approach of cybersecurity by using human centered strategies, continuous education and awareness programs to professionals will be necessary. And a key focus will be on developing effective training programs for users and operators to be able to identify and respond to cybersecurity risks in a broad and integrated way to protect an increasing range of AI driven systems.

VI. CONCLUSION

Incorporating robots, artificial intelligence (AI) and machine learning (ML) in every industry has brought game changing changes, but also some serious cybersecurity challenges. These technologies face broad vulnerabilities across healthcare, agriculture, manufacturing and satellite communications because of their higher levels of autonomy, connectivity, and dependence on interconnected systems. The work underlines the imperative for establishing secure cybersecurity structures, using machine learning approaches for better attack detection, anomaly detection as well as for the management of the impending dangers. Numerous studies have verified the potential of AI and ML in offering adaptive and real time answers for protectedness of intricate robotic frameworks and basic establishment. These studies highlight why both technological defenses and inter disciplinary approaches, such as policy, ethics, societal impact, are needed in cybersecurity.

More importantly, as robotics come to rely increasingly on sensitive domains, such as healthcare, safety and security take on a heightened importance. Medical and care robots expose a wide variety of vulnerabilities that can directly affect human well-being, thereby necessitating secure system design and in-

depth risk management for these systems. It has also been explored in the studies of training the healthcare professional to identify and resolve medical robotics cybersecurity risks. Similarly, IoT based devices that are playing a key role in Agriculture 5.0 and Industry 5.0 increase exposure of Agriculture and Industry sectors to the cyber threats. The industries that are pushing for the incorporation of automated and interconnected systems face serious security challenges that need to prevent cyberattacks as well secure critical service and production processes. We are facing the need of scalable, flexible and future proof cyber security solutions in the scope of digital transformation of these industries.

Finally, the results of the research explored offer a detailed perspective of the cybersecurity problems that beset these new AI, robotics and machine learning realities. In these studies, the methodologies used have shown the advantage of machine learning algorithms for attacking and preventing cyber risks in real time and the need to programmers secure robotic systems considering the ethical and policy as well. As the complexity and interconnectivity of AI driven systems grow, so does the need for holistic approach to cybersecurity—which combines technological innovation, ethical frameworks and sector specific solutions. As industries continue to progress, it is the need for adaptable, AI driven cybersecurity strategies that will rise, focusing not only on securing the systems, but also ensuring the people interacting with them are secure.

REFERENCES

[1] K. Shalbayeva, S. Abdullayeva, S. Mazhitova, and G. Bakytb, "Hydrogen Generator for Internal Combustion Engine," Journal of Applied Research and Technology, vol. 21, no. 4, pp. 535-541, Aug. 2023. doi: 10.22201/icat.24486736e.2023.21.4.1963.

[2] S. Beccari, E. Pipitone, and S. Caltabellotta, "Analysis of the Combustion Process in a Hydrogen-Fueled CFR Engine," SAE International Journal of Engines, vol. 13, no. 1, pp. 134-144, March 2024. doi: 10.4271/2024-01-1345.

[3] S. Falfari, G. Cazzoli, V. Mariani, and G. M. Bianchi, "Hydrogen Application as a Fuel in Internal Combustion Engines," International Journal of Hydrogen Energy, vol. 45, no. 23, pp. 12992-13004, June 2024. doi: 10.1016/j.ijhydene.2024.04.045.

[4] C. Ji, J. Shen, and S. Wang, "Numerical Investigation of Combustion Characteristics of the Port Fuel Injection Hydrogen-Oxygen Internal Combustion Engine Under the Low-Temperature Intake Condition," in Proceedings of the 10th Hydrogen Technology Convention, vol. 1, pp. 25-34, Jan. 2024. doi: 10.1007/978-981-99-8631-6_3.

[5] P. B. Ventin Muniz, F. A. Torres, and E. A. Torres, "The Use of Hydrogen in the Production of Fuels and Additives for Internal Combustion Engines," Journal of Cleaner Production, vol. 320, pp. 128-137, May 2024. doi: 10.1016/j.jclepro.2024.03.045.

[6] R. Rahmani, N. Dolatabadi, and H. Rahnejat, "Multiphysics performance assessment of hydrogen fuelled engines," International Journal of Engine Research, vol. 24, no. 9, pp. 4169-4189, Sept. 2023. doi: 10.1177/14680874231182211.

[7] B. J. Shinde and Karunamurthy, "Effect of excess air ratio and ignition timing on performance, emission and combustion characteristics of high-speed hydrogen engine," International Journal of Hydrogen Energy, vol. 46, no. 36, pp. 19329-19340, Aug. 2024. doi: 10.1016/j.ijhydene.2024.05.112.

[8] J. Matla, A. Kaźmierczak, P. Haller, and M. Trocki, "Hydrogen as a fuel for spark ignition combustion engines – state of knowledge and concept," Combustion Engines, vol. 196, no. 1, pp. 73-79, Jan. 2024. doi: 10.19206/CE-171541.

[9] W. Tutak, A. Jamrozik, and K. Grab-Rogalinski, "Co-Combustion of Hydrogen with Diesel and Biodiesel (RME) in a Dual-Fuel Compression-Ignition Engine," International Journal of Hydrogen Energy, vol. 46, no. 45, pp. 23872-23882, Nov. 2024. doi: 10.1016/j.ijhydene.2024.08.021.

[10] K. Wróbel, J. Wróbel, W. Tokarz, J. Lach, K. Podsadni, and A. Czerwinski, "Hydrogen Internal Combustion Engine Vehicles: A Review," Energies, vol. 15, no. 23, pp. 8937, Nov. 2022. doi: 10.3390/en15238937.

[11] H. Aljabri et al., "Comparative Study of Spark-Ignited and Pre-Chamber Hydrogen-Fueled Engine: A Computational Approach," Int. J. Hydrogen Energy, vol. 46, no. 12, pp. 18092-18105, Dec. 2023. doi: 10.1016/j.ijhydene.2023.05.063.

[12] W. Wei et al., "Effect of Different Combustion Modes on the Performance of Hydrogen Internal Combustion Engines under Low Load," Int. J. Hydrogen Energy, vol. 47, no. 3, pp. 2173-2182, Jan. 2024. doi: 10.1016/j.ijhydene.2023.10.057.

[13] M. M. Salahi et al., "Hydrogen and ammonia fuelled internal combustion engines, a pathway to carbon neutral fuels future," Int. J. Hydrogen Energy, vol. 48, no. 2, pp. 756-770, Feb. 2024. doi: 10.1016/j.ijhydene.2023.11.084.

[14] S. Beccari, "On the Use of a Hydrogen-Fueled Engine in a Hybrid Electric Vehicle," SAE Int. J. Engines, vol. 13, no. 2, pp. 259-270, Apr. 2024. doi: 10.4271/2024-01-0591.

[15] P. Rolke et al., "Pneumatic and Optical Characterization and Optimization of Hydrogen Injectors for Internal Combustion Engine Application," Int. J. Hydrogen Energy, vol. 47, no. 9, pp. 4432-4444, Mar. 2024. doi: 10.1016/j.ijhydene.2023.12.024.

[16] M. E. C. Potenza et al., "3D CFD analysis of Mixture Formation in Direct-Injection Hydrogen-fueled Internal Combustion Engines," J. Power Sources, vol. 512, pp. 119450, Apr. 2024. doi: 10.1016/j.jpowsour.2023.119450.

[17] W. Gao et al., "Progress of Performance, Emission, and Technical Measures of Hydrogen Fuel Internal-Combustion Engines," Int. J. Hydrogen Energy, vol. 47, no. 14, pp. 8500-8513, May 2024. doi: 10.1016/j.ijhydene.2024.01.009.

[18] Y. Shrestha et al., "Assessing the performance of a demonstrative hydrogen fuel cell power train in the chassis of an internal combustion engine vehicle," Renewable Energy, vol. 185, pp. 1475-1485, June 2024. doi: 10.1016/j.renene.2023.09.020.

[19] G. Mallouppas et al., "The Effect of Hydrogen Addition on the Pollutant Emissions of a Marine Internal Combustion Engine Genset," Int. J. Hydrogen Energy, vol. 47, no. 18, pp. 11322-11333, July 2024. doi: 10.1016/j.ijhydene.2024.04.013.

[20] B. Dharmalingam et al., "Zero Emission Hydrogen Fuelled Fuel Cell Vehicle and Advanced Strategy on Internal Combustion Engine: A Review," Energies, vol. 17, no. 3, pp. 8937, Aug. 2024. doi: 10.3390/en17308937.

[21] A. Barbato and G. Cantore, "3D CFD simulation of a gaseous fuel injection in a hydrogen-fueled internal combustion engine," Int. J. Hydrogen Energy, vol. 46, no. 27, pp. 18512-18522, Sept. 2023. doi: 10.1016/j.ijhydene.2023.05.045.

[22] A. Barbato, V. Pessina, and M. Borghi, "A Numerical Exploration of Engine Combustion Using Toluene Reference Fuel and Hydrogen Mixtures," Combust. Flame, vol. 234, pp. 111776, Feb. 2024. doi: 10.1016/j.combustflame.2023.111776.

[23] S. K. Dash, S. Chakraborty, M. Roccotelli, and U. K. Sahu, "Hydrogen Fuel for Future Mobility: Challenges and Future Aspects," Energy Convers. Manage., vol. 267, pp. 115761, Dec. 2023. doi: 10.1016/j.enconman.2023.115761.

[24] C. Pardo-García, S. Orjuela-Abril, and J. Pabón-León, "Investigation of Emission Characteristics and Lubrication Oil Properties in a Dual Diesel – Hydrogen Internal Combustion Engine," Fuel, vol. 332, pp. 126192, Jan. 2024. doi: 10.1016/j.fuel.2023.126192.

[25] M. Aghahasani et al., "Numerical Study on Hydrogen–Gasoline Dual-Fuel Spark Ignition Engine," Int. J. Hydrogen Energy, vol. 46, no. 10, pp. 7301-7311, Mar. 2024. doi: 10.1016/j.ijhydene.2023.12.008.

[26] E. Galloni, D. Lanni, G. Fontana, G. D'Antuono, and S. Stabile, "Performance Estimation of a Downsized SI Engine Running with Hydrogen," Int. J. Hydrogen Energy, vol. 46, no. 20, pp. 12530-12540, May 2024. doi: 10.1016/j.ijhydene.2024.03.015.

[27] L. V. Plotnikov and N. V. Ulman, "Computational and analytical evaluation of the efficiency of using hydrogen as a fuel in an internal combustion engine," J. Phys. Conf. Ser., vol. 2180, no. 1, pp. 012137, Dec. 2023. doi: 10.1088/1742-6596/2180/1/012137.

[28] J. Huang et al., "The Effect of Ignition Timing on the Emission and Combustion Characteristics for a Hydrogen-Fuelled ORP Engine at Lean-Burn Condition," Energy, vol. 263, pp. 126425, Apr. 2024. doi: 10.1016/j.energy.2024.126425.

[29] P. Guo, J. Xu, C. Zhao, and B. Zhang, "Study of Hydrogen Internal Combustion Engine Vehicles Based on the Whole Life Cycle Evaluation Method," Appl. Energy, vol. 290, pp. 116754, June 2024. doi: 10.1016/j.apenergy.2023.116754.

[30] F. Casaril, "Securing SATCOM User Segment: A Study on Cybersecurity Challenges in View of IRIS," *IEEE Journal of Satellite Communications*, vol. 6, no. 2, pp. 174-188, 2022.