VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 3, July-Septemeber 2024 *pp:01-10*

Machine Learning Techniques for Cyber Security in Internet of Robotic Things

Asad Raza [1]*, **Shahzad Memon** [2], **Muhammad Ali Nizamani** [3], **Lachman Dhomeja** [1], **Nisar Memon** [5], **Khalid Charan** [1]

[1]A H S Bukhari Postgraduate Centre of ICT Faculty of Engineering and Technology University of Sindh, Jamshoro, Pakistan; [2]Department of Electronics Engineering, Faculty of Engineering and Technology, University of Sindh, Jamshoro, Pakistan.; [3]Department of Information Technology, Faculty of Engineering and Technology, University of Sindh, Jamshoror, Pakistan; [5]Department of Telecommunication Engineering, Faculty of Engineering and Technology, University of Sindh, Jamshoro, Pakistan.

Keywords: *Internet of Robotics Things, Cybersecurity, Autonomous control, Operations safety, Machine Learning.*

Journal Info:
Submitted:
July 20, 2024
Accepted:
August 14, 2024
Published:
August 15, 2024

Abstract

Robots are becoming common in domestic, medical, industrial, entertainment, and educational routine activities. The use of robots automates the work processes thus minimizes human labor. The Robots perform complex and repetitive tasks with efficiency and agility, therefore, the conventional industrial manufacturing process are being replaced by smart manufacturing. Robotics encompasses the design and development of robot-based automated systems. It integrates various emerging technologies i.e. operational technology (OT), cloud computing, and artificial intelligence (AI). The Internet of Robotic Things (IoRT) seamlessly combines robots and Internet of Things (IoT) devices, enabling connectivity through the Internet. IoRT enables simple robots to coordinate with each other to achieve well-defined goals by creating a multi-robot system. Cyber security is an inherent challenge for IoRTs because of the interconnected infrastructure and reliance on critical industrial operations on the internet. Any cyber-attack can affect the ongoing operations and compromise the safety of robots. The growing interest among governments, researchers, and industries in robotics and automation demands a dependable cyber-security solution. This paper explores machine learning (ML) based cyber security solutions to mitigate cyber vulnerabilities and threats to IoRT and its dependent systems.

***Correspondence author email address:** asadraza825@gmail.com
DOI: 10.21015/vtse.v12i3.1870

1 Introduction

Automation in manufacturing, military, entertainment, health, logistics and agriculture by the help of robots is common nowadays. Industry 5.0 is focused on AI and smart manufacturing. Smart manufacturing depends on AI, robotic things, IoT and automation systems. A

robot is a combination of cyber and physical objects and termed as cyber physical systems. IoRT provides interconnectivity platform, which connects robotics with IoT and enables robots, various other devices and application to communicate with each other via the intranet or the internet. For example, the smart agricultural robotic system that consists of sensors, agro-robots, autonomous vehicles such as drones and driverless machinery to carry various agriculture tasks to reduce farmers' costs and improve efficiency and production. Systems of robotic thing can achieve enhanced efficiency and adaptability across multiple application through combination of divers sensor arrays and robotic agents using IoRT by boosting its functionality and versatility [1]. Exposure of such smart systems to cyber space is prone to be victim of various cyber security threats and vulnerabilities. Multi robotic systems (MRS) a collection of varying sizes, shapes, and capabilities [2], heterogeneity and interoperability further broaden the surface of cyber-attacks against IoRT.

Robots primarily consist of software and hardware components. Software components include operating systems i.e., Linux, robotic operating system (ROS), and hardware i.e., sensors, IoT devices. Robotic things interact with the physical world using various sensors and IoT devices and interact in cyberspace with other robots using various software applications and communication networks [3].

Robot-based automated manufacturing systems may go under various cyber-attacks that halt production processes and may result in industrial financial loss. Use of robots in military and other national security platforms [4], and cloud and file server via robotic wireless communication are some other important areas where lack of secure networking, authentication, authorization, and advanced IDS are security challenges. Therefore, the cyber security solutions are essential to mitigate cyber security threats and vulnerabilities, and secure robotic-based automated systems from cyber-attacks.

The literature reports various cyber-attacks such as denial of service (DoS), distributed denial of service (DDoS), Man in the middle (MiTM), ransomware, wireless jamming, information disclosure and espionage. Moreover, malware, a malicious software that infiltrates devices and networks through vulnerabilities; social engineering, individuals into compromising security; advanced persistent threat (APT), sophisticated cyberattacks targeting long-term data theft or operational disruption; and intrusion, an unauthorized access attempts or malicious behavior [5], are among the list of cyber security threats. Like other cyber systems, IoRT is also exposed to these challenges as major security threat [6]. Furthermore, some other emerging attacks which may not be detectable in a traditional intrusion detection system (IDS) for various industries relying on the IoRT based operations, and the advancement in technology enables industry to develop new complex and critical robotic systems also broaden the threat vectors.

Significant advancements in ML boost its applications in various domains, such as cybersecurity for mitigation of vulnerabilities and threats of cyber-attacks to the cyber systems. Various ML based security systems have been developed with high accuracy to detect cyber-attacks in robotic-based systems. Supervised, semi-supervised, unsupervised, and reinforcement learning techniques are common in ML. The supervised learning requires labeled data and unsupervised learning works on unlabeled data while semi-supervised algorithms can learn from labeled and unlabeled data. Reinforcement learning has the potential to mitigate threats to IoRT systems, particularly in human-robot collaboration systems [7]. Since IoRT can be connected to long-term care or the cloud through the internet, insecure communication between users and robots could lead to cyber-attacks [8].Various ML Algorithms such as support vector machine (SVM), logistic regression, Decision Tree (DT), Random Forest classifier (RFC), Naïve bayes, K-Nearest Neighbors (KNN), artificial neural network (ANN), Convolutional neural networks (CNN), and recurrent neural networks (RNN) have been successfully applied to address a range of security challenges in IoRT environments. The algorithms boast unique strengths and adoptable to specific challenges, and offer promising solutions for building robust cybersecurity systems

for the IoRT.

This paper provides a comprehensive survey of ML based techniques utilized to mitigate the vulnerabilities and threats to the IoRT. The paper first presents the classification of robots, followed by the three-layered architecture of IoRT, and then various ML-based security solutions proposed by cybersecurity researchers for safeguarding emerging robotic technology

2 Methodology

We grouped the robotic-based systems into to industrial robots, field robots, service robots the classifications. The classes are further divided in sub categories according to the available literature. Literature suggests various IoRT architectures consisting different count of layers as shown in Table I. We choose the most common three layered architecture for its Cyber security challenges and their available solutions.

We searched ML based methods used for IoRT security as mentioned in Table III. The methods are summarized for each layer of the three layered architecture, accordingly.

2.1 Robotic based Systems

Robotics-based systems utilize robots to reduce workload, increase work efficiency and boost production. These systems also assist humans in various tasks [15]. They are particularly valuable for performing complex tasks that are repetitive, difficult and time consuming for humans. Fig 1 illustrates some existing robotics-based systems and is discussed in subsequent section.

2.2 Industrial Robots

Industrial robots are a prime example of robots used extensively in the manufacturing, electronics, and automotive industries. In fact, they are the most widely employed robots in manufacturing and production settings [16]. These versatile machines excel in automating complex and repetitive tasks across various industries, including automotive, electronics, pharmaceuticals, packaging, and quality inspection. Additionally, industrial robots play a crucial role in enhancing efficiency and safety in the workplace. The assembly line in the automotive industry is a prominent example of how industrial robots can achieve superior efficiency and consistency compared to human workers.

Table 1. LAYERED ARCHITECTURES IN LITERATURE

Reference	Layers
[9]	1. Hardware Layer (“Robotic Things” layer) 2. Network Connectivity 3. Internet Connectivity / IoT protocols 4. Robotic Platform Support 5. M2M2A Cloud Platform Support 6. Big Data Services 7. IoT Business Cloud Services 8. IoT Cloud Robotics Infrastructure 9. Application Layer
[10]	1. Physical 2. Network and Control 3. Service and Applications
[11]	1. Physical 2. Network and Control 3. Service and Applications
[12]	yyyy
[13]	1. Hardware layer 2. Support layer 3. Network layer 4. Application layer
[14]	1. Hardware/robotic things layer 2. Network layer 3. Internet layer 4. Infrastructure layer 5. Application layer

2.3 Healthcare Robots

Healthcare robots are specifically designed to assist our healthcare professionals and patients. They are used for fully automated or assisted healthcare tasks, including diagnosis, laboratory, patients real time monitoring, nursing assistant and surgery [17]. Some prominent examples of healthcare robots include surgical robots, laboratory robots, and patient monitoring robots. Laboratory robots automate laboratory tests, sample handling and analysis, significantly improving efficiency and accuracy in healthcare things.

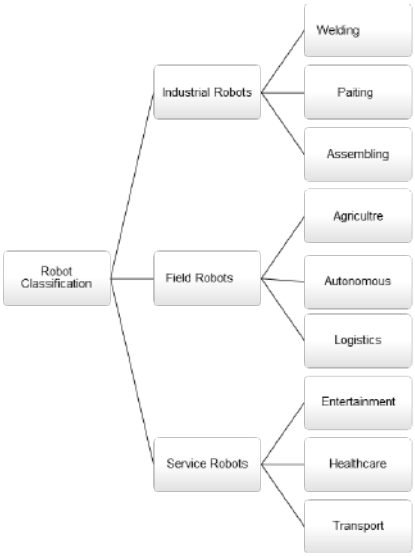

Figure 1. Classification of Robots

2.4 Autonomous Robots

Autonomous robots are primarily utilized for military and surveillance purposes with unnamed aerial vehicles (UAVs) or drones being prominent examples. However, their applications extend far beyond military and defense sectors, demonstrating their effectiveness in diverse fields such as transportation, environmental conservation, communication, agriculture, and disaster management [18].

2.5 Agricultural Robots

Agricultural robots, also known as Agro robots, are valuable tools used in various tasks such as planting, monitoring, and harvesting of crops [19]. These autonomous robots can perform a wide range of tasks from autonomously harvesting crops to assisting farmers with other essential duties. In addition, agriculture robots can be remotely controlled, allowing farmers to monitor crops from any location, regardless of their physical presence in the fields.

2.6 Entertainment Robots

Entertainment robots play a diverse role in engaging and entertaining people [20]. They can be utilized to create immersive experiences including virtual and augmented reality environments. Examples of entertainment robots include robot toys, robotic dogs, gaming robots and humanoid robots.

2.7 Internet of Robotic Things (IoRT) Architecture

IoRT has many applications, such as robotic arms in smart manufacturing, robots in e-commerce, agricultural robots in precision agriculture, military robots in military conflicts, military surveillance. IoRT mainly consists of three-layer architecture [21] shown in figure 2 and discussed in the following section of the paper.

2.8 Physical Layer

Physical layer lowest layer and is mostly used for data acquisition. It mostly interacts with the physical world. The sensors, GPS, RFID and IoT devices embedded with robotic things used to interact and collect data from the real world. Control and navigation systems are very dependable on the physical layer. Physical damage, device modification and hardware Trojan are some threats to the physical layer. Cloud computing can be used due to limitation of physical layer such as heterogeneity, interoperability, and limited storage capability. The Physical layer mostly is under threat due to physical attacks such as physical damage, node tampering and hardware Trojan.

2.9 Network and Control Layer

Data transmission and control operations are mostly done at the network layer. This layer consists of network operation which is mostly concerned with data communication and networking of robotic things and IIoT devices, robots, sensors are integrated with each other through this layer, while control is concerned with control and navigation of robotic things. This layer consists of controllers, routers, storage devices, cloud servers and communication protocols.Network operations may include the local network, the internet, Radio Frequency Identification (RFID), WiFi, Bluetooth and Near Field Communication (NFC). Robots communicate with others to create multi-robot systems using network layer. This layer increases the attack surface due to its connectivity with internet and networking via various network protocols so security at network and control layer is important risk and threat mitigation. Most dangerous attacks at this layer are ransomware, data leakage, Man in the middle (MiTM)

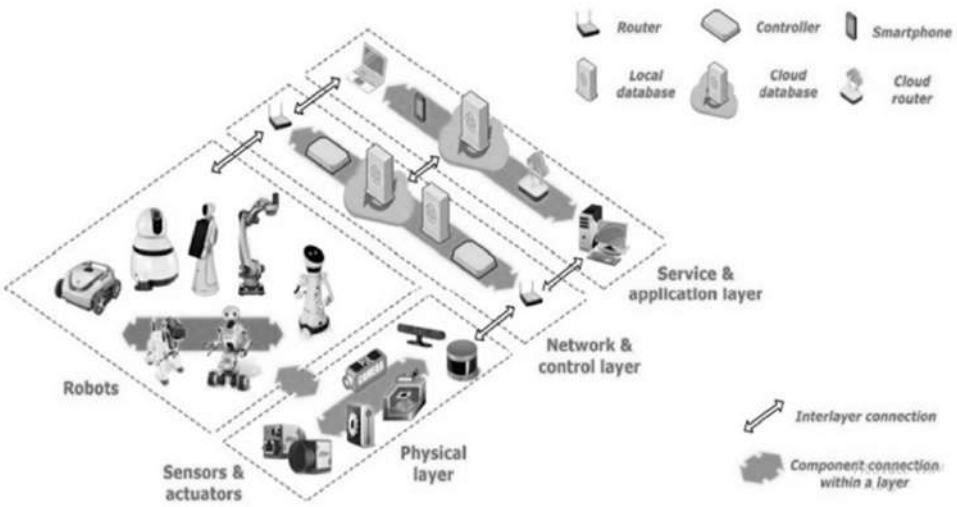

Figure 2. Three Layer Architecture of IoRT [22]

and DDoS. Cybersecurity systems such as firewall, intrusion detection and prevention systems and security information and event management (SIEM) can be used for layer security. The network and control layer mostly is under threat due to cyber-attacks such as IP spoofing, MiTM and backdoor. This layer needs secure network communication between robotic-to-robotic things or robots to IoT devices or vice versa.

2.10 Service and Application Layer

This layer is used to run services and applications for operations, monitoring and controlling robots, sensors and IIoT devise. This application is used to send requests to perform robotic tasks. Interactive applications and visualization services may be available in his layer to which used for real time data analytics, monitoring and controlling of robots. AI can be used at this layer to automate robotic based systems different processes. Cyber-attacks which may disturb service and application layer are DDoS, SQL Injection, data leakage, XSS, spyware and ransomware.

The protocols and components associated with IoRT three layers architecture are shown in Table I.

2.11 ML based Security of IoRT

IoRT integrated with IoT/IIoT devices, robotic things and computers. These devices use various applications and protocols and OS. So, there are lot security risks, threats and vulnerability exist which need to be mitigated for security of IoRT to reduce attack surface. Robotic based systems implementation in the industrial environment is complex, and its integration with IoT devices needs network security for secure communication and collaboration. Robotic things are under various threats and attack surfaces, it can be vulnerable from the network or OS. Robotic things can be attacked with DoS attack to sabotage running operations of IoRT environment. This attack can damage industrial operations for a while which may result in not providing services to users. IoRT with DoS attack is illustrated in figure 3.

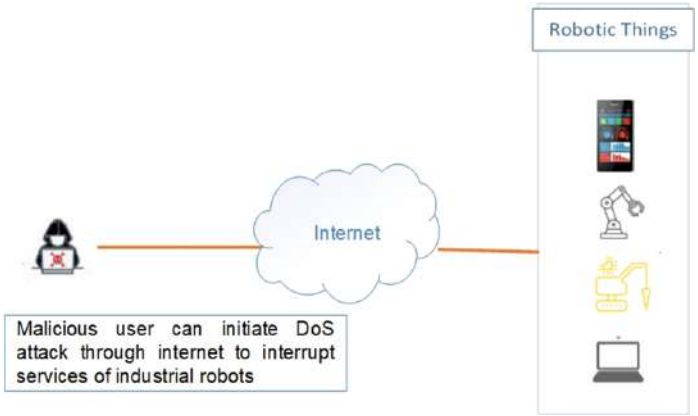

Figure 3. DoS attack scenario on IoRT

Threat actors can also initiate DDoS attack using compromised computers or botnet users, which is

Layer	Components/Protocols
Physical layer	Robots, sensors, actuators, IoT devices
Network and control layer	Routers, controllers, Bluetooth, WiFi, TCP, UDP, IP, NFC, RFID, Zigbee
Service and application layer	Applications, cloud services, Smart Phones, Tablets, REST API

Table 2. Layered Architecture Components/Protocols

more dangerous than DoS attack because it sends huge traffic due to which services become overwhelmed and use all their resources due to malicious requests. DDoS attack on IoRT environment is shown in figure 4.

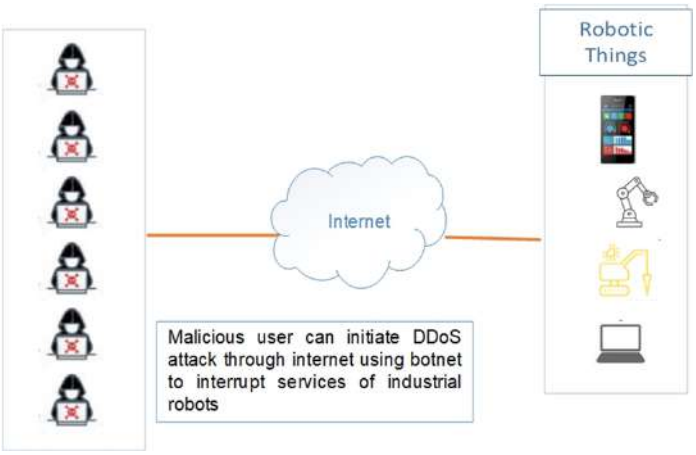

Figure 4. DDoS attack scenario on IoRT

Robotic things in IoRT environment can be physically damaged by threat actors and they can be remotely damaged due to vulnerability in robotic operating system or application used by robotic things. This attack scenario is illustrated in figure 5.

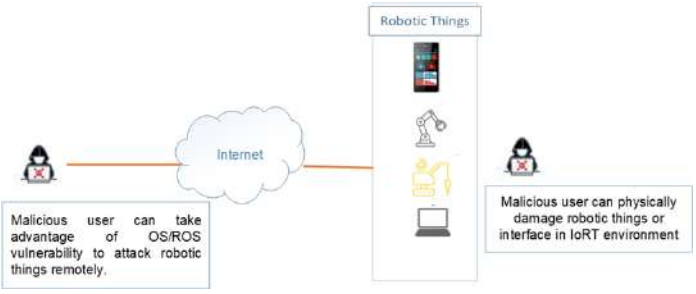

Figure 5. Physical and remote access attack scenario on IoRT

The physical attacks on robots such as physical damage can be mitigated with physical controls such as security gates, CCTV cameras, identify cards, behavior analysis, tracking and biometrics [23] however, due to advancement in technology, cyber-attack detection is difficult for new, complex systems and networks, so robotic based smart systems and environments need proactive threat detection systems with ML techniques. We have discussed attack detection from existing work which has been done by researchers.

AI is an essential component to develop more intelligent robots. However, ML and deep learning (DL) methods are also used for robot security of. Various research has been done in IoT and cyber physical systems security. We have discussed existing robotics security work for IoT security with ML and DL. Some of the major attacks on robotic systems are worms, ransomware, Trojans, and random access trojan (RAT), rootkit, botnet, spyware, and passwords, DoS and DDoS.

A random forest classifier (RFC) was proposed for detection of hardware trojan. RFC was evaluated with 36 hardware trojan features and efficiency detected Trojans in circuits [24]. Graph neural networks (GNN) were proposed to detect hardware trojan and was evaluated with the custom dataset. The experimental results showed that the proposed method achieved 97% recall and 84% precision [25]. The Deep convolutional neural network (DCNN) was proposed to detect hardware trojans in IC design and was trained with IC images. DCNN was trained and evaluated with two datasets synthetic ISCAS and Trust-Hub and experimental results showed that the proposed DNN achieved 97.4% and 99% accuracy [26].Decision tree-based IDS was proposed for detection of denial of service and command injection attacks on mobile robotic vehicles. The proposed model was trained with cyber input and physical features. Cyber features

contain network traffic and disk data while physical features include power consumption capacity, mobile robotic vehicles speed and robot jittering [27]. Power fingerprint-based IDS was proposed for replay attack detection in industrial robots. Three robot models were used for evaluation of proposed IDS and experimental results showed that it achieved 99.9% detection rate [28].

The malicious PDF detection method was proposed with the DL model. Robots can share or receive malicious PDF from humans, which can be a threat to robot security. The proposed DL model evaluation explored that the proposed method achieved a 99.48% F1-score with low resource consumption and performance of the mobile robots [29]. The authors proposed CNN and SVM for global positioning system (GPS) spoofing attack detection in autonomous vehicles. The proposed method was evaluated with CALRA simulator and experimental results showed that CNN and SVM achieved 99%, 99% accuracy as best while 82%,96 as worst case [30]. Botnet attack detection system was proposed with CNN and LSTM for industrial internet of things. The IIoT devices are integrated with industrial robots, so securing IIoT devices is also crucial for robot security. The authors used various DL models i.e. ANN, gated recurrent unit (GRU) and long short-term memory (LSTM). The authors evaluated the proposed DL models with IIoT botnet dataset, and that dataset has class imbalance problem which was tackled with resampling techniques. The experimental results showed that all models achieved promising accuracy score of more than 98% [31]. The network IDS was proposed with multilayer perceptron neural network for GPS spoofing attack detection in Unmanned aerial vehicles (UAV) networks. The proposed IDS was evaluated with TEXBAT and MAVLINK datasets and experimental study showed that the proposed IDS on TEXBAT achieved 83.23% accuracy and 99.93% accuracy on MAVLINK dataset [32].

Various robot systems for industrial automation have been developed with robotic operating systems (ROS). ROS utilization for robotic applications may also increase cyber threats due to risks and vulnerabilities associated with the OS. The authors proposed integrating ROS-based application with Message Queuing Telemetry Transport (MQTT) for secure communication between IoRT. The proposed safe communication approach with authentication and encryption controls have secured the robotic applications from various cyber-attacks such as MiTM and hijacking attacks [33].

ML based methods used for IoRT security are summarized in Table II.

3 Conclusions

Robots are becoming common in daily life. IoRT is an emerging research area, which connects robots and IoT. This paper introduces IoRT and its applications in various areas. The classification of robots is described in detail, and the paper presents three-layer architecture of IoRT and the scenarios in which IoRT environment is exposed to cyber attacks. The IoRT applications are applied in many systems including complex industrial smart manufacturing systems and critical smart power grid. Cybersecurity challenges rise due to this increasing complexity. We have discussed various challenges posed to IoRT like cyber and physical attacks and ML based security solutions for mitigation of such attacks on IoRT. Furthermore, this paper explores the potential of AI-based methods, various frameworks and models for securing IoRT and its integrated IoT devices.

Author Contributions

Asad Raza: Conceptualisation, data collection, supervision,methodology **Shahzad Memon**: Data collection, experimental work and writing the original draft. **Muhammad Ali Nizamani**: Data labelling, proofreading. **Lachhman Dhomeja**: Algorithm testing, review original draft.: **Nisar Memon**: Data collection, validation, editing **Khalid Charan**: experiments and Writing the original draft.

Compliance with Ethical Standards

The authors declare no conflict of interest. This research required human participation for online signature data collection. However, informed consent was obtained from all individual participants included in the study.

ML Techniques Proposed	Limitations of Proposed Techniques
RFC [18]	The proposed RFC true positive rate score can be improved with other ML techniques such as CNN.
GNN [19]	The proposed model achieved better recall and precision scores which can be further improved.
DCNN [20]	The proposed CNN accuracy on synthetic ISCAS data can be further improved.
DT [21]	The proposed DT model achieved 93.81% accuracy, which needs further improvement.
Power Fingerprinting [22]	The proposed technique can be combined with ML techniques to develop a more effective IDS.
SVM, DT, K-Nearest Neighbors (KNN), Deep Neural Network (DNN) [23]	The proposed model achieved 98.9% recall, which can be improved with CNN and an ensemble of DL models.
CNN, SVM [24]	The proposed method was evaluated with small datasets; however, evaluation with large datasets is needed.
ANN, Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) [25]	ANN achieved 99% accuracy, while LSTM and GRU achieved 98%; however, the architecture and hyperparameter optimization of the DL models were not discussed.

Table 3. ML techniques proposed for the security of IoRT

Funding Information

This research has not received funds from any institution.

References

[1] A. López, D. Jaramillo, P. Salgado, J. Montes, and P. Rueda, "Architectures and methodologies of internet of robotic things systems: A systematic review," *Nanotechnology Perceptions*, pp. 262–272, 2024.

[2] K. Homayun, M. Tham, and Y. C. Chang, "Internet of robotic things for mobile robots: concepts, technologies, challenges, applications, and future directions," *Digital Communications and Networks*, vol. 9, no. 6, 2023.

[3] H. Khujamatov, E. Reypnazarov, D. Khasanov, and N. Akhmedov, "Iot, iiot, and cyber-physical systems integration," in *Advances in Science, Technology and Innovation*, 2021.

[4] M. Bistron and Z. Piotrowski, "Artificial intelligence applications in military systems and their influence on sense of security of citizens," *Electronics (Switzerland)*, vol. 10, no. 7, 2021.

[5] Z. Guan, L. Bian, T. Shang, and J. Liu, "When machine learning meets security issues: A survey," in *2018 International Conference on Intelligence and Safety for Robotics, ISR 2018*, 2018.

[6] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security (Int J Inf Secur)*, vol. 21, no. 1, 2022.

[7] H. Terra, K. Riaz, K. Raizer, A. Hata, and R. Inam, "Safety vs. efficiency: Ai-based risk mitigation in collaborative robotics," in *2020 6th International Conference on Control, Automation and Robotics, ICCAR 2020*, 2020.

[8] S. H. Chang, C. H. Hsia, and W. Z. Hong, "A secured internet of robotic things (iort) for long-term care services in a smart building," *The Journal of Supercomputing*, vol. 79, no. 5, 2023.

[9] S. J. DeCanio, "Robots and humans – complements or substitutes?," *Journal of Macroeconomics (J Macroecon)*, vol. 49, 2016.

[10] J. Arents and M. Greitans, "Smart industrial robot control trends, challenges and opportunities within manufacturing," 2022.

[11] M. Kyrarini *et al.*, "A survey of robots in healthcare," 2021.

[12] D. Floreano and R. J. Wood, "Science, technology and the future of small autonomous drones," 2015.

[13] H. Durmus, E. O. Gunes, M. Kirci, and B. B. Ustundag, "The design of general purpose autonomous agricultural mobile-robot: 'agrobot'," in *2015 4th International Conference on Agro-Geoinformatics, Agro-Geoinformatics 2015*, 2015.

[14] R. Bogue, "The role of robots in entertainment," *Industrial Robot*, vol. 49, no. 4, 2022.

[15] L. Romeo, A. Petitti, R. Marani, and A. Milella, "Internet of robotic things in smart domains: Applications and challenges," 2020.

[16] I. Afanasyev *et al.*, "Towards the internet of robotic things: Analysis, architecture, components and challenges," in *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, 2019.

[17] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of iot equipment: A survey of recent advances and opportunities," *IEEE Transactions on Industrial Informatics (IEEE Trans Industr Inform)*, vol. 18, no. 7, 2022.

[18] T. Kurihara and N. Togawa, "Hardware-trojan detection based on the structural features of trojan circuits using random forests," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E105A, no. 7, 2022.

[19] R. Yasaei, L. Chen, S.-Y. Yu, and M. A. A. Faruque, "Hardware trojan detection using graph neural networks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2022.

[20] R. Sharma, V. S. Rathor, G. K. Sharma, and M. Pattanaik, "A new hardware trojan detection technique using deep convolutional neural network," *Integration*, vol. 79, 2021.

[21] T. P. Vuong, G. Loukas, D. Gan, and A. Bezemskij, "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles," in *2015 IEEE International Workshop on Information Forensics and Security, WIFS 2015 - Proceedings*, 2015.

[22] H. Pu, L. He, C. Zhao, D. K. Y. Yau, P. Cheng, and J. Chen, "Fingerprinting movements of industrial robots for replay attack detection," *IEEE Transactions on Mobile Computing (IEEE Trans Mob Comput)*, 2021.

[23] Y. Cui, Y. Sun, J. Luo, Y. Huang, Y. Zhou, and X. Li, "Mmpd: A novel malicious pdf file detector for mobile robots," *IEEE Sensors Journal (IEEE Sens J)*, vol. 22, no. 18, 2022.

[24] M. Shabbir, M. Kamal, Z. Ullah, and M. M. Khan, "Securing autonomous vehicles against gps spoofing attacks: A deep learning approach," *IEEE Access*, vol. 11, 2023.

[25] M. Mudassir, D. Unal, M. Hammoudeh, and F. Azzedin, "Detection of botnet attacks against industrial iot systems by multilayer deep learning approaches," *Wireless Communications and Mobile Computing (Wirel Commun Mob Comput)*, 2022.

[26] O. Jullian, B. Otero, M. Stojilović, J. J. Costa, J. Verdú, and M. A. Pajuelo, "Deep learning detection of gps spoofing," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2022.

[27] M. Mukhandi, D. Portugal, S. Pereira, and M. S. Couceiro, "A novel solution for securing robot communications based on the mqtt protocol and ros," in *Proceedings of the 2019 IEEE/SICE International Symposium on System Integration, SII 2019*, 2019.

[28] H. Pu, L. He, C. Zhao, D. K. Y. Yau, P. Cheng, and J. Chen, "Fingerprinting movements of industrial robots for replay attack detection," *IEEE Transactions on Mobile Computing*, 2021.

[29] Y. Cui, Y. Sun, J. Luo, Y. Huang, Y. Zhou, and X. Li, "Mmpd: A novel malicious pdf file detector for mobile robots," *IEEE Sensors Journal*, vol. 22, no. 18, 2022.

[30] M. Shabbir, M. Kamal, Z. Ullah, and M. M. Khan, "Securing autonomous vehicles against gps spoofing attacks: A deep learning approach," *IEEE Access*, vol. 11, 2023.

[31] M. Mudassir, D. Unal, M. Hammoudeh, and F. Azzedin, "Detection of botnet attacks against industrial iot systems by multilayer deep learning approaches," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[32] O. Jullian, B. Otero, M. Stojilović, J. J. Costa, J. Verdú, and M. A. Pajuelo, "Deep learning detection of gps spoofing," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2022.

[33] M. Mukhandi, D. Portugal, S. Pereira, and M. S. Couceiro, "A novel solution for securing robot communications based on the mqtt protocol and ros," in *Proceedings of the 2019 IEEE/SICE International Symposium on System Integration (SII 2019)*, 2019.