Cyber Security and Applications 3 (2025) 100074

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Addressing cybersecurity challenges in robotics: A comprehensive overview

Jibrilla Abubakar Tanimu [a,*], Wafia Abada [b]

[a] School of Computing, University of Portsmouth, Portsmouth PO12UP, United Kingdom
[b] University of Abdelhamid Mehri Constantine 2, Constantine 25000, Algeria

ARTICLE INFO

Keywords:
Robotics
Encryption
Vulnerabilities
Threat detection
Unauthorized access
Cybersecurity

ABSTRACT

As robotics technology becomes increasingly integrated into various sectors, ensuring the cybersecurity of robotic systems is paramount. This article provides an in-depth exploration of the cybersecurity challenges confronting robotics and offers strategies to address these concerns. With the growing connectivity and networking capabilities of robots, vulnerabilities such as unauthorized access, data breaches, and network attacks are significant threats [1]. Protecting sensitive data collected and processed by robots is crucial to preserving privacy and trust. Remote access features, while enhancing operational flexibility, also pose security risks if not adequately secured. Weak authentication mechanisms and insecure interfaces could allow malicious actors to compromise robot functionality. Furthermore, robots are susceptible to malware and cyber-attacks, including viruses, worms, and ransomware. To mitigate these risks, a comprehensive approach is necessary, incorporating secure design principles, robust authentication mechanisms, encryption techniques, and cybersecurity training. Collaboration among industry stakeholders, researchers, policymakers, and cybersecurity experts is essential to develop resilient robotic systems capable of withstanding evolving cyber threats. This article underscores the importance of addressing cybersecurity challenges in robotics to ensure the safety and security of robotic deployments across diverse domains. As robotics technology evolves and becomes integral across various sectors, prioritizing cybersecurity [2] is crucial to protect these systems from unauthorized access, data breaches, and network attacks. The interconnected nature and remote access features of robots pose significant vulnerabilities. Comprehensive measures, including secure design, encryption, and cybersecurity training, are essential. Collaboration among industry stakeholders, researchers, policymakers, and cybersecurity experts is vital for developing resilient robotic systems. This article highlights the urgent need to address cybersecurity challenges to ensure the safety and integrity of robotic deployments.

1. Introduction

In recent years, the integration of robotics into various domains such as manufacturing, healthcare, transportation, and defense has significantly revolutionized industry practices and societal operations [3]. These advancements, highlighted in Table 1, have brought about tremendous benefits, improving efficiency, precision, and capabilities in numerous fields. However, these technological strides have concurrently led to an increase in cybersecurity concerns surrounding robotic systems. As robots become more interconnected and autonomous, they are exposed to a wide range of cyber threats, posing substantial risks to their functionality, safety, and integrity.

Cybersecurity challenges in robotics are multifaceted, encompassing vulnerabilities in hardware and software components, communication protocols, data privacy issues, and the potential for malicious manipulation of robotic behaviors. Robots play crucial roles in industrial automation, medical procedures, unmanned vehicles, and household assistance, making the ramifications of cyberattacks on these systems far-reaching and severe [4–6]. For instance, a compromised medical robot could lead to disastrous outcomes in surgical procedures, while a hijacked industrial robot could disrupt manufacturing processes or cause physical harm.

A notable example illustrating the severity of cyber threats targeting robotic systems is the Stuxnet worm. Discovered in 2010, this sophisticated malware specifically targeted industrial control systems, including programmable logic controllers (PLCs) used in nuclear facilities [7–10]. The Stuxnet incident underscored the potential for cyberattacks to inflict physical damage by manipulating the behavior of interconnected robotic components, highlighting the dire need for robust cybersecurity measures.

Moreover, the proliferation of Internet of Things (IoT) [11] devices and the adoption of cloud computing in robotics have introduced new

Peer review under responsibility of KeAi Communications Co., Ltd.
* Corresponding author.
E-mail addresses: jibrilla.tanimu@port.ac.uk (J.A. Tanimu), wafia.abada@univ-constantine2.dz (W. Abada).

https://doi.org/10.1016/j.csa.2024.100074
Received 28 April 2024; Received in revised form 5 July 2024; Accepted 3 October 2024
Available online 3 October 2024

Table 1
Systems components and their use in robots.

System	Uses
Sensors	-Perception: detecting distance, proximity, temperature, light intensity, and sound -Health Monitoring: detecting anomalies, malfunctions, or signs of wear and tear -Environmental Monitoring: such as temperature, humidity, air quality, and radiation levels.
Actuators	-Stability and Balance: play a crucial role in maintaining the stability and balance of robots, especially those with dynamic or humanoid designs, by adjusting their center of mass, posture -Manipulation: provide robots with the ability to manipulate objects using grippers, arms -Energy Conversion: convert electrical, pneumatic, hydraulic, or other forms of energy into mechanical motion, powering various robotic functions and systems.
Controller	- Overseeing and coordinating various functions. -Controllers manage locomotion, ensuring precise movement and navigation. - Implementing algorithms for tasks like object detection, path planning, and obstacle avoidance. - Regulate power distribution, optimizing energy usage and battery life.
Manipulators and End Effectors	-Manipulators are robotic arms designed to manipulate objects in various environments. -Allowing for flexibility and dexterity in movement -Tailored to specific tasks, such as gripping, cutting, welding, or painting. -Equipped with end effectors, specialized tools or attachments, to interact with objects.
Power Supply	-Provide the energy necessary to operate various components and systems. - Advances in battery technology, including lithium-ion and solid-state batteries, continue to improve the performance and efficiency of robotic power supplies. -Some robots utilize energy-efficient designs and power management techniques to extend battery life and optimize energy consumption.
Communication Interface	-Facilitate data exchange and control between different components and external devices. -Controllers, and other robots within a network. - Communication interfaces include Ethernet, Wi-Fi, Bluetooth, and serial ports (e.g., RS-232, RS-485).
Safety Systems	- Prevent accidents and protect human operators and bystanders. - Safety-rated sensors, such as laser scanners, ultrasonic sensors, and vision systems, monitor the robot's surroundings for obstacles or obstructions. - Programmable safety logic to ensure that robots operate within predefined safety parameters.
Programming and Control Software	-Enable the creation, execution, and management of robot tasks and behaviors. -Execution of programmed tasks, coordinating movements of robot joints, actuators, and end effectors.

attack surfaces and vectors for cyber intrusions. Adversaries can exploit vulnerabilities in sensor networks, actuators, and control algorithms to gain unauthorized access, disrupt operations, or exfiltrate sensitive data. As the reliance on robotic systems continues to grow, addressing these cybersecurity challenges becomes imperative to ensure the secure and reliable operation of these advanced technologies.

Addressing cybersecurity challenges in robotics requires a multidisciplinary approach, involving expertise in robotics engineering, cybersecurity, data privacy, risk management, and policy development. By understanding the evolving threat landscape and implementing robust security measures, stakeholders can mitigate the risks posed by cyber threats and ensure the continued advancement and adoption of robotic technologies in a secure manner. This research article aims to delineate the security challenges inherent in robotics and propose mitigation strategies to address these threats. The remainder of this article is organized as follows: Section 2 provides a background on attacks targeting robotic systems. Section 3 details the primary cybersecurity vulnerabilities identified in robotics. Section 4 explores recent real-world cyber incidents involving robotics, offering illustrative scenarios. Section 5 discusses security countermeasures and potential mitigation strategies. Section 6 focuses on security measures specific to robotic systems. Section 7 presents a discussion of the research findings. Section 8 concludes by summarizing the key findings and implications of the study. Finally, Section 9 outlines future directions for enhancing the work.

2. Background on robotics

As robotics technology continues to evolve and permeate various sectors, including manufacturing, healthcare, transportation, and agriculture, the integration of cyber-physical systems has become increasingly prevalent. However, along with the transformative benefits of robotics, there are significant cybersecurity challenges that must be addressed to ensure the safety, integrity, and reliability of robotic systems [12]. This article provides a comprehensive overview of the cybersecurity challenges facing robotics and explores potential solutions to mitigate these risks.

One of the primary cybersecurity challenges in robotics is the proliferation of connectivity and networking capabilities. Modern robots are often equipped with internet connectivity, wireless communication protocols, and network interfaces to facilitate remote monitoring, control, and data exchange. While these features enhance functionality and enable real-time collaboration, they also introduce vulnerabilities that could be exploited by malicious actors. Unauthorized access, data breaches, and network attacks are among the risks associated with interconnected robotic systems as shown in Table 2.

Robots collect and process vast amounts of sensitive data, ranging from proprietary algorithms and operational metrics to personal information and medical records. Protecting this data from unauthorized access, tampering, or theft is paramount to safeguarding privacy and maintaining trust. Data security vulnerabilities in robotic systems could lead to intellectual property theft, financial loss, regulatory non-compliance, and reputational damage for organizations [13].

Remote access capabilities allow users to control and monitor robots from anywhere via the internet. While remote access facilitates operational flexibility and efficiency, it also introduces cybersecurity risks. Weak authentication mechanisms, unencrypted communication channels, and insecure remote-control interfaces could enable malicious actors to gain unauthorized access to robotic systems, manipulate their behavior, or disrupt operations.

Robots are susceptible to various forms of malware, including viruses, worms, ransomware, and remote access trojans [13,14]. Malicious software could exploit vulnerabilities in robot operating systems as shown in Fig. 1, software libraries, communication protocols, or sen-

Table 2
Vulnerabilities in robot system.

System	Vulnerability	Consequences
Programming Control Software	-Lack of security update -Spoofing -Insufficient access control -Software vulnerability -Lack of secure coding practice -Insecure communication protocol	- Theft of valuable data - Data destruction -Unauthorized access -Regulatory compliance operations -System instability -Malicious code execution
Communication interface	-Jamming attack -Lack of firewalls -Lack of training -Poor management -Hardware failure -Insecure protocol -Lack of integrity checks -Vulnerability firmware	-Loss of communication -Getting access to confidential information -Reputational damage -Data interception -Tampering -Denial of service (DoS) -Network infiltration
Sensors	-Data manipulation -Spoofing -Sensor jamming -Sensor data leakage -Physical tempering	-Safety hazards -Data manipulation -Operational disruption -System malfunction -Misinformation
Actuators	-Unauthorized access -Manipulation of control signal -Firmware vulnerabilities -Physical tempering -Denial of service	-Financial implication -Loss of control -Malicious action -safety risk -Operational disruption
Controller	-Weak authentication -lack of encryption -Firmware vulnerabilities -Remote code execution -Denial of service	-System disruption -Safety risk -Financial loss -Data manipulation -Unauthorized access

sor interfaces to compromise system integrity, steal sensitive data, or disrupt critical functions. Cyber-attacks targeting robotic systems could have far-reaching consequences, including production downtime, financial losses, safety hazards, and damage to brand reputation.

3. Cyber security in robotics

3.1. Network system

The Network system components such as communication interfaces, sensors, actuators, and control systems, are vulnerable to various cyber-attacks, including unauthorized access, data tampering, and denial-of-service attacks. To mitigate these risks, robust cybersecurity measures are required.

One key aspect of securing the network systems is implementing secure communication protocols. Secure communication protocols ensure that data transmitted between network components is encrypted and authenticated, preventing unauthorized access or interception by malicious actors [15]. Additionally, access control mechanisms play a crucial role in restricting access to critical network components, ensuring that only authorized users or devices can interact with them. Regular security audits and vulnerability assessments are also essential for identifying and addressing potential security vulnerabilities in network system components, thereby enhancing the overall cybersecurity posture of robotics systems. By prioritizing cybersecurity measures, organizations can safeguard network system components in robotics against cyber threats and ensure the integrity and reliability of robotic operations.

3.2. Remote access control

Remote access control, is critical for ensuring the integrity and security of robotic systems. Remote access control mechanisms enable operators or administrators to access and manage robotic systems from remote locations, posing potential security risks if not properly secured.

To mitigate these risks, robust authentication and authorization mechanisms should be implemented to verify the identity of remote users and restrict their access based on predefined privileges. Secure communication channels, such as virtual private networks (VPNs) or encrypted protocols, should be employed to protect data transmitted between the remote operator and the robotic system from interception or tampering by unauthorized parties.

Regular monitoring and logging of remote access activities are also essential for detecting and responding to suspicious or unauthorized access attempts promptly [16]. By implementing stringent remote access control measures, organizations can minimize the risk of unauthorized access and ensure the secure operation of robotic systems in various applications, ranging from industrial automation to healthcare and beyond.

3.4. Data security and privacy

Ensuring robust data security and privacy measures in robotics is crucial to safeguard sensitive information and protect against potential threats. One key aspect is implementing encryption protocols to secure data transmission between robotic systems and external networks, ensuring that data remains confidential and protected from interception or tampering [17].

Moreover, access controls play a vital role in restricting unauthorized access to sensitive data within robotic systems. By employing authentication mechanisms and role-based access control [18] (RBAC) policies, organizations can enforce strict access privileges, ensuring that only authorized personnel can interact with sensitive data.

Additionally, organizations should prioritize data anonymization and pseudonymization techniques to anonymize personally identifiable information (PII) and mitigate privacy risks. By obscuring sensitive data elements, organizations can prevent the identification of individuals and minimize the potential impact of data breaches or unauthorized disclosures.

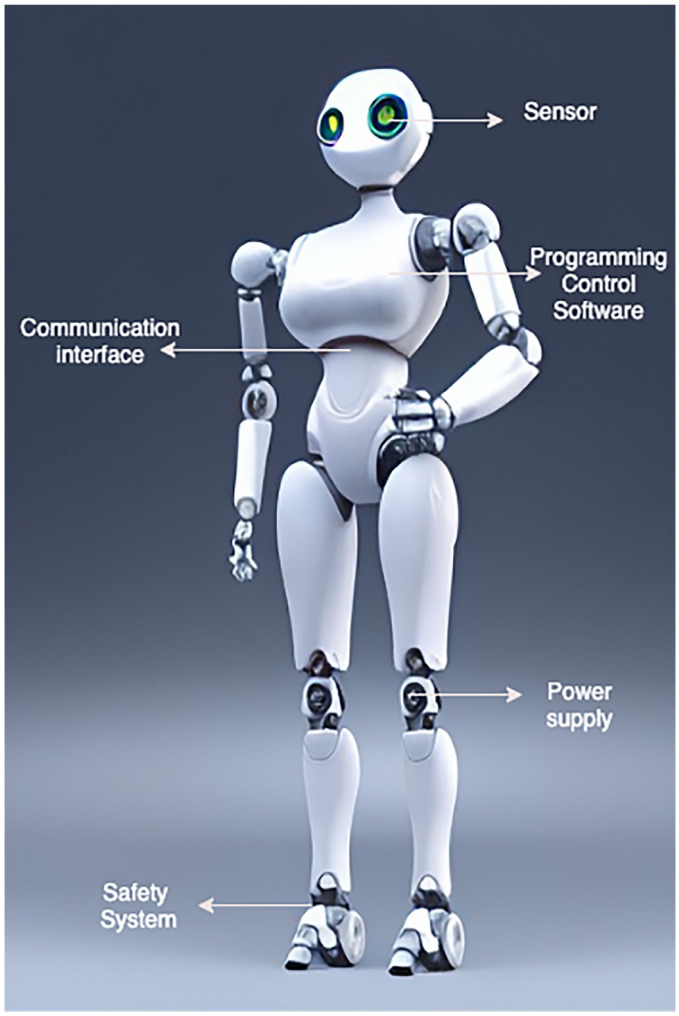

Fig. 1. Human robotic illustration.

A comprehensive approach to data security and privacy in robotics involves the implementation of encryption, access controls, and anonymization techniques to safeguard sensitive data and uphold privacy standards in robotic operations.

3.5. Sensor

Security in robotics, particularly concerning sensors, is paramount to prevent potential vulnerabilities and ensure the integrity of data collected by these devices as illustrated in Table 2. One crucial aspect is implementing authentication mechanisms to verify the identity of sensors and ensure that data is sourced from trusted sources. By employing cryptographic protocols [19], such as digital signatures, organizations can authenticate sensor data and verify its integrity, protecting against data tampering or spoofing.

Furthermore, organizations should implement secure communication channels between sensors and control systems to prevent eavesdropping or interception of sensitive data. By encrypting data transmissions and using secure communication protocols, such as Transport Layer Security (TLS), organizations can safeguard sensor data during transmission and mitigate the risk of unauthorized access.

Additionally, organizations should regularly monitor sensor networks for anomalies or suspicious activities, enabling timely detection and response to potential security incidents. By implementing intrusion detection systems and anomaly detection algorithms, organizations can proactively identify and mitigate security threats, ensuring the reliability and security of sensor data in robotics applications.

3.6. Industrial control system

Security in robotics, particularly concerning industrial control systems (ICS), is critical for maintaining the safety and integrity of industrial operations. One key consideration is ensuring the confidentiality, integrity, and availability of data and control commands within the ICS environment [8]. By implementing access controls and encryption mechanisms, organizations can protect sensitive data and prevent unauthorized access or manipulation of control systems.

Furthermore, organizations should regularly update and patch industrial control systems to address known vulnerabilities and mitigate the risk of exploitation by malicious actors. Additionally, organizations can segment ICS networks to limit the impact of security incidents and prevent lateral movement by attackers within the network.

Moreover, organizations should conduct regular security assessments and penetration testing of industrial control systems to identify and address potential security weaknesses. By proactively assessing and improving the security posture of ICS environments, organizations can enhance resilience against cyber threats and ensure the safety and reliability of industrial operations.

4. Cyberattacks on robot

Cyberattacks on robot systems represent a significant threat to their functionality, safety, and the broader ecosystem they operate. While there have been relatively few documented instances of cyberattacks directly targeting robots, the potential consequences underscore the importance of safeguarding these systems against malicious intrusions, some of these incidents are shown in Table 3.

One notable example occurred in 2017 when researchers from IO Active uncovered vulnerabilities in the SoftBank Robotics NAO and Pepper robots. These vulnerabilities could potentially allow hackers to access the robots remotely, manipulate their movements, and even capture audio and video data without authorization. This revelation raised concerns about the security of robots deployed in various settings, including homes, businesses, and healthcare facilities [20].

Table 3
Recent incidents in robots.

Year	Incident	Consequences
2023 [29]	The robotic arm mistook a man for a box of vegetables, seizing him and forcefully pushing his body against a conveyor belt.	Resulting to death.
2021 [30]	During a malfunction at Tesla's Giga Texas factory near Austin, a robot viciously attacked a Tesla engineer, resulting in a brutal and bloody altercation.	Resulting to injuries.
1979 [31]	First time an industrial robot kill human	Resulting to death.

Similarly, in a study conducted by cybersecurity researchers at the University of Washington, they demonstrated how they could remotely hijack a telepresence robot used for remote communication in healthcare settings. By exploiting security flaws in the robot's software, the researchers were able to gain control of its movements and camera, potentially compromising patient privacy and safety [21].

These examples highlight the diverse range of cyber threats facing robot systems, from unauthorized access and control to data exfiltration and privacy breaches. As robots become increasingly interconnected and autonomous, the potential attack surface expands, making them vulnerable to a variety of cyber threats.

To mitigate these risks, researchers and industry practitioners are actively developing cybersecurity solutions tailored to the unique characteristics of robot systems. This includes implementing secure communication protocols, access control mechanisms, and intrusion detection systems[11], [22]. Additionally, ongoing efforts to enhance the security-by-design principles in robot development and promote cybersecurity awareness among stakeholders are crucial in safeguarding against future cyberattacks on robot systems.

Stuxnet Worm Targeting Industrial Robots:

The Stuxnet worm, discovered in 2010, targeted industrial control systems, including programmable logic controllers (PLCs) used in supervisory control and data acquisition (SCADA) systems. Stuxnet specifically aimed at disrupting uranium enrichment facilities in Iran, reportedly causing significant damage to centrifuges by altering their rotational speeds. While not directly targeting robots, the Stuxnet incident highlights the potential for cyberattacks to manipulate critical infrastructure, including robotic systems.

Hospital Robot Vulnerabilities Exploited for Ransomware Attacks:

In a hypothetical scenario presented by cybersecurity researchers, vulnerabilities in hospital robots, such as surgical or delivery robots, are exploited by ransomware attackers [23]. By gaining unauthorized access to these robots, attackers could disrupt medical procedures, compromise patient safety, or demand ransom payments to restore control. This highlights the potential consequences of cyberattacks on robots deployed in critical healthcare settings.

Drone Hijacking for Espionage Purposes:

While not traditional robots, unmanned aerial vehicles (UAVs) or drones are increasingly used for surveillance, reconnaissance, and other tasks [24,25]. In a simulated experiment, researchers demonstrated the ability to hijack commercial drones by exploiting vulnerabilities in their communication protocols. By gaining control of these drones, attackers could conduct espionage activities, gather sensitive information, or even launch physical attacks. This underscores the importance of securing the communication channels and control systems of robotic devices, including drones.

These examples illustrate the diverse range of cyber threats facing robot systems and the potential impact on various sectors, including industry, healthcare, and national security.

5. Cryptographic solution and protocols for robotics systems

Cryptographic solutions and protocols play a vital role in ensuring the security of robots in various cyber-physical systems. One common cryptographic solution used for securing robot communications is encryption. Encryption involves encoding data in such a way that only authorized parties can access it, thereby preventing unauthorized access or tampering. By encrypting data exchanged between robots and other devices or systems, cryptographic protocols ensure that sensitive information remains confidential and secure from potential adversaries.

Another cryptographic solution employed in robot security is digital signatures. Digital signatures provide a means of verifying the authenticity and integrity of data transmitted between robots and external entities. By digitally signing messages or commands sent by robots, cryptographic protocols enable recipients to verify that the information originated from a trusted source and has not been altered in transit. This helps mitigate the risk of data tampering or manipulation, ensuring the reliability and trustworthiness of robot communications in cyber-physical environments.

Moreover, cryptographic protocols such as secure key exchange mechanisms are crucial for establishing secure communication channels between robots and remote servers or control systems [26]. Secure key exchange protocols enable robots to securely negotiate and establish cryptographic keys for encrypting and decrypting data transmissions. By ensuring the confidentiality and integrity of cryptographic keys during the exchange process, these protocols prevent unauthorized parties from intercepting or tampering with communication sessions. Cryptographic solutions and protocols play a crucial role in safeguarding robots against cybersecurity threats and ensuring the integrity, confidentiality, and authenticity of data exchanged in cyber-physical systems [27].

6. Security and countermeasure

This section is dedicated to assessing the vulnerabilities inherent in robotic systems and proposing effective strategies to mitigate potential cyber threats as shown in Table 4. This section plays a critical role in ensuring the integrity, confidentiality, and availability of robot operations, particularly in environments where security breaches could lead to serious consequences.

1. Vulnerability Assessment:

This entails identifying and analyzing potential weaknesses within robotic systems, including vulnerabilities in software, hardware components, communication protocols, and human-machine interfaces. Through comprehensive vulnerability assessments, we can gain insights into the specific areas of vulnerability within the robot's architecture.

2. Threat Analysis:

Involves conducting a thorough analysis of potential threats that could exploit identified vulnerabilities. These threats may include malware attacks, unauthorized access attempts, data breaches, manipulation of sensor data, or denial-of-service attacks. By understanding the nature of these threats, we can develop targeted countermeasures to mitigate their impact.

3. Risk Evaluation:

Assessing the potential risks associated with identified vulnerabilities is essential for prioritizing security efforts. We evaluate the likelihood and potential impact of security breaches on robot operations, safety, data integrity, and user privacy. This risk assessment helps allocate resources effectively to address the most critical security concerns.

4. Countermeasures:

Proposing effective countermeasures is a key aspect of the security and countermeasures section. These countermeasures may include implementing encryption techniques, access control mechanisms, authentication protocols, intrusion detection systems, secure coding practices, and regular software updates. Additionally, we may explore advanced security solutions such as anomaly detection algorithms and behaviour-based monitoring systems.

5. Incident Response:

Developing robust incident response protocols is crucial for promptly detecting, analyzing, and containing security incidents. We outline procedures for responding to security breaches, including incident detection, notification, containment, eradication, and recovery. Establishing clear incident response processes helps minimize the impact of security breaches and ensures rapid recovery of affected systems.

6. Compliance and Standards:

Table 4
Possible mitigation.

System	Mitigation
Human Factor	-Proper training and awareness programs -Enforcing strict access control policies to limit user privileges. -Deploy monitoring system to track user behavior and detect anomalous activities. -Implement multifactor authentication mechanisms to enhance the security of user account -Conduct regular security audits and assessment to identify vulnerabilities in human-robot. -Ensure that communication channel between human and robot are encrypted and secure to protect sensitive data.
Remote Access Control	-Implementing strong authentication -Utilizing Virtual private networks (VPN) to established secured connections. -Regular security update with the latest security patches to address known vulnerabilities and protect against threats. -Strong encryption protocol to protect data confidentiality. -Monitor longing by implementing mechanisms to track remote access control.
Network Connectivity	-Using secure implementation protocol such as transport layer security (TLS) or secure shell (SSH) to encrypt data transmission. -Implement network monitoring tools to continuously monitor the network traffic and detect an unusual activity. -Conducting regular security auditing and assessment of network security infrastructure. -Segmenting the network in to separate network zones for robot systems -Deploy an intrusion detection prevention system (IDPS) to monitor network traffic.
Power System control	-Implement redundant power supplies and backup power source to ensure continuous operation of the robot system. -Implement power management features and algorithms to optimized power consumption. -Ensure compliance with relevant safety standard. -Install surge protection devices and voltage regulators to protect robot system from voltage spikes. -Regular maintenance and inspection of power distribution cables.
Communication Interface	-Implementing encryption protocols such as SSL/TLS to secure data transmission over communication interfaces. -Implementing access control policies and mechanisms to restrict access to communication interface based on user's roles. -Installing firewalls and network filtering devices to filter incoming and outgoing traffic. -Use strong authentication mechanisms such as passwords, digital certificates to verify the identity of communication endpoint and prevent an authorized access. -Deploy intrusion detection and prevent system (IDS/IPS) to monitor network traffic.
Controls	-Use secure communication protocol (SSH, HTPPS) for transmitting control commands between human and robot controls. -Regular audit and monitoring of control systems to detect vulnerabilities, misconfigurations or unauthorized changes. -Implement role-based access control (RBAC) to assign specific permissions and privileges to different users based on their roles. -Employ encryption techniques to secure control signals and commands transmitted over command between human operation and robots.

Compliance with cybersecurity standards and regulations is essential for ensuring the effectiveness of security measures. We address compliance requirements relevant to robotic systems and adhere to industry best practices to mitigate risks effectively. This includes compliance with standards such as ISO/IEC 27,001, NIST Cybersecurity Framework, and GDPR (General Data Protection Regulation).

7. Discussion

The integration of robotics into various sectors, from manufacturing to healthcare, necessitates a robust cybersecurity framework to protect these systems from an array of cyber threats. The article has highlighted the multifaceted nature of cybersecurity challenges in robotics, emphasizing the critical need for comprehensive and collaborative approaches to mitigate risks.

One of the significant issues identified is the susceptibility of robotic systems to unauthorized access and data breaches [28]. These vulnerabilities stem from the interconnected nature of modern robotic systems, which often rely on network communications for operational flexibility and efficiency. To counteract these threats, the implementation of advanced authentication mechanisms and secure communication protocols is paramount. Furthermore, encryption techniques must be rigorously applied to safeguard sensitive data transmitted across networks.

Another pressing concern is the threat posed by malware and other cyber-attacks, such as ransomware, which can severely disrupt robotic operations and compromise system integrity. Addressing these challenges requires a multi-layered security strategy that includes the development of resilient software architectures, regular security audits, and continuous monitoring for potential threats. Additionally, there is a need for dedicated cybersecurity training for personnel involved in the development and maintenance of robotic systems to ensure they are equipped to handle evolving cyber threats.

The article also underscores the importance of collaboration among industry stakeholders, researchers, policymakers, and cybersecurity experts. Such collaboration is essential for the development of standardized security protocols and the sharing of best practices. By fostering a culture of shared responsibility and continuous learning, the robotics industry can enhance its overall security posture and better protect against cyber threats.

8. Conclusion

In conclusion, as robotics technology continues to evolve and become increasingly integrated into various sectors, it is imperative to prioritize cybersecurity measures to safeguard robotic systems. The interconnected nature of robots introduces significant vulnerabilities, including unauthorized access, data breaches, and network attacks, which can compromise sensitive data and erode trust. Remote access features, while offering operational flexibility, also present security risks if not properly secured, highlighting the importance of robust authentication mechanisms and secure interfaces.

Moreover, the threat of malware and cyber-attacks, such as viruses, worms, and ransomware, poses additional challenges to the security of robotic systems. To address these risks, a comprehensive approach is essential, encompassing secure design principles, encryption techniques, and cybersecurity training for stakeholders involved in robotics development and deployment. Collaboration among industry players, researchers, policymakers, and cybersecurity experts is critical to developing resilient robotic systems capable of withstanding evolving cyber threats.

In essence, this article emphasizes the urgent need to address cybersecurity challenges in robotics to ensure the safety, integrity, and security of robotic deployments across diverse domains. By implementing robust cybersecurity measures and fostering collaboration among stakeholders, we can enhance the resilience of robotic systems and mitigate the potential impact of cyber threats on society.

9. Future work

Future research should prioritize the comprehensive collection and systematic analysis of data on recent cybersecurity incidents involving robotic systems across various industries. This effort will help identify prevalent threats and vulnerabilities and assess the impact of different types of cyber-attacks on robotic operations. Proposing and implementing sophisticated encryption methods tailored specifically for robotic systems is crucial. These methods should provide robust security without significantly compromising the performance or operational efficiency of the robots. Incorporating artificial intelligence and machine learning algorithms into robotic systems can enhance their ability to detect and respond to cyber threats in real-time, as AI-driven threat detection systems can analyze vast amounts of data to identify anomalies and potential security breaches, enabling quicker and more effective responses.

Additionally, developing and testing comprehensive security frameworks that encompass secure design principles, risk assessment methodologies, and incident response strategies is essential. These frameworks should be adaptable to various robotic systems and applications. Encouraging interdisciplinary research and collaboration between cybersecurity experts, roboticists, and industry practitioners can lead to innovative solutions that address the unique security challenges of robotics. Joint initiatives and knowledge-sharing platforms can facilitate the exchange of ideas and best practices. Finally, enhancing the cybersecurity awareness and skills of users and developers of robotic systems through targeted education and training programs can significantly reduce the risk of cyber-attacks. These programs should cover the latest security threats, defensive techniques, and the importance of adhering to security protocols.

Availability of data and material

Not applicable.

Authors contribution

All authors have read and approved the final manuscript.

Funding

This research did not receive any funding.

Declaration of competing interest

The authors affirm that they have no competing interests.

Acknowledgement

Not Applicable.

References

[1] A. Krishnan, Killer Robots, Routledge, 2016, doi:10.4324/9781315591070.
[2] M. Alsharif, S. Mishra, M. AlShehri, Impact of Human Vulnerabilities on Cybersecurity, Computer Systems Science and Engineering 40 (3) (2021) 1153–1166, doi:10.32604/CSSE.2022.019938.
[3] I. Abeykoon, X. Feng, A Forensic Investigation of the Robot Operating System, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2017, pp. 851–857, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.131.
[4] A. Laitinen, M. Niemelä, J. Pirhonen, Demands of Dignity in Robotic Care, Techné: Research in Philosophy and Technology 23 (3) (2019) 366–401, doi:10.5840/techne20191127108.
[5] J.H. Hong, E.T. Matson, and J.M. Taylor, "Design of Knowledge-Based Communication between Human and Robot Using Ontological Semantic Technology in Firefighting Domain," 2014, pp. 311–325. doi: 10.1007/978-3-319-05582-4_27.
[6] P. Schulte, Future war: AI, drones, terrorism and counterterror, Handbook of Terrorism and Counter Terrorism Post 9/11, Edward Elgar Publishing, 2019, doi:10.4337/9781786438027.00045.
[7] A. Krishnan, Killer Robots, Routledge, 2016, doi:10.4324/9781315591070.
[8] R.R. Murphy, S. Tadokoro, A. Kleiner, Disaster Robotics, 2016, pp. 1577–1604, doi:10.1007/978-3-319-32552-1_60.
[9] I. Abeykoon, X. Feng, A Forensic Investigation of the Robot Operating System, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2017, pp. 851–857, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.131.
[10] F.A. Auat Cheein, R. Carelli, Agricultural Robotics: Unmanned Robotic Service Units in Agricultural Tasks, IEEE Industrial Electronics Magazine 7 (3) (Sep. 2013) 48–58, doi:10.1109/MIE.2013.2252957.
[11] P. Simoens, M. Dragone, A. Saffiotti, The Internet of Robotic Things, Int. J. Adv. Robot. Syst. 15 (1) (2018) 172988141875942, doi:10.1177/1729881418759424.
[12] F. Jahan, W. Sun, Q. Niyaz, M. Alam, Security Modeling of Autonomous Systems, ACM. Comput. Surv. 52 (5) (2020) 1–34, doi:10.1145/3337791.
[13] H. Noura, R. Couturier, C. Pham, A. Chehab, Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2019, pp. 1–8, doi:10.1109/WiMOB.2019.8923144.
[14] H. Choi, S. Kate, Y. Aafer, X. Zhang, D. Xu, Cyber-Physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York, NY, USA, 2020, pp. 263–278, doi:10.1145/3372297.3417249.
[15] R.D. Marcus, Learning 'Under Fire': Israel's improvised military adaptation to Hamas tunnel warfare, Journal of Strategic Studies 42 (3-4) (2019) 344–370, doi:10.1080/01402390.2017.1307744.
[16] R. Steff, J. Burton, S.R. Soare, Emerging Technologies and International Security, Routledge, 2020, doi:10.4324/9780367808846.
[17] A. Nuhu, A.F. Mat Raffei, M.F. Ab Razak, Abubakar Ahmad, Distributed Denial of Service Attack Detection in IoT Networks using Deep Learning and Feature Fusion: A Review, Mesopotamian Journal of CyberSecurity 2024 (2024) 47–70, doi:10.58496/MJCS/2024/004.
[18] D.S. Jat and C. Singh, "Artificial Intelligence-Enabled Robotic Drones for COVID-19 Outbreak," 2020, pp. 37–46. doi: 10.1007/978-981-15-6572-4_5.
[19] G. Golovko, A. Matiashenko, N. Solopihin, DATA ENCRYPTION USING XOR CIPHER," Системи управління, навігації та зв'язку, Збірник наукових праць 1 (63) (2021), doi:10.26906/sunz.2021.1.081.
[20] A. Chowdhury, G. Karmakar, and J. Kamruzzaman, "Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches," 2017, pp. 284–299. doi: 10.4018/978-1-5225-2154-9.ch019.
[21] P. Dash, M. Karimibiuki, K. Pattabiraman, Stealthy Attacks against Robotic Vehicles Protected by Control-based Intrusion Detection Techniques, Digital Threats: Research and Practice 2 (1) (2021) 1–25, doi:10.1145/3419474.
[22] J. Petit, S.E. Shladover, Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems (2014) 1–11, doi:10.1109/TITS.2014.2342271.
[23] A. Chowdhury, G. Karmakar, and J. Kamruzzaman, "Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches," 2017, pp. 284–299. doi: 10.4018/978-1-5225-2154-9.ch019.
[24] B. Kehoe, S. Patil, P. Abbeel, K. Goldberg, A Survey of Research on Cloud Robotics and Automation, IEEE Transactions on Automation Science and Engineering 12 (2) (2015) 398–409, doi:10.1109/TASE.2014.2376492.
[25] A. Morris, et al., Recent developments in subterranean robotics, J. Field. Robot. 23 (1) (2006) 35–57, doi:10.1002/rob.20106.
[26] D. Tiwari, B. Mondal, S.K. Singh, D. Koundal, Lightweight encryption for privacy protection of data transmission in cyber physical systems, Cluster. Comput. 26 (4) (2023), doi:10.1007/s10586-022-03790-1.
[27] Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects, Mesopotamian Journal of Cyber Security (2022) 1–4, doi:10.58496/MJCS/2022/001.
[28] A. Laitinen, M. Niemelä, J. Pirhonen, Demands of Dignity in Robotic Care, Techné: Research in Philosophy and Technology 23 (3) (2019) 366–401, doi:10.5840/techne20191127108.
[29] Available at https://www.dailymail.co.uk/sciencetech/article-12869629/Tesla-robot-ATTACKS-engineer-companys-Texas-factory-violent-malfunction-leaving-trail-blood-forcing-workers-hit-emergency-shutdown-button.html.
[30] Available at https://www.businessinsider.com/robot-crushed-man-death-mistook-him-box-vegetables-south-korea-2023-11.
[31] Young, B. (2018). The first 'killer robot' was around back in 1979. https://science.howstuffworks.com/first-killer-robot-was-around-back-in-1979.htm.