

Comprehensive Guide to Home Robot Security: From System Analysis to Solution Recommendation

Seyyed Mohsen Hashemi^{1,*} and Patrick C. K. Hung²

¹ Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran 1477893855, Iran

² Faculty of Business and IT, Ontario Tech University, Oshawa, ON L1G0C5 Canada, zpatrick.hung@ontariotechu.ca

*Corresponding author: hashemi@srbiau.ac.ir

Abstract: The increasing range of applications for home robots has heightened the need to address their security challenges. Evaluating the security of these robots requires considering not only potential vulnerabilities but also the diversity of their applications and architectures. This study highlights the limitations of prior research on home robot security and underscores the necessity for more comprehensive investigations. By incorporating insights from analogous systems such as Cyber-Physical Systems (CPS) and smart home technologies, we draw relevant comparisons to enhance understanding. Home robots, as integral components of smart home ecosystems, demand a focus on safety, privacy, and security across CPS architecture layers. Effective deployment requires tailored security frameworks guided by reference models and architectures. Constraints in computing power and energy necessitate cloud and fog computing for robust solutions. Additionally, mapping threats, vulnerabilities, and mechanisms while addressing AI-induced challenges, such as expanded attack surfaces and ethical concerns, is critical for optimal risk management.

Keywords: Home Robot, Cyber-Physical System, Smart Home, Security, Privacy, Safety

1 Introduction

This section commences by delineating the scope of home robots, examining their foundational concepts, and emphasizing the significance of security as a pivotal aspect of the topic, along with the distinguishing characteristics of home robots. The section further addresses the challenges and proposed solutions discussed in the article. Finally, it outlines the article's contributions and presents an overview of the structure of the subsequent content.

A robot is a reprogrammable, multifunctional electromechanical device designed to execute tasks typically performed by humans [1]. A home robot, also referred to as a domestic robot, is an autonomous system primarily employed for household chores. Additionally, it may serve applications in education, entertainment, or therapy.¹

According to ISO 8373 [2], robots can be classified into several categories: industrial, home, service, and military. This study does not address industrial and military robots, as they are beyond its scope. While service and social robots share certain functions with home robots, they are not confined to the home environment.

The primary objective of this work is to enhance the security of home robots, ensuring their reliable operation while identifying and addressing key security challenges within this domain.

The preliminary review revealed that, in addition to the diverse applications and quality attributes inherent in home robots, a notable conflict exists between their security features, privacy concerns, and safety requirements. Moreover, the implementation of security mechanisms in home robots is constrained by limited computational and energy resources. These challenges collectively characterize home robots as distinct systems that necessitate customized approaches to security.

¹ Encyclopædia Britannica, "Robot | Definition, History, Uses, Types, & Facts," <https://www.britannica.com/technology/robot-technology>, accessed: 2024-08-01.

This system exhibits differences when compared to analogous systems. Unlike industrial robots, home robots operate in environments characterized by higher levels of uncertainty, which significantly increases their safety risks. In contrast to Cyber-Physical Systems (CPS), home robots involve distinct privacy considerations. Furthermore, when compared to smart home systems, home robots incorporate more advanced actuators, thereby intensifying safety-related threats.

Given these challenges and the growing adoption of home robots, ensuring their security is of paramount importance. Consequently, the development of comprehensive solutions to safeguard the security of home robots is essential. The principal challenges and proposed solutions discussed are outlined as follows:

- Given the paramount importance of ensuring security in home robots, our initial step was to assess the state of security in existing literature. However, we encountered considerable variability in the functionalities of home robots, which introduced complexity into this analysis.
- The functions of the application determine the system's architecture [3], and architectural decisions are crucial for achieving a high level of security within the system [4]. Therefore, to evaluate the security of a home robot, it is essential to assess both its applications and architecture.
- After analyzing the applications and architectures, we directed our focus to reviewing the relevant research on their security aspects. However, it was observed that research on the security of home robots is both limited and fragmented.
- Due to the limited research on the security of home robots, we have expanded the scope of our investigation. To this end, we have incorporated security topics from robotics, cyber-physical systems (CPS), and smart home technologies to develop more comprehensive security solutions for home robots.
- Home robots, as a subset of robots, possess physical characteristics that are closely associated with CPS [5]. An approach to evaluating the security of home robots involves analyzing the potential threats and vulnerabilities inherent in CPSs, as well as the security mechanisms that have been implemented.
- Since smart homes and home robots operate within similar environments and face comparable security threats, we have employed a smart home security analysis to assess the security of home robots.

A thorough review of the existing literature revealed that studies focusing on the security of home robots are limited. More specifically, no dedicated survey or literature review articles addressing the security of home robots currently exist. While related works in analogous fields such as Cyber-Physical Systems (CPS), smart homes, and general robotics provide valuable insights, they do not specifically address the unique security challenges and requirements of home robots. Consequently, this manuscript stands out by not only reviewing the limited works directly related to home robots but also by drawing insights and methodologies from survey papers in these related domains. Specifically, the adoption of classifications and the development of frameworks for addressing security issues were inspired by these related studies. This integrated approach, combining a focused review on home robots with insights from related domains, establishes the novelty and significance of this work.

This article seeks to offer a comprehensive examination of the security aspects associated with home robots. The primary contributions of this research are outlined as follows:

- Analyzing the security, architecture, and applications of home robots.
- Integrating insights from CPS, robotics, and smart home security to enhance the security of home robots.
- Providing a comprehensive set of guidelines derived from studies on home robot security.

Following this article, the "Method" section will present an in-depth security analysis of home robots and related systems. In contrast, the "General Direction" part will provide an overview of the primary orientations. The "Conclusion" section will subsequently summarize the findings and draw final conclusions.

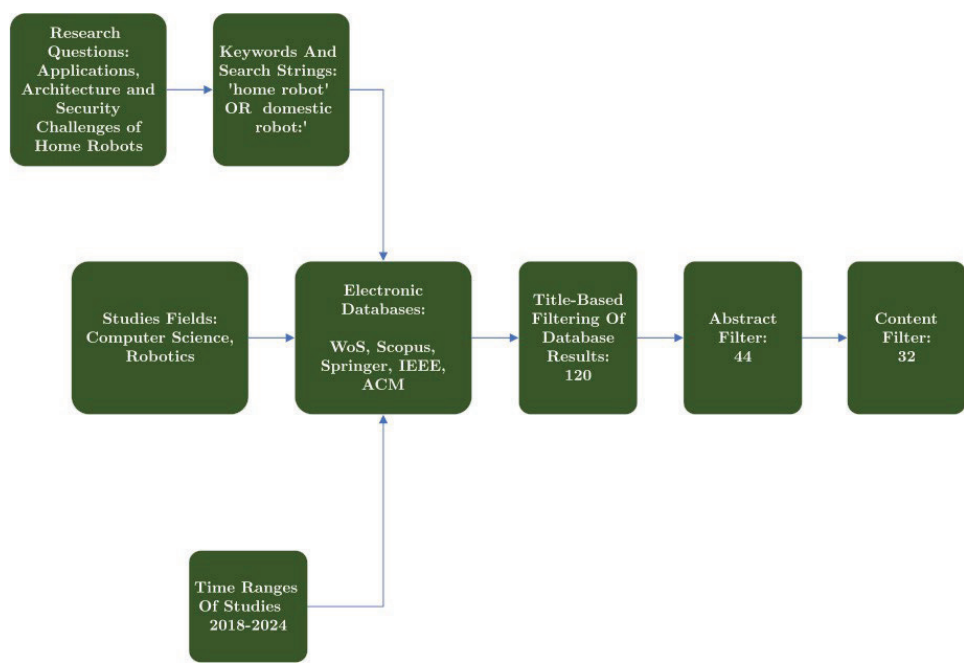


Figure 1. Systematic Review Methodology for Analyzing Home Robot Applications, Architectures, and Security Challenges

2 Method

This section evaluates the security of home robots by first addressing concerns related to their applications and architecture. Furthermore, security challenges encountered in comparable systems will be examined, with an emphasis on adapting solutions to enhance the protection of home robots.

2.1 Home Robot Security Analysis

In this subsection, we analyze the security challenges associated with home robots, which are influenced by their applications and architectures. To achieve this, a systematic review was conducted to address three key research questions: the applications of home robots, their architectural considerations, and associated security concerns. Keywords were derived from these questions, but due to the limited availability of relevant literature, the search string was refined to “home robot” or “domestic robot.” To address the scarcity of sources, the temporal scope of the review was expanded to include studies from 2014 to 2024. The review focused on computer science research and utilized databases such as Web of Science, Scopus, Springer, IEEE, ACM, and Google Scholar. Filters were applied based on the study field, time range, and search string. Relevant studies were selected for their alignment with the research questions, prioritizing discussions on applications, architecture, and security mechanisms while excluding works centered on specific algorithms or unrelated topics. This process is visually summarized in Figure 1.

Table 1. Applications of Home Robots

Applications and Sub-applications			References
Social Robot			[6, 7, 8, 9]
Companion Robot			[10]
Care	Elderly Care Robot	General	[6, 10, 11, 12, 13, 14, 15]
		Fall Detection	[11, 16]
	Single Care		[17]
	Child Care Robot	General	[13]
		Telepresence	[18]
	Personal Care		[19]

Cooking		[6, 20]
	General	[16]
Entertainment	Music Player	[6]
	Social Media Access	[13]
	Drug Reminder	[16]
	Drug and Food Estimation	[21]
Health Care	Medication Reminders	[6, 22]
	Monitor Health	[22]
	General	[6, 23]
	Clean Floors	[22]
Cleaning and Organization	Vacuuming	[20]
	Self-making Bed	[20]
	Automatic Bookshelf or Cupboard	[20]
	General	[16, 22, 23]
Find and Bring Objects	Bring Coffee	[20]
Cloth	Folds Laundry	[20]
	Garment Folding	[20]
	Dressing	[22]
Lawn Mower		[20]
Movable Trash Bins		[20]
Home Security	Monitoring of Houses	[13, 24, 25]
Smart Home Assistant		[26, 27]
Rollator Walker		[28]
Transfer		[22]

The functions and applications defined for home robots determine their assets and, consequently, the associated threats and vulnerabilities that must be addressed. Therefore, we will explore these aspects as an introduction to the security of home robots. Table 1 presents the categories of home robot applications, with corresponding references cited in each row.

Given the diverse functions and applications of home robots, employing reference models for the initial analysis and design of security measures for home robots is a recommended approach.

Another important aspect to consider when discussing the security of home robots is their architectural design. These architectural considerations directly influence the levels of security, safety, and privacy. It is essential to ensure the security of home robots while also addressing other critical quality dimensions, such as energy efficiency and performance, and to engage with the technical debates surrounding these aspects.

A variety of topics have been explored concerning the architectural considerations for home robots. Table 2 categorizes these topics and lists the relevant articles. Given the multiple aspects of home robot architecture, it is advisable to address their security early on through the use of a reference architecture. Considering the limitations in energy and computing resources, cloud computing infrastructure emerges as a viable solution.

Finally, studies addressing security, safety, and privacy in home robots were reviewed. These studies concentrated on aspects such as threats, vulnerabilities, attacks, and security mechanisms, alongside general topics related to security principles. Table 3 presents the security considerations. It appears that the security issues identified in home robot studies are primarily non-technical, with privacy being the foremost concern. The significance of safety in home robots is amplified by environmental uncertainties, and security concerns are frequently addressed at the network layer.

Table 2. Architecture considerations of home robots

	Architecture Consideration	References
Infrastructure	Cloud	[28]
	Mobile phone	[27]
	Home Personal Computer (PC)	[28, 7]
System	Smart home	[27, 29, 30]
	Robot group	[23]
	Autonomous	[18]
Operation modes	Remote controller (monitor, command execution)	[7]
Device behavior	Interactive	[18]
	Proactive, reactive	[10]
Device appearance	Creature, object	[10]
Device function	Assistive, companion, service	[10]
Device mobility	Mobile, stationary	[10]
Separable device		[31]
Infrastructural services	Object recognition (detection)	[21, 12],
	Remote control	[31]
	Obstacle avoidance	[31]
	Tracking (follow user, come to the user)	[31]
	Power metering	[31]
	Assistance decision maker	[12]
	Positioning and navigation, map construct	[12] [19, 16],
	Grasping	[12]
	User interface	[12, 20]
	Robots collaboration management	[20]
	Face and gesture recognition	[20, 19, 16]
	Simultaneous Localization and Mapping (SLAM)	[19]
	Planning	[19]
	Text to speech	[16]
	Speech recognition (robot call)	[16]
	Robot setup	[16]
	Self-charge	[16]
	Image and video transfer and automatic video recording	[28]
	Distance estimation	[28]
Software service design	Representational State Transfer (REST) as a platform independent protocol	[32]
Sensor	Laser, noise, light	[12]
Robot and human interaction	Verbal, non-verbal	[20]
Design goals	Engaging, unobtrusive, device-like, respectful, reassuring	[26]

An analysis of home robot applications, architecture, and security reveals that security concerns have not been adequately addressed. Given the limitations in current home robot security research, it is crucial to place greater emphasis on identifying and addressing security concerns, vulnerabilities, and threats.

Table 3. Security Issues of Home Robots

Security Considerations		References
Main Issues	Attacks	Denial of Service (DoS)
		Analyzing packet capture
		Privacy violation (especially for social interactions with robots) for some goals (location, object, information)
	Threats	Active and passive eavesdropping
		Network security breach
		Robot vandalism
		Spying
		Interface application
		Remote execution of code
		Status Check
	Vulnerabilities	Allocation of a static Internet Protocol (IP) Address
		Availability of open ports
		Unsupervised data exchange
		Internet connection
		Webcam
		Authentication
		Two-factor authentication
	Mechanisms	Biometrics as a second factor in authentication
		The privacy-utility tradeoff for remotely teleoperated robots that decrease image quality when sending it
		Situational awareness
		Privacy
		Ethical implications: Assisting elderly or disabled people, monitoring of houses, accessing social media, childcare
General Issues	Principles	Trust
		Safety: The home robot faces more uncertainty in the environment than the industrial robot, posing more safety concerns.
Architecture Issues	Security issues are primarily discussed in the network layer.	

2.2 Examining Security in Systems Analogous to Home Robots

In this section, we aim to address the security concerns associated with home robots by conducting a complementary security analysis of systems similar to home robots. Given that home robots are a specific type of robot and can be classified as cyber-physical systems (CPS) due to their physical attributes, and considering that smart homes operate in a comparable environment, we analyze the security of these systems to integrate their findings into the security framework for home robots.

The review presented in this section was conducted through a series of systematic steps to ensure a comprehensive analysis of security issues relevant to home robots. Initially, research questions were formulated to explore security challenges in robots, cyber-physical systems (CPS), and smart homes, focusing on their applicability to home robot security. Key terms such as “robot,” “CPS,” “smart home,” along with “security,” “privacy,” and “safety,” were identified, emphasizing the semantic overlap between these concepts. Given the extensive body of research in these domains, the study prioritized review papers, incorporating terms like “survey” and “systematic literature review” into the search string. The review was conducted across major electronic databases, including Web of Science, Scopus, Springer, IEEE, ACM, and Google Scholar, applying filters to select computer science studies published between 2014 and 2024. Papers were rigorously screened based on their titles and abstracts, duplicates were eliminated, and the remaining studies were categorized according to the research questions. Finally,

a backward snowballing technique was employed, screening references of the selected studies to identify additional relevant works, thereby ensuring a robust and thorough review process.

This systematic review process is depicted in Figure 2, offering a detailed overview of the methodological steps undertaken.

It is important to emphasize that this analysis aims to identify the security landscape and issues relevant to home robots, rather than conducting an in-depth evaluation of the security of analogous systems such as robots, CPS, or smart homes. To achieve this, we employ classification techniques to analyze the existing literature. While this approach offers less detail than a comprehensive security analysis, it allows us to systematically categorize the studies and extract insights that will serve as the foundation for developing a research framework to enhance home robot security.

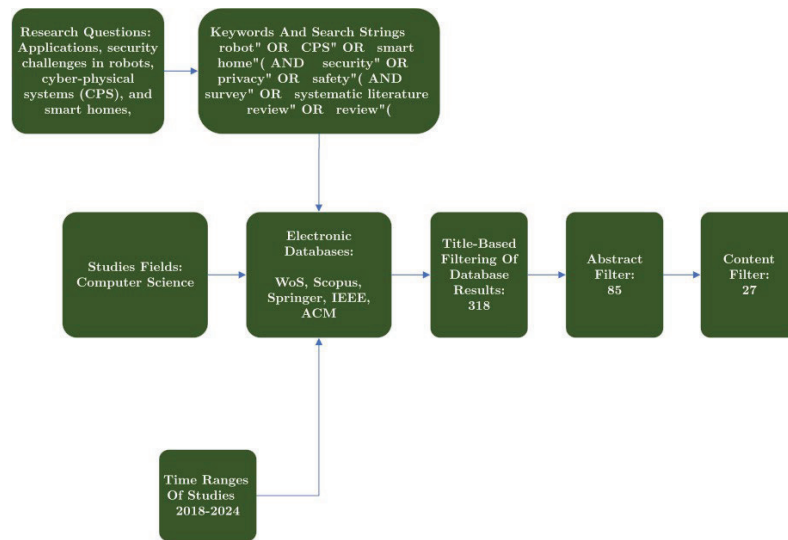


Figure 2. Systematic Review Framework Leveraging Security Insights from Related Systems for Home Robots

Papers on robots, CPS, and smart homes will be analyzed separately. Through a general classification and analysis of the security of each system, we will outline potential directions for improving home robot security. The dimensions of article classification, as shown in Figure 3, are as follows:

The general description of the dimensions proposed for classifying security topics is outlined as follows:

- General security issues
 - Security principle or quality attributes: safety, privacy, security, trust, confidentiality, integrity, and availability
 - Legal and ethical concerns: These are particularly important in the sense of privacy.
 - Standards: Include safety and security standards.
 - Challenges: Include system architecture challenges that affect system security.
- Main Security issues
 - Vulnerabilities: Assets and identifying their vulnerabilities are among the most important aspects of security analysis.
 - Threats: This dimension includes threat paths.
 - Attacks: This dimension includes attack paths.
 - Mechanisms: Mechanisms are built around threats, attacks, and vulnerabilities. They can also be classified by the timing of the actions. The solution, control, mitigation strategy, and method are considered equivalent to the mechanism.
- Architecture (Architecture considerations are discussed when and where it was necessary)
 - Assets
 - * Cyber, physical, and cyber-physical are types of cyber-physical components.
 - * Hardware, applications, middleware, and communications are types of cyber components.
 - Layers
 - * Perception, communication, and application are common layers.
 - Infrastructure Types: Infrastructure enhances energy efficiency and computing capabilities and includes cloud, fog, edge, gateway, PC, and mobile.

Subsequently, each of the analogous systems will be analyzed according to these dimensions.

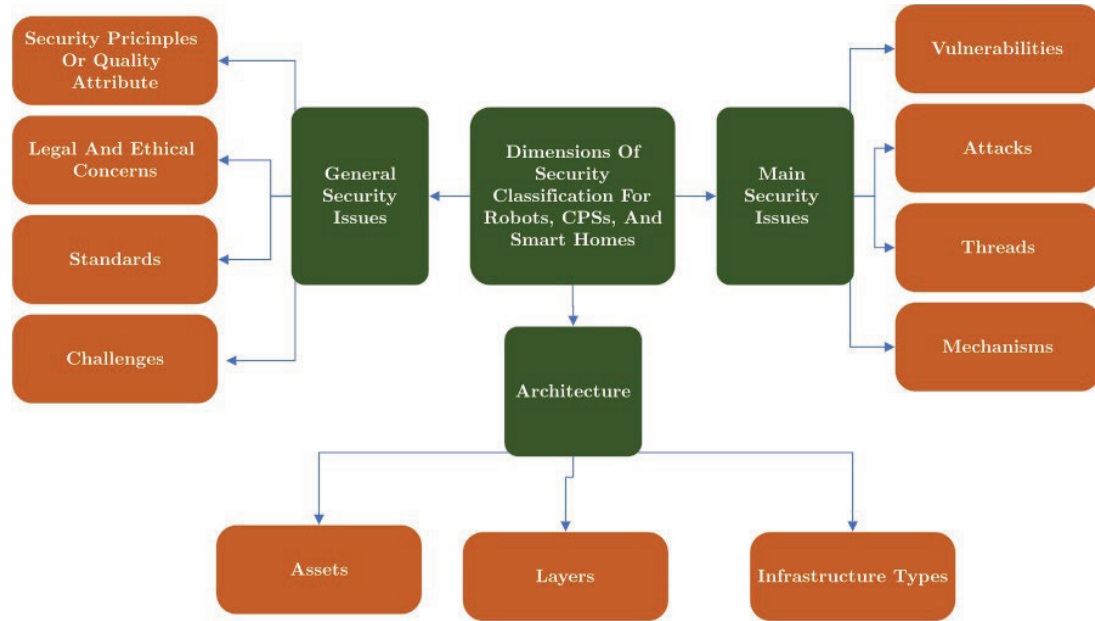


Figure 3. Dimensions of Security Classification for Robots, Cyber-Physical Systems (CPS), and Smart Homes

2.2.1. Robot Security

Review articles on robot security were reviewed to identify relevant concepts for home robots.

A survey was conducted to assess users' primary privacy concerns [38]. The results indicated that protecting identity and financial information are the foremost priorities. Additionally, users' understanding of the importance of privacy is influenced by their level of technological knowledge.

The article presented in [39] examines the privacy challenges associated with the use of Artificial Intelligence (AI) in robots and reviews various global legal frameworks. It explores one such framework for the coordinated deployment of AI in robots and analyzes the privacy concerns that arise from its implementation. The challenges and issues related to robot reliability and safety, along with an in-depth analysis of robot safety, are discussed in [40]. Key advancements in robotics include the ability to move simultaneously with humans, cooperate and engage in physical contact with the robot, perform automation tasks, multitask, and operate in uncertain environments. These developments have introduced new safety challenges when compared to earlier industrial robots. The article presents a series of activities aimed at improving safety in response to the evolving capabilities of robots.

A specific topic discussed regarding robot safety is the field of Human-Robot Interaction (HRI). In this regard, the article presented in [41] provides a systematic review of the safety levels required in HRI. The paper focuses on the primary functions of Human-Robot Interaction, including Robot Perceptions, Cognitive Control, Action Planning, Hardware Safety Features, and Societal and Psychological Factors. These areas are considered as the key domains related to safety in human-robot relationships.

According to ISO standard 8373: 2012 [42], service robots and home robots share similar functions. In light of their close relationship, we examine an article on the security of service robots [43]. This article offers an overview of the initial risk analysis for service robots and explores various examples of potential threat vectors and attacks.

Another article [44] focuses on the cyber-physical security of mobile service robots. The article first presents statistics on known threat vectors in CPS, followed by a classification of assets, attack vectors, and the effects of these attacks on the robot. It then examines a set of mechanisms and ultimately connects these mechanisms to relevant security functions.

The article presented in [45] discusses cyber-physical threats within the context of robotics. Although not a review, this article is analyzed due to its examination of various threats to robots, evaluation of risks based on these threats, and proposed solutions to mitigate those risks. Utilizing the Confidentiality, Integrity, and Availability (CIA) triad of security, the article investigates various attack vectors and their effects, with a particular focus on harmful threats.

In [46], a threat model is presented to facilitate a better understanding of the potential risks associated with home robots. The article also provides a comprehensive set of possible attack effects to support more effective risk analysis. The proposed risk model is based on attack effects and considers the various types of robot users. Privacy risks related to social robots are assessed with a focus on sensor data, while safety risks are evaluated through a series of scenarios. Finally, the article identifies several attacks that could lead to privacy and security issues.

Robot security threats are further explored in [47], which provides an overview of various robot attacks. The article examines the security aspects of three types of business robots, identifying their vulnerabilities and proposing methods to mitigate risks. Although the article includes several privacy tips, they are non-technical in nature and were not discussed in detail.

In [48], a range of attacks and corresponding mitigation processes are examined, although these are not classified in detail. This article is noteworthy for its comparison of the vulnerabilities of two home robots, Rovio and Spykee, specifically focusing on eavesdropping, noise interference, and vulnerabilities related to audio and video streaming.

The study presented in [49] investigates attacks across multiple layers, including data, networks, operating systems, and physical components. It also explores various tools for securing the widely used middleware, Robot Operating System (ROS). Furthermore, the research examines the security aspects of different types of robots, taking into account their diverse functionalities.

Significant advancements in robotics and their security, including the history of their initial deployment in industrial settings, early safety incidents, the integration of safety and security models, the development of security models based on the Robot Operating System (ROS), the creation of a robot vulnerability database, and the formulation of a security assessment framework for robots, are thoroughly discussed in [50].

Artificial Intelligence (AI) introduces unique security challenges for robotics, particularly when integrated into decision-making processes. For instance, Large Language Models (LLMs) significantly enhance robotic capabilities but also introduce substantial security risks, especially when handling sensitive data or executing automated operations. Key concerns include expanding attack surfaces, implementing effective defensive strategies, addressing ethical considerations, and managing HRI. These challenges must be carefully addressed to mitigate risks and ensure the safe and effective integration of AI into robotics. [51].

Table 4 presents a detailed overview of key topics associated with robot security, offering valuable insights into the various dimensions of the challenges and potential solutions for ensuring the security and safety of robotic systems.

Table 4. Overview of Security Issues and Classifications for Robots

Issue	Classification or General Description	References
General issues	Privacy issues	[38, 39]
	Safety issues	[40, 41, 50]
	Architecture layers	[49]
	AI usage	[51]
	ROS Middleware	[49, 50]
Vulnerabilities	Comparison of two home robots (Rovio and Spykee)-50	[48, 50]
Threats	Classification based on Degree of risk	[45]
	Classification based on Assets that are the target of an attack	[43]
Attacks	Classification based on the motives of the attackers	[43]
Main issues	Without classification	[46, 47, 48]
	Classification based on the type of attack and the time that we apply the mechanism	[44]
Mechanisms	Risk analysis	[46]
	Classification based on the type of assets	[43, 47]
	Without classification	[48]

The following is a list of directions for enhancing home robot security derived from the review of robot security literature:

- Given the similarities between home robots and other types of robots, many security concerns can be adapted and customized for home robots.
- The design of home robots should take into account their applications, functions, quality attributes, as well as the unique challenges and standards specific to robots.
- The importance of privacy must be explicitly acknowledged, and the value of data, along with its associated risks, should be carefully considered when implementing security mechanisms. Additionally, privacy concerns related to artificial intelligence in home robots must be addressed.
- Ensuring safety poses significant challenges both at the robot level and within the home environment. Home robots must adhere to established safety standards, with particular attention given to factors such as uncertainty, human interaction, and the physical effects that these robots may experience.
- Securing a home robot should be approached through risk management. Assets, vulnerabilities, security principles, threats, attacks, and mechanisms must be thoroughly considered within the risk management framework. Mapping these entities in the risk analysis process is crucial, as it directly influences understanding and enhances the overall security of the home robot.
- The timing of security mechanisms, the associated risks, and the security level of each mechanism must be carefully determined to ensure an optimal balance between protection and system performance.
- The security of ROS middleware must be a key focus in enhancing the safety and security of robots.
- Integrating AI into robots enhances functionality but introduces security challenges, such as increased attack surfaces and ethical concerns. Addressing these issues is crucial for safe AI integration in home robotics.

2.2.2. *CPS Security*

In this section, we aim to strengthen the security of home robotics by utilizing established security solutions from CPS. This is achieved through a comprehensive review of existing security measures employed in CPS to identify strategies applicable to home robotics.

Several studies offer foundational insights into CPS security by addressing general concepts, architectures, and security principles. For example, [52] categorizes security challenges through the lenses of control theory and cybersecurity, with an emphasis on specific CPS types and their associated assets, such as communication protocols and PLC software.

Another study, [53], introduces a comprehensive CPS model structured around a three-layer architecture comprising the application, data transfer, and perception execution layers. The study further classifies relevant attacks within each layer. Similarly, [54] proposes a versatile framework that achieves a balance between generalization and specialization, rendering it applicable to a wide range of CPS types, albeit with certain limitations. This framework emphasizes a three-layer CPS architecture—perception, communication, and application—while providing valuable insights into the physical, cyber-physical, and cyber components across various CPS implementations.

Further contributions to general CPS topics are provided in [55], which presents a layered CPS architecture while exploring control and sensor components, as well as the integration of CPS with IoT systems. Similarly, [56] offers a comprehensive examination of CPS security and privacy, providing an overview of key CPS concepts and addressing challenges such as heterogeneity, seamless integrity, and mobility. Additionally, this study discusses CPS virtualization for resource sharing and introduces a framework encompassing cyber, physical, and hybrid security measures.

On the more specialized side, several studies provide in-depth analyses of security mechanisms, attack types, vulnerabilities, and risk management strategies in CPS. For instance, [57] examines vulnerabilities, threats, security attacks, and privacy concerns within CPS, offering a comprehensive set of solutions while categorizing threats according to CPS layers. This study is notable for its detailed exploration of current research in CPS security. Similarly, [58] investigates the integration of smart CPS with IoT, classifying attacks and security methods based on CPS layers and addressing challenges such as data volume and energy efficiency considerations.

[59] categorizes CPS security into information security and control security, highlighting the distinctions between CPS security and traditional cybersecurity. This study offers a detailed assessment of security risks, attacks, and challenges across different CPS layers. Similarly, [60] focuses

specifically on sensor security, analyzing attacks targeting sensors and exploring corresponding defense mechanisms.

Risk management is a critical topic explored in [55], which discusses threats, vulnerabilities, and attacks from both cyber and physical perspectives, as well as solutions such as cryptography, intrusion detection systems, and forensics. The work by [61] also contributes to this area by examining CPS security through the lens of both cyber (information) and physical (control) perspectives, analyzing vulnerabilities and solutions. Finally, a comprehensive survey by [62] categorizes CPS security into architectural layers, applications, and mechanisms, providing an in-depth analysis of attacks, defense strategies, and technologies relevant to CPS security within specific scenarios. Similarly, [63] examines CPS security with a focus on cyber and user interactions, addressing critical factors such as availability, safety, and reliability. This study also highlights key distinctions between CPS and traditional IT security, while discussing risk design and estimation, as well as security controls within the physical domain.

The following key directions for enhancing home robot security have been derived from the comprehensive review of CPS security:

- While CPS operates at a higher level of abstraction compared to robots, numerous studies provide a comprehensive perspective on security. In the context of home robot security, it is essential to account for challenges presented by specific CPS. Furthermore, CPS mechanisms and solutions can be effectively leveraged, given the complexity and architectural similarities between the two domains.
- Developing reference models and architectures for home robots, similar to those in CPS, enhances our understanding of security challenges and provides clarity on the implementation of security mechanisms in home robots.
- As with CPS, real-time decision-making, environmental uncertainty, mobility, heterogeneity, distribution, layer integrity, and the integration of cyber and physical components present challenges for home robots. Moreover, high data volumes and unwanted events, particularly when combined with IoT, are additional challenges.
- A layered architecture that separates cyber and physical (or control) components should be considered in home robot security assessments. Furthermore, the interrelationships between these layers must also be evaluated in security assessments.
- Although CPS security issues are relatively well-established, their application to home robots necessitates a thorough risk analysis.
- While availability is a critical concern in CPS, it may not be as paramount for home robots. In contrast, safety and privacy issues, particularly for home robots, should be prioritized over availability.

Table 5. Overview of Security Issues and Classifications for CPS

Issues		Classification and General Descriptions	References
General Issues		Differences with ICT security, CPS security challenges, and requirements	[56, 57, 58, 59, 63]
	Vulnerabilities	Classification Based on the cyber and physical components	[55]
		Classification based on architecture layers	[57]
Main Issues	Threats	Classification Based on the Abstract Threats as attack vectors	[56]
		Classification Based on cyber and physical components	[55]
		Classification Based on architectural layers	[58, 59]
	Attacks	Classification Based on the type and function of the attack	[56]
		Classification Based on cyber and physical components	[55]
		Classification Based on the type of attack	[56]
	Mechanisms	Classification Based on cyber and physical components	[57]
		Classification Based on architectural layers	[59, 62]
		Some mechanisms without classification	[55, 56, 58]

2.2.3. *Smart Home Security*

This section examines security measures in the field of smart homes that could be applicable to home robots. Smart home security encompasses multiple dimensions, each addressed in various studies.

Comprehensive frameworks and technological solutions are addressed in [64], which examines the growth of the Internet of Things (IoT), its characteristics, and the security of its layers. The study proposes a four-layer architecture (perception, cyber, physical, user).

In terms of security issues and risk reduction strategies, [65] highlights the difficulties posed by the heterogeneity, diversity, and complexity of smart homes. The article emphasizes that while privacy and security concerns are ubiquitous, they become particularly critical in the smart home context.

When examining vulnerabilities and attacks, [66] provides a brief overview of IoT and smart home applications, focusing on architecture and cloud integration, identifying vulnerabilities in connected objects, cloud services, and applications, and discussing various types of attacks and contemporary defense mechanisms. Additionally, [67] investigates voice-based attacks and their countermeasures.

Another article, [68], reviews well-known smart home communication protocols, highlighting their security and privacy issues and analyzing the security features of several popular smart home platforms. For security mechanisms and strategies, [69] examines privacy, security, authentication, and risk analysis mechanisms, though it does not classify security issues.

Finally, [70] provides a thorough exploration of smart homes, including security requirements, architecture, attacks, and mechanisms. It compares smart homes with cyber networks, identifying unique concerns such as energy and physical security, social engineering, and privacy. The article proposes centralized, distributed, and hybrid architectures and discusses the importance of technologies like blockchain for dynamic, transparent, and distributed access models. It also highlights how cloud technology can overcome energy and computational limitations in smart homes. It addresses the role of soft security, emphasizing the impact of managing human factors such as trust and user awareness on enhancing security.

The general classification of topics related to smart home security is provided in Table 6. The following is a list of directions for home robot security obtained from the smart home security review.

- Specific challenges, like device incompatibility and Internet connection in the smart home, are more important than home robots. On the other hand, because both systems' working environment is home, privacy is their common concern. Home robots' safety is important because of the physical actuators, so research into home robots' safety goes beyond a smart home.
- Privacy in a home robot is as important as in a smart home. Due to the large volume of studies on the privacy of smart homes, it is necessary to incorporate them into the home robot. Challenges such as user trust, user awareness of the sensor-collected information, and the confidentiality of context data such as time and location are some of the smart home privacy challenges that are also being addressed for the home robot.
- Communication protocols and the variety of devices in the smart home are less considered by the home robot. However, there are also challenges, such as a mobile home robot, that are not so important in the smart home.
- The smart home is more at risk due to the pervasive internet connection, although mobility can also increase the robot's privacy risk. That is why smart home articles focus on communication security, and home robot articles focus on the camera and robot sensors.
- There are limitations to computing capabilities and energy consumption in a home robot similar to smart home devices, and infrastructure technologies like the cloud must be used. Cloud-based architecture and gateway-based architecture that are provided for smart homes can also be used for a home robot.
- It should be noted that due to IoT development, we must consider home robots as a part of the smart home architecture.
- The use of blockchain technology, with its dynamic, transparent, and distributed access models, also holds the potential for enhancing security in home robots.

Table 6. Overview of Security Issues and Classifications for Smart Home

Issues	Classification	References
Main Issues	General Issues The Internet of Things(IoT) challenges	[65]
	Vulnerability Software flaws	[68]
	Classification based on security principles violated by the attack	[65]
	Classification based on architectural layers	[64, 66]
	Classification based on security principles violated by the attack	[66]
	Attacks Classification based on the activity of the attack over time	[66]
	Security in collaboration systems (cloud)	[66]
	Classification based on the connected object	[66]
	Classification based on attack target asset	[64, 66]
	Classification based on the activity of the attack over time and the type of attack in the cloud architecture	[64, 70]
	Mechanisms Classification based on architectural layers	[66]
	Classification based on the gateway architecture and its layers	[67]
	Without classification	[68, 69]

3 Discussion and General Direction

After conducting a study on home robot security and the security of similar systems such as CPS and smart homes, general guidelines for home robot security are presented below.

- Home robots encounter several challenges, including heterogeneity, diversity, mobility, real-time requirements, environmental uncertainty, and the integration of cyber-physical components. These challenges impact the architecture, security, and operational mechanisms of home robots, all of which must be carefully considered.
- Given the diversity of home robots, it is essential to utilize reference models and reference architectures to establish security frameworks. Additionally, customizations can be applied to address the specific requirements of each type of home robot.
- Due to the rapid expansion and decreasing costs of smart home devices, home robots can be regarded as integral components of the smart home ecosystem.
- Home robots and smart home devices face constraints in computing capability and energy consumption, which makes it essential to use infrastructures with higher computing capacity and energy efficiency for implementing robust security mechanisms. Cloud and Fog computing, for example, can provide the required resources to execute security algorithms and processes that might otherwise be infeasible on resource-constrained devices.
- A multi-layered architecture should be implemented for home robots, with cyber and physical components clearly defined in each layer. Additionally, assessing security across layers presents another significant challenge.
- Privacy and safety in home robots must be addressed simultaneously. Given the uncertainty of the operational environment, ensuring the safety of home robots is of paramount importance. Additionally, privacy is crucial for home robots, just as it is in smart homes.
- Mapping threats, vulnerabilities, and mechanisms in relation to one another, while incorporating principles of security, safety, and privacy, can lead to an optimal risk management system.
- Threats, attack vectors, and various dimensions of the mechanism (such as operating time) are also critical factors to consider when securing a home robot.
- Integrating AI into home robotics enhances functionality but introduces security challenges, such as increased attack surfaces and ethical concerns. Addressing these issues is crucial for safe AI integration in domestic robotics.

4 Conclusion

A preliminary review of the application, architecture, and security of home robots was conducted to gain a comprehensive understanding of their vulnerabilities, threats, attacks, and security mechanisms. Given the limited content available on home robot security, it was necessary to explore security

topics from similar systems. The security of general types of home robots, including robots and CPS, was investigated. Additionally, since the operating environment of home robots closely resembles that of smart home systems, smart home security was also reviewed. A compilation of security recommendations for home robots was provided in the sections on robot, CPS, and smart home security. In conclusion, home robots face challenges such as heterogeneity, mobility, real-time requirements, and environmental uncertainties, all impacting their architecture and security mechanisms. Utilizing reference models and architectures, with customizations for each robot type, is essential. As integral components of smart homes, these robots often have limited computing capabilities and energy resources, necessitating the use of cloud and fog computing for robust security measures. Implementing a multi-layered architecture with clearly defined cyber and physical components is crucial. Addressing privacy and safety concurrently, especially given the unpredictability of home environments, is imperative. Mapping threats, vulnerabilities, and mechanisms, while integrating security, safety, and privacy principles, leads to optimal risk management for home robots. Ultimately, the integration of Artificial Intelligence into home robots, while enhancing their functionality, introduces critical security challenges that must be carefully addressed to ensure their safe and effective deployment.

5 Acknowledgment

We thank all the researchers who helped us to conduct this research.

6 Declaration

- **Financial or non-financial interest:** All authors certify that they have no affiliations with or involvement in any organization or entity with any financial or non-financial interest in the subject matter or materials discussed in this manuscript. This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.
- **Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.
- **Availability of Data and Materials:** Dataset or special materials that need to refer to availability have not been used.

References

- [1] P.S. Shrugare, A.A. Bokde, N.U. Kashte and S.S. Raut (2018). "Smart phone based robot for domestic purpose using bluetooth". *Sensors*, 115200: 230400, 460800.
- [2] G.S. Virk, S. Moon, and R. Gelin (2008). "ISO standards for service robots", in *Advances in Mobile Robotics 2008*, pp. 133–138.
- [3] K. M. Adams (2015). *Non-functional Requirements in Systems Analysis and Design*. Springer International Publishing, vol. 28.
- [4] Q. Feng *et al.* (2016). "Towards an architecture-centric approach to security analysis", in *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, IEEE.
- [5] P. Jain, P. K. Aggarwal, P. Chaudhary, K. Makar, J. Mehta, and R. Garg (2021). "Convergence of IoT and cps in robotics", in *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation*. Springer, pp. 15–30.
- [6] T. Heuer, I. Schiering, and R. Gerndt (2019). "Me and my robot – sharing information with a new friend", in E. Kosta *et al.* (eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, 20–24 August 2018, Revised Selected Papers*, ser. IFIP Advances in Information and Communication Technology, Cham: Springer International Publishing, vol. 13, pp. 189–204.
- [7] J. Miller, A. Williams, and D. Perouli (2018). "A case study on the cybersecurity of social robots", in *ACM/IEEE International Conference on Human-Robot Interaction*.
- [8] S. Šabanović and W.-L. Chang (2016). "Socializing robots: constructing robotic sociality in the design and use of the assistive robot PARO". *AI & Society*, 31, 537–551.
- [9] B. Cagiltay and B. Mutlu (2024). "Toward family-robot interactions: A family-centered framework in HRI", in *Proceedings of the 2024 ACM/IEEE International Conference on Human-Robot Interaction*, pp. 76–85.

- [10] I. Deutsch, H. Erel, M. Paz, G. Hoffman, and O. Zuckerman (2019). “Home robotic devices for older adults: Opportunities and concerns”. *Computers in Human Behavior*, 98, 122–133.
- [11] E. Bonizzoni *et al.* (2018). “UWB tracking for home care systems with off-the-shelf components”, in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*.
- [12] F. Michalis, A. Margherita, and S. Constantine (2017). “Applying a multimodal user interface development framework on a domestic service robot”, in *Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments*. Island of Rhodes, Greece: ACM, pp. 378–384.
- [13] D. Miglani and A. Hensman (2015). “Vision for secure home robots: Implementation of two-factor authentication”, in *2015 IEEE International Symposium on Technology and Society (ISTAS)*. IEEE, pp. 1–4.
- [14] T. Schulz, J. Herstad, and H. Holone (2018). *Privacy at Home: An Inquiry into Sensors and Robots for the Stay at Home Elderly*. Springer International Publishing.
- [15] M. Yani, A. Besari, N. Yamada, and N. Kubota (2020). “Ecological-inspired system design for safety manipulation strategy in home-care robot”, in *2020 International Symposium on Community-centric Systems (CcS)*. IEEE, pp. 1–6.
- [16] D. Fischinger *et al.* (2016). “Hobbit, a care robot supporting independent living at home: First prototype and lessons learned”. *Robotics and Autonomous Systems*, 75, 60–78.
- [17] G. Gao, Y. Zhang, Y. Bu, and P. Shih (018). “Design exploration on robots to support single women at home in China”, in *2018 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*. IEEE, August, pp. 1–6.
- [18] A. Dante, I. Yuichi, and T. Fumihide (2017). “Design of a home telepresence robot system for supporting childcare”, in *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Portland, OR: ACM, pp. 131–134.
- [19] B.-J. Lee and B.-T. Zhang (2016). “Aupair: A home robot for personal care”, in *Proceedings of the 2016 International Symposium on Perception, Action, and Cognitive Systems (PACS2016)*. Seoul, Korea: Seoul National University, 27–28 October.
- [20] D. Sakamoto, Y. Sugiura, M. Inami, and T. Igarashi (2016). “Graphical instruction for home robots”. *Computer*, 49: 7, 20–25.
- [21] T. Suzuki (2017). “Latest data processing technologies for living state estimation”, in *2017 International Symposium on Micro-NanoMechatronics and Human Science (MHS)*. IEEE, pp. 1–3.
- [22] J. Beer, A. Fisk, and W. Rogers. (2015). “Commanding home robots: A comparison between older adults with and without mobility loss”, in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 59, no. 1. Los Angeles, CA: SAGE Publications, pp. 70–74.
- [23] P. Kalla, K. Ramji, and P. Ravindranath (2018). “Swarm home robots: Next gen maids”, in *2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*.
- [24] Z. Chang, J. Zhong, R. Zhan, M. Liu, and B. Chen (2024). “Design of smart home service robot based on stm32f103”, in *Proceedings of the Third International Conference on Electronic Information Engineering and Data Processing (EIEDP 2024)*, vol. 13184. Bellingham, WA: SPIE, July 2024, pp. 1722–1727.
- [25] K. H. Rahouma, A. R. Ibrahim, and Y. B. Hassan (2022). “Design and implementation of a surveillance smart home robot”. *Egyptian Computer Science Journal*, 46: 2.
- [26] M. Luria *et al.* (2016). “Designing Vyo, a robotic smart home assistant: Bridging the gap between device and social agent”, in *2016 25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*.
- [27] X. Feng and X. Huang (2014). “The research of smart home robots based on 3g mobile network”. *Applied Mechanics and Materials*, 631, 184–187.
- [28] P. Benavidez, M. Kumar, S. Agaian, and M. Jamshidi (2015). “Design of a home multi-robot system for the elderly and disabled”, in *2015 10th System of Systems Engineering Conference (SoSE)*. IEEE, pp. 392–397.
- [29] K. Chiu, C. Lai, and H. Chu (2020). “Apply importance performance analysis to explore innovation resistance of home robot”, *International Journal of Mechanical Engineering and Robotics Research*, 9: 5, 716–720.
- [30] M. Luperto, J. Monroy, J. Renoux, F. Lunardini, N. Basilico, M. Bulgheroni, A. Cangelosi, M. Cesari, M. Cid, A. Ianes, and J. Gonzalez-Jimenez (2022). “Correction to: Integrating social assistive robots, IoT, virtual communities and smart objects to assist at-home independently living elders: the movecare project”. *International Journal of Social Robotics*, 14: 9, 2045.

- [31] C.-W. Chen, S.-P. Tseng, Y.-T. Hsu, and J.-F. Wang (2017). “Design and implementation of human following for separable omnidirectional mobile system of smart home robot”, in *2017 International Conference on Orange Technologies (ICOT)*. IEEE, pp. 210–213.
- [32] T.-H. Yang and W.-P. Lee (2016). “Intelligent service reconfiguration for home robots”, in *Advances in Recon-figurible Mechanisms and Robots II*. Springer, pp. 735–745.
- [33] D. Butler *et al.* (2015). “The privacy-utility tradeoff for remotely teleoperated robots”, in *ACM/IEEE International Conference on Human-Robot Interaction*.
- [34] L. Urquhart, D. Reedman-Flint, and N. Leesakul (2019). “Responsible domestic robotics: exploring ethical implications of robots in the home”. *Journal of Information, Communication and Ethics in Society*, 17: 2, 246–272.
- [35] G. Várkonyi (2020). “Application of the general data protection regulation on household social robots”. Ph.D. dissertation, Szegedi Tudományegyetem (Hungary).
- [36] M. Shinohara, D. Sakamoto, T. Ono, and J. E. Young (2023, December). “Understanding privacy-friendly design of robot eyes”, in *Proceedings of the 11th International Conference on Human-Agent Interaction*, pp. 133–141.
- [37] I. Lee (2021). “Service robots: A systematic literature review”. *Electronics*, 10: 21, 2658.
- [38] S. Balali *et al.* (2019). *Privacy Concerns in Robot Teleoperation: Does Personality Influence What Should Be Hidden?* Springer International Publishing, 2019, reference 43.
- [39] K. Ishii (2019). “Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects”. *AI & Society*, 34, 509–533.
- [40] J. Guiochet, M. Machin, and H. Waeselynck (2017). “Safety-critical advanced robots: A survey”. *Robotics and Autonomous Systems*, 94, 43–52.
- [41] A. Zacharaki, I. Kostavelis, A. Gasteratos, and I. Dokas (2020). “Safety bounds in human robot interaction: A survey”. *Safety Science*, 127, 104667.
- [42] *Robots and robotic devices – Vocabulary*, <https://www.iso.org/standard/55890.html>, Std. ISO 8373:2012 (2012).
- [43] M. A. Olivares-Mendez, P. Esteves-Verissimo, M. Völz, and H. Voos (2017). “A perspective of security for mobile service robots”, in *ROBOT 2017: Third Iberian Robotics Conference: Volume I*, vol. 693. Springer, p. 88.
- [44] W. Dudek, W. Szykiewicz, and I. Technology (2019). “Cyber-security for mobile service robots—challenges for cyber-physical system safety”. *Journal of Telecommunications and Information Technology*, reference 48.
- [45] K. M. Ahmad Yousef, A. AlMajali, S. A. Ghalyon, W. Dweik, and B. J. Mohd (2018). “Analyzing cyber-physical threats on robotic platforms”. *Sensors*, 18: 5, 1643.
- [46] V. Matellán, T. Bonaci, and G. Sabaliauskaite (2018). *Cyber-security in Robotics and Autonomous Systems*. Elsevier, reference number 50.
- [47] R. Kumar, P. Pattnaik, and P. Pandey (2017). *Detecting and Mitigating Robotic Cyber Security Risks*. IGI Global, reference number 51.
- [48] A. Chowdhury, G. Karmakar, and J. Kamruzzaman (2017). “Survey of recent cyber security attacks on robotic systems and their mitigation approaches”, in *Detecting and Mitigating Robotic Cyber Security Risks*. IGI Global, pp. 284–299.
- [49] A. Botta, S. Rotbei, S. Zinno, and G. Ventre (2023). “Cyber security of robots: A comprehensive survey”. *Intelligent Systems with Applications*, 18, p. 200237.
- [50] V. Mayoral-Vilches (2022). “Robot cybersecurity: A review”. *International Journal of Cyber Forensics and Advanced Threat Investigations*, Jan 2022.
- [51] S. Neupane, S. Mitra, I. A. Fernandez, S. Saha, S. Mittal, J. Chen, N. Pillai, and S. Rahimi (2024). “Security considerations in AI-robotics: A survey of current methods, challenges, and opportunities”. *IEEE Access*, Feb 2024.
- [52] E. Bou-Harb (2016). *A Brief Survey of Security Approaches For Cyber-Physical Systems*. New York: IEEE, reference number 69.
- [53] L. Cao *et al.* (2020). “A survey of network attacks on cyber-physical systems”. *IEEE Access*, 8, 44219–44227, reference number 70.
- [54] A. Humayed *et al.* (2017). “Cyber-physical systems security—a survey”. *IEEE Internet of Things Journal*, 4: 6, pp. 1802–1831, reference number 71.

- [55] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli (2020). “Cyber-physical systems security: Limitations, issues and future trends”. *Microprocessors and Microsystems*, 77, 103201.
- [56] A. A. Nazarenko and G. A. Safdar (2019). “Survey on security and privacy issues in cyber physical systems”. *AIMS Electronics and Electrical Engineering*, 3: 2, 111–143.
- [57] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park (2018). “A survey on cyber physical system security for IoT: issues, challenges, threats, solutions”. *Journal of Information Processing Systems*, 14: 6, 1361–1384.
- [58] F. Khalid, S. Rehman, and M. Shafique (2020). “Overview of security for smart cyber-physical systems”, in *Security of Cyber-Physical Systems*. Springer, pp. 5–24, reference number 74.
- [59] Y. Ashibani and Q. H. Mahmoud (2017). “Cyber physical systems security: Analysis, challenges and solutions”. *Computers & Security*, 68, 81–97.
- [60] J. Li *et al.* (2020). “Adversarial attacks and defenses on cyber-physical systems: A survey”. *IEEE Internet of Things Journal*, 7: 6, 5103–5115, reference number 76.
- [61] I. Ahmad, M. Zarrar, T. Saeed, and S. Rehman (2018). “Security aspects of cyber physical systems”, in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, pp. 1–6.
- [62] Z. Wang, W. Xie, B. Wang, J. Tao, and E. Wang (2021). “A survey on recent advanced research of cps security”. *Applied Sciences*, 11: 9, 3751.
- [63] C. Kumar, S. Marston, and R. Sen (2020). “Cyber-physical systems (cps) security: State of the art and research opportunities for information systems academics”. *Communications of the Association for Information Systems*, 47: 1, 36.
- [64] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal (2021). “Smart home security: Challenges, issues and solutions at different IoT layers”. *The Journal of Supercomputing*, 77: 12, 14053–14089.
- [65] M. Kuyucu, Ş. Bahtiyar, and G. İnce (2019). “Security and privacy in the smart home: A survey of issues and mitigation strategies”, in *2019 4th International Conference on Computer Science and Engineering (UBMK)*. IEEE, pp. 113–118.
- [66] M. Khawla and M. Tomader (2018). “A survey on the security of smart homes: issues and solutions”, in *Proceedings of the 2nd International Conference on Smart Digital Environment*, pp. 81–87.
- [67] Y. Meng *et al.* (2018). “Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures”. *IEEE Wireless Communications*, 25: 6, 53–59, reference number 101.
- [68] X. Feng, Y. Wang, L. Jiang, Y. Huang, and T. Li (2018). “A survey on internet of things security based on smart home”, in *2018 5th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*. IEEE, pp. 84–91.
- [69] A. J. Barriga and S. Yoo (2018). “Security over smart home automation systems: A survey”, in *International Conference of Research Applied to Defense and Security*. Cham: Springer International Publishing, pp. 87–96.
- [70] J. Yang and L. Sun (2022). “A comprehensive survey of security issues of smart home system: “spear” and “shields,” theory and practice”. *IEEE Access*, 10, 124167–124192.