SpringerLink

[**Published: 19 March 2021**](https://link.springer.com/article/10.1007/s10207-021-00545-8#article-info)

***I***[***nternational Journal of Information Security***](https://link.springer.com/journal/10207)***(2021)***

**Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations**

**Abstract**

**The recent digital revolution led robots to become integrated more than ever into different domains such as agricultural, medical, industrial, military, police (law enforcement), and logistics.**

**Robots are devoted to serve, facilitate, and enhance the human life. However, many incidents have been occurring, leading to serious injuries and devastating impacts such as the unnecessary loss of human lives. Unintended accidents will always take place, but the ones caused by malicious attacks represent a very challenging issue. This includes maliciously hijacking and controlling robots and causing serious economic and financial losses.**

**This paper reviews the main security vulnerabilities, threats, risks, and their impacts, and the main security attacks within the robotics domain.**

**In this context, different approaches and recommendations are presented in order to enhance and improve the security level of robotic systems such as multi-factor device/user authentication schemes, in addition to multi-factor cryptographic algorithms. We also review the recently presented security solutions for robotic systems.**

**Introduction**

**With the latest digital revolution and the heavy reliance on Artificial Intelligence (AI), smart robots are being employed to speed up the transformation of digital operations. In this context, the market of intelligent machines, including autonomous robots, is exponentially growing; more than 40 million robots were reportedly sold between 2016 and 2019. Robotics is one of those technologies that are witnessing tremendous expansion and growth especially with the rise of the ongoing COVID-19 pandemic. Moreover, its emergence into the Internet of Things (IoT) domain led it to be called the Internet of Robotic Things. In fact, robots play a crucial role in modern societies, offering various opportunities to help in various domains, including civilian and military sectors, as well as agricultural, industrial, and medical ones. However, there are several concerns related to robots’ deployment in critical infrastructures (e.g. industrial, medical, etc.). These concerns are mainly related to security, safety, accuracy and trust. Security is primarily related to the level of protection of these robots against different types of cyber-attacks. Safety is related to the reduction of the likelihood of accidents’ occurrence(s), accuracy is based on performing the intended task without any faults/mistakes, while trust is based on the level of satisfaction and capability of these robots to accurately perform and replace humans in certain fields and activities. However, various security concerns, issues, vulnerabilities, and threats are constantly arising, including the malicious misuse of these robots via cyber-attacks, which may result in serious injuries and even death.**

**Motivation**

**Robots are being adopted in various sectors such as agriculture (crop monitoring and watering), industry (building and construction), military (combat and logistics), disaster relief (search and rescue), and health care (remote surgeries, remote deliveries, anti-COVID-19 use, etc.). However, recent robotic-related incidents and misuses gained the media’s attention, where casualties or/and fatalities cases were reported in incidents related to terrorism/cyber-terrorism, sabotage, and espionage. Therefore, this paper discusses why robot manufacturers must consider safety, security, and accuracy in their initial design, and it highlights the recent efforts and robotic-based solutions to overcome and reduce the impact and spread of COVID-19, with lessons learnt to overcome any possible future pandemic spread.**

**Therefore, this paper highlights the main robotic domains of use, fields of operation, and application fields. In addition, this paper surveys the main security threats and vulnerabilities that surround the robotic domain while presenting a variety of suitable solutions to mitigate them. In fact, a risk assessment is also presented in a qualitative manner based on the risk level and occurrence, and presenting their most suitable solutions. This paper also presents the main applications of robotics in the global fight against the ongoing COVID-19 pandemic, especially with the use of Artificial Intelligence (AI) and Machine Learning (ML) solutions, while highlighting additional robotic technologies, and the importance of their applications in tele-medicine and virtual clinics/care domains. In summary, this work aims to summarize the existing solutions that only focus on a single security aspect, with no clear security and safety recommendations being made with respect to designing secure and safe robotic systems. As such, the objective is to ensure that future security solutions strike a good balance between robots’ performance and their corresponding security and safety levels. Moreover, several recommendations were presented for the design of secure robotic systems in addition to identifying a set of possible research directions within the robotic security domain.**

**Objectives and contributions**

**The objective of this paper is to highlight the importance of adopting the various robotic techniques (i.e. drones, robots, AI, etc.) in every aspect of both the cyber and physical worlds. Also, the paper emphasizes that the robotic domain suffers from a set of security and safety threats that can lead to dangerous attacks. In this context, we review the robotics security threats, vulnerabilities, and attacks, in addition to providing a qualitative risk assessment for these attacks. Equally important, we present a set of possible solutions to overcome these attacks.**

**Moreover, the robustness and efficiency of these solutions are analyzed, and we suggest several recommendations to increase the security level of robotic systems. In summary, this paper provides a global review about the robotic security, which is not well presented in the literature.**

**The main contributions of this paper can be summarized as follows:**

**1.**

**We illustrate the multi-purpose use of robots in various domains, to set the stage for the understanding and evaluation of robotic security attacks and their impacts.**

**2.**

**We highlight the different security vulnerabilities, risks, types of attacks, and their sources.**

**3.**

**We present a new taxonomy of how attacks take place, along with their impact, nature, structure, and concerns.**

**4.**

**We propose a list of recommendations and security requirements to safeguard robots against such attacks, to minimize their damage, and hence, to make the corresponding applications safer to deploy and use.**