International Journal of Information Security (2022) 21:115–158
https://doi.org/10.1007/s10207-021-00545-8

REGULAR CONTRIBUTION

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

Jean-Paul A. Yaacoub[1] · Hassan N. Noura[2] · Ola Salman[1] · Ali Chehab[1]

Published online: 19 March 2021

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.

Keywords Robotics · Security systems · Security attacks · Countermeasures · Risk analysis · Counter-terrorism/insurgency · Robotics against COVID-19

1 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 [1,2]. In this context, the market of intelligent machines, including autonomous robots, is exponentially growing [3]; more than 40 million robots were reportedly sold between 2016 and 2019 [4].

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 [5]. 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 [6]. 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 [7,8].

1.1 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

✉ Ola Salman
oms15@mail.aub.edu

[1] Department of Electrical and Computer Engineering, American University of Beirut, Beirut 1107 2020, Lebanon

[2] FEMTO-ST Institute, Univ. Bourgogne Franche-Comté (UBFC), Besançon, France

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.

1.2 Related work

According to [9], various robotic challenges were discussed, out of which, security was considered among the hardest ones. Advanced robot systems became more prone to a variety of cyber-attacks [10–12] that target their data or (operating) systems' confidentiality, integrity, availability, authentication, and/or privacy [13,14]. The main security threats and vulnerabilities targeting robotic systems were described in [15,16]. Furthermore, a set of known robotic cyber-attacks were presented in [17] and various efforts were combined to reduce the exposure of the Robot Operating System (ROS) to various security vulnerabilities, as indicated in [18]. Moreover, a set of energy-efficient security mechanisms were presented in [19]. In [20], Guiochet et al. investigated the safety of applications based on robots-humans interaction . In [21], Dieber et al. evaluated the security of ROS by applying penetration tests while presenting countermeasures to harden its security. A recent work [22,23] listed the current cyber-defence trends in industrial control systems. In addition, in [24], Jahan et al. reviewed the secure modelling of autonomous systems including robotic ones.

Unfortunately, the related work lacks a global understanding of the robotics security issues and their causes. Moreover, no recommendations have been made in regards of designing secure robotic systems.

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 [25], while highlighting additional robotic technologies [26–28], and the importance of their applications in tele-medicine and virtual clinics/care domains [29]. 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.

1.3 Objectives and contributions

The objective of this paper is to highlight the importance of adopting the various robotic techniques (i.e. drones, robots, underwater vehicles, 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 analysed, 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.

1.4 Organization

This paper consists of eight sections and is organized as follows: Sect. 2 reviews the use of robots in multiple domains. Section 3 highlights the robotics issues and challenges, including the main security threats, risks, and vulnerabilities. Section 4 classifies the main robotic cyber-attacks according to different layers such as physical and network layers, where the main security and safety concerns are discussed, with a qualitative risk assessment being proposed. In Sect. 5.1, the robotic cyber-threat intelligence is presented

along its advantages, while also highlighting three active responses including active security awareness, response, and management. In Sect. 5, different effective security countermeasures are discussed to ensure protection for robotic systems' layers. The authentication, identification and verification processes are also discussed, along with the need for effective multi-factor authentication techniques to restrict access to authorized privileged robots/users only. In Sect. 6, we present the main security requirements and recommendations for future research directions over the security aspect in the robotics domains. Section 7 concludes the paper.

2 Robot application domains

Robots have been deployed in different domains and employed in different fields, including civilian and military ones, which are summarized in Fig. 1. The figure illustrates the various robotic usages in different fields of operations for many tasks and purposes such as photography, product delivery, agriculture, wildlife monitoring, policing, search and rescue, emergency response, crisis/disaster response, casualty evacuation, reconnaissance and surveillance, counter-terrorism/insurgency, counter-IEDs/unexploded ordnance, border patrol, infrastructure inspections, and science. There are different types of robots depending on their field of operation: Unmanned Aerial Vehicles (UAVs) such as drones, Autonomous Unmanned Aircraft Vehicles (AUAVs), Unmanned Aerial Combat Vehicles (UACVs) and Unmanned Aircraft Systems (UASs) [30,31], Unmanned Ground Vehicles (UGVs) such as robots and autonomous vehicles [32], and Unmanned Underwater Vehicles (UUVs) such as underwater drones, Autonomous Surface Vehicle (ASV), Remotely Operated Underwater Vehicles (ROUVs) and Autonomous Underwater Vehicles (AUVs) [33,34].

This section discusses the main use of robots in industrial [35,36], medical [37], disaster and agriculture fields, in addition to police and military ones [30].

2.1 Industrial field

Industrial robots are mainly used in order to reduce manpower. Robots have become artificially smart and able to perform jobs faster, safer, and with higher efficiency [38]. Such jobs include manufacturing, construction, transportation, and quality control. In particular, robots are being used in hazardous locations to perform dangerous tasks. They are also capable of performing repetitive tasks with the same precision and accuracy, better than their human counterparts.

2.2 Medical field

Robots have been deployed in the medical domain to be used in tele-medicine, virtual care, and remote treatment concepts [29,39]. In fact, they were designed to serve as medical robots, surgical robots, and hospital robots [40]. They are used to perform small surgeries accurately, and new medical robots are capable of performing Cardio-Pulmonary Resuscitation (CPR) [41].

2.3 Agriculture field

Robots are used in agriculture due to their efficient and increased performance in reducing manpower and resource consumption [42]. They are used to perform some tasks efficiently, especially when dealing with a large farming area that requires at least a dozen of workers and several days. This enhances irrigation, crop testing, crop agriculture, and so on.

2.4 Disaster field

Disaster robots can be used to reach and find helpless people who were isolated by floods, or stuck and lost somewhere [43,44]. Disaster robots can perform jobs and reach places that humans cannot [45]. Their famous use was when Search and Rescue (SAR) robots were deployed to locate and find lost Thai cave boys safely [46]. Moreover, robots were used in the firefighting domain [47,48], which helps in sparing the lives of firefighters and to access areas that are deemed too dangerous, too small, and/or too risky for firefighters. In fact, both robots and UAVs were used after the devastating Beirut port explosion that occurred at around 6:07 pm on August 4th, 2020, to help with assessing the damage and impact radius, as well as in the search for missing personnel [49–52]. The explosion was caused by the alleged detonation of 2750 tonnes of Ammonium Nitrate due to lack of proper storage, equivalent to 1.1 kilotons of TriNitroToluene (TNT), and is considered as one of the most powerful non-nuclear explosions in history.

2.5 Police and law enforcement field

Robots are being deployed in various police fields, especially when it comes to shooting down, neutralizing, or eliminating suspects in places that are considered too dangerous and that could lead to the loss of valuable officers' lives. A well-known use case of this application is when the police used a robot strapped with a C4 explosive and detonated it in order to kill the Dallas shooter [53]. In fact, the Israeli police is known to have used drones (i.e. spiderman urban assault drone), with others equipped with tear gas to counter the Gaza protests and to reduce the threat imposed by possibly armed infil-

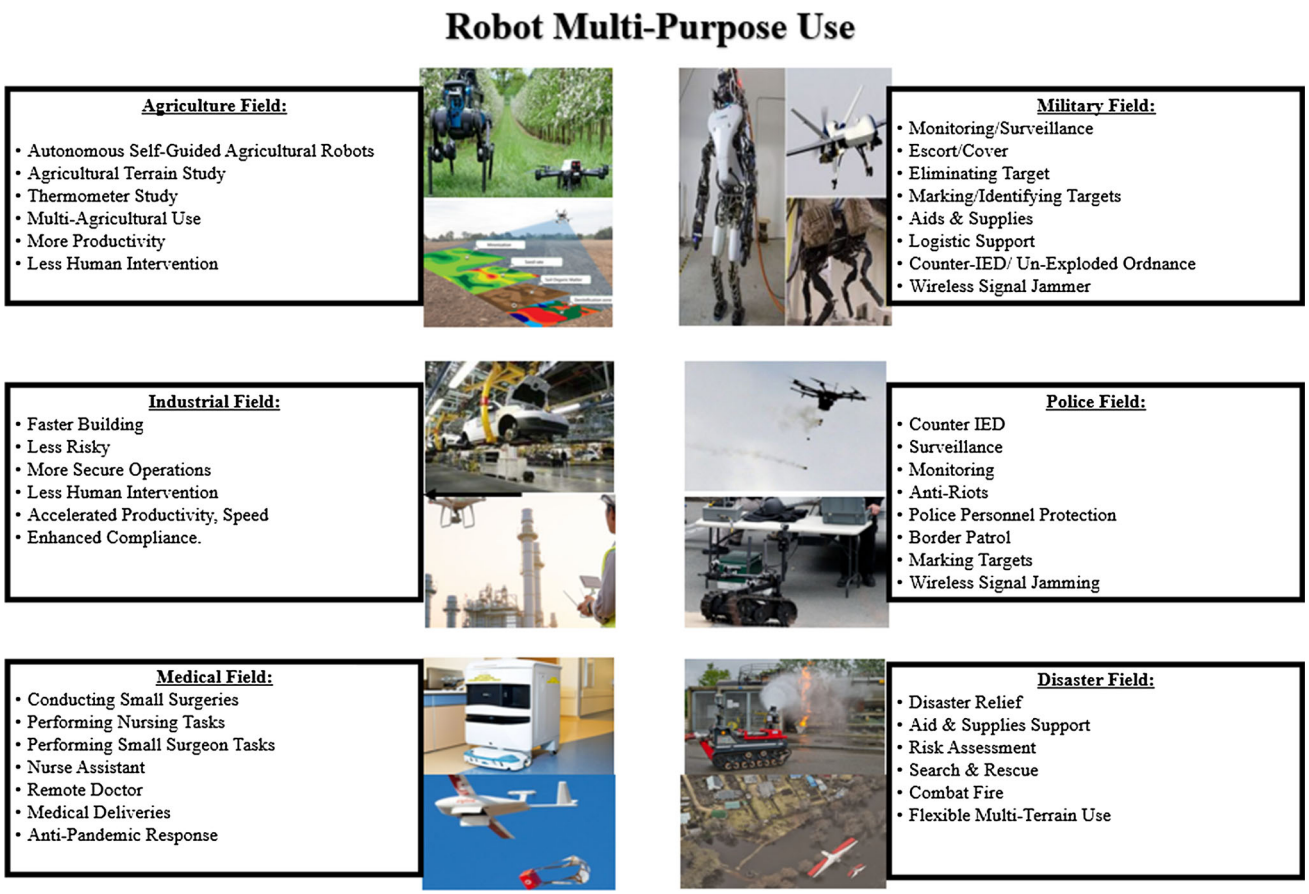

Fig. 1 Robot's use in certain fields

trators [54,55] and burning/armed explosive incendiary kites and balloons [56]. Indian, South African, and Dutch police are also known to have used "Skunk" drones which are armed and equipped with pepper spray. The American police and law enforcement are also using "weaponized drones" armed with tasers, tear gas, and rubber bullets [57].

2.6 Military field

Military robots became the latest adopted weapons to be used in most of military operations, especially with the extensive use of Unmanned Aerial Vehicles (UAVs) to perform target detection and to launch airstrikes [58]. Moreover, robots were used to counter the Improvized Explosive Device (IED) threat, especially in Iraq and Afghanistan [59]. In fact, they were being used by the British army in Northern Ireland since 1970s [60], to combat the IEDs threat imposed by the Irish Republican Army (IRA) and its different factions and descendants [61–63]. Such robot techniques (Unmanned Ground Vehicles (UGVs) and Unmanned Aerial Vehicles (UAVs)) evolved and were also used by US-led NATO forces (including the UK) in Iraq and Syria [64,65], in Yemen, Afghanistan, and Pakistan [66–69]. Also, France used them in Mali, Somalia, and Nigeria [70,71] against the Islamic State (ISIS/ISIL) and Al-Qaeda operatives, and other terrorist factions (i.e. Boko Haram, Al-Shabab). Turkey also used mainly combat drones (i.e. Bayraktar TB2), and UGV robots (TMR 2 (Kutlu), Zafer (Victory) and KAPLAN) in its campaign in Libya (along the United Arab Emirates who used Chinese-made UCAVs: Wing Loong II [72]) against Haftar forces, and in Syria against Syrian troops, Kurdish factions and Hezbollah members [73,74]. Turkey also assisted Azerbaijan (using loitering munition such as Alpagu and Kargu, and UCAVs such as Bayraktar TB2) with help from Israel (using loitering munition such as Orbiter, Heron and Harop variants, and LORA missiles) [75,76] during the Nagorno-Karabakh conflict [77] against Armenia. Russia also reportedly used drones and UGVs in its conflict in Syria, Libya, and Ukraine [64,78,79]. Iran developed its own UGVs and UAVs, with many UAV variants being used in Yemen, Lebanon, Iraq, Syria, and Gaza (Shahed, Ababil, Ayoub, Samad, Mohajer, Karrar, Mirsad, Qasef, etc.) via its operators [80], advisers [81–83] and proxies (i.e. Houthis, Hamas, Hezbolah, Palestinian Islamic Jihad (PIJ)) [84–86]. However, Israel extensively relied on developing Anti-UAV/UGV countermeasures (i.e. Iron Dome patriot missiles, AI-based sensors,

facial-recognition and heat-measuring cameras, jammers, laser-guided weapons, etc.), and introduced its own advanced version of UAV and UGV variants to combat the threatening Iranian presence in Syria (Unit 840, trans-border operations near Golan Heights), Southern Lebanon (Hezbollah tunnels and cross-border operations) [87–89], the West Bank and Gaza Strip [Hamas Group 9 specializing in tunnel warfare, cross-border operations (Nahal Oz tunnel attack, 2014 [90]), and Naval Commando Unit specializing in underwater tunnel capabilities, and underwater naval operations (Zikim Beach Landing, 2014)] [91–93]. Finally, armed drone swarms or Uninhabited Air Vehicles (UiAVs) may well be used by the UK next summer in 2021.

Robots were also used in the precision-guided munitions, precision-guided fragmentation munitions, precision-guided airstrikes and shelling, smart bombs and Satellite Navigation (SATNAV) munition [94–96]. Moreover, robotics became included in the naval warfare domain as part of autonomous boats, ships, submarines, torpedoes and as part of Naval Mine Counter-Measures (NMCM), passive Anti-Submarine Warfare (ASW) [97–99], anti-piracy operations (i.e. Somalian coasts, Nigeria's Niger Delta, Gulf of Guinea, Gulf of Aden [100,101], and Guardafui Channel) and countering-terrorism, relying on the Combined Task Force 150 (CTF-150 stationed in Bahrain) and the establishment of the Maritime Security Patrol Area (MSPA)) [102–104].

In fact, the robotic technology was not excluded from being adopted and used by both terrorists and insurgents alike. Robotics including tele-operated sniper rifles, assault rifles and machine guns, as well as remote-controlled autonomous vehicles and unmanned ground vehicles mounted with heavy machines guns were extensively used in conflicts such as in Syria, Iraq, and Libya by different fighting factions and insurgent groups (i.e. ISIS/ISIL, Al-Nusra, Al-Qaeda and Anti-Guaddafi forces) [105–107], in addition to the extensive use of drones and UAVs [108–110], and ISIS developed their own techniques [111–114].

2.7 Counter-pandemic field

During the ongoing COVID-19 pandemic caused by the SARS-CoV-2 virus [25], which started its outbreak in late 2019, the extensive use of robots, drones, UAVs, autonomous and unmanned vehicles grew fast, along the adoption of AI and ML techniques to ensure a faster detection of infected personnel and to limit the outbreak and infection rates [115]. In May 2020, a drone representing the "Anti-COVID-19 Volunteer Drone Task Force" was urging New-Yorkers to wear their masks and maintain their social distancing, and respect quarantine rules [116,117]. In France, "Big Brother" drones were used to enforce social distancing before being banned in May 2020 [118]. Other European countries also included the use of drones and robots such as Finland, Russia, UK, Germany, Belgium, Italy, Spain, Portugal, and Greece. Other countries were also reported to adapt a similar technique including Turkey, Hong Kong, China (Wuhan), South Korea, Japan, India (using Mitra medical robot), Singapore, Australia, and New Zealand to monitor cases and maintain medical supply tests, labs and deliveries, aerial spray and disinfection, as well as consumers delivery [116,119]. Moreover, there was a remarkably extensive use and reliance on AI tools by Middle Eastern and North African countries such as Tunisia (using P-Guards or Robocop), Morocco, Bahrain, Saudi Arabia, Egypt, Qatar, Oman, Kuwait, the United Arab Emirates (i.e. Dubai), Lebanon and Israel including speed cameras, drones and robots to enforce quarantine rules, perform deliveries, and maintain social distancing [120–122], aside using police/military patrols and helicopters with speakers. In fact, drones were also used to monitor cases and ensure medical deliveries and testing samples to limit the COVID-19 outbreak in Africa [123]. Medical surgeries and operations were also carried out by robots including humanoids to reduce the exposure of medical staff that was already stressed out due to high COVID-19 cases [124,125]. Thus, this paves the way to futuristic robotics-assisted telemedicine and telehealth applications, based on the lessons learnt and to-be-learnt, during the Ebola outbreak and the ongoing COVID-19 pandemic, such as the smart field hospital trial in Wuhan, China, and the use of smart medical "Xiao Bao" robot [126], as well as the use of "companion robots" to combat loneliness [127]. This will help in remotely examining and monitoring infected patients, controlling the outbreak, minimizing the exposure, disinfecting areas, delivering medicines and food, raising awareness, and measuring vital signs for early detection.

3 Robotics security: issues, vulnerabilities, threats, and risks

Despite the great advantages and promising future the robotic field holds, some major concerns are still lurking around, and imposing serious threats and issues [128] that can potentially affect both humans and machines. For this reason, these main issues and challenges are presented in this section.

3.1 Security issues

Robotic issues are not limited to one, but to many aspects that could exploit any vulnerability/security gap to target robotic systems and applications alike [10,10,129]. The aim is to identify and classify them to gain a better insight, which helps other fellow researchers in their quest to identify, tackle and overcome them.

- *Lack of secure networking* which renders the communication between robots/machines and humans insecure and prone to various attacks [130,131].
- *Lack of proper authentication* which leads to an unauthorized access using standard usernames and passwords, which can be easily trespassed by a given attacker.
- *Lack of confidentiality* which is due to the use of weak encryption algorithms that can be easily broken, leading to the interception and exposure of robotic sensitive data and design plans.
- *Lack of privacy* can result in the exposure of business deals and trades that can affect the reputation of a given organization, and the exposure of the collaboration between different robotic security firms.
- *Lack of integrity* which is due to the use of weak message authentication protocols that can be easily compromised, leading to the alteration of robotic sensitive data, stored or in transit.
- *Lack of verification* which does not include strong biometric features to prevent any abuse of privilege or unauthorized access.
- *Lack of authorization* it defines the right physical access based on the assigned access controls inside robotic labs, factories, and industries [10].
- *Misconfiguration and bad programming* which may render the robotic systems and operating systems incapable of performing the intended tasks at the required accuracy level, and thus, threatening their human operators and badly affecting the software features.
- *Lack of tamper-resistant hardware* renders robots prone to damage and/or partial/total destruction, which can lead to the loss of the robot's functional and operational capabilities.
- *Lack of self-healing processing* leaves the robotic system prone to the possibly of cascading attacks with the inability to recover or react in time to prevent further degradation in its performance. Hence, a self-healing process is required to ensure that robotic systems can sense faults or disruptions and can reconfigure the back-up resources.
- *Lack of safety designs* is very risky and has proven in many real-case incidents to be lethal and threatening towards humans with a remarkable number of casualties and fatalities, aside the economic/financial losses.
- *Lack of security by-design features* leads to breaking into the robotic system's architecture and design to scan and exploit its vulnerability/security gap(s) for further attacks, including malicious data injection and modification [10].
- *Lack of AI-based designs* affects the operational and functional performance of robots when being assigned a task, with both accuracy and performance being affected.
- *Lack of update* for the robotic operating system, firmware, and software may result in various cyber-physical attacks.
- *Lack of advanced IDS solutions* is also a major issue, especially when relying on intrusion detection system that either detect anomaly, behaviour or signature pattern of a given malware, rather than relying on advanced hybrid and lightweight or AI-based IDS solutions. The same is true for the use of Honeypots.
- *Lack of penetration testing* could lead to security breaches of the deployed applications.
- *Lack of security patches* increases the chance of basic and advanced attacks such as stealing of sensitive data, remote access, and rootkit.
- *Lack of personnel training* is also a serious issue since personnel working in the coding robotic domain, or as human operators, or as IT or chief executives, are targeted by social engineering, reverse engineering and phishing attacks.
- *Lack of human–machine collaboration* could affect the human activity in terms of labour, work, and performance.
- *Lack of employee screening* could result in having an insider attack led by a whistle-blower that leaks sensitive data and exposes classified information and sensitive robotic details.

3.2 Security vulnerabilities

Robotic systems are prone to various vulnerabilities [132, 133] that can affect their performance in terms of connectivity, productivity, operations, and accuracy. This paper presents several vulnerabilities that are challenging:

- *Network vulnerability* with the lack or the adoption of basic security measures, robotic systems are vulnerable to various wired/wireless communication and connections attacks including replay, man-in-the-middle, eavesdropping, sniffing, spoofing, etc.
- *Platform vulnerability* includes the lack of constant updates of software and firmware patches, as well as security patches to maintain a secure up-to-date robotic system. This results into also having configuration and database vulnerabilities.
- *Application vulnerability* applications that are not tested and evaluated for coding or compatibility bugs, can also affect the robotic system's performance. Hence, further testing is essentially required.
- *Security vulnerability* the adoption of new security measures without thorough testing can sometimes affect the performance of both robotic systems and devices. Hence, testing is essential before deployment.
- *Bad practice vulnerability* includes the bad choice of security measures and means, as well as lack of coding

skills, which can be easily re-modified to cause errors or to perform the wrong tasks.
- *Update vulnerability* robots are also prone to update vulnerabilities that can cause their systems and operating systems to act differently due to the new update, including the loss of unsaved data, interruption of the ongoing process, etc.
- *Heterogeneity and homogeneity vulnerability* the heterogeneous nature of robotic systems makes their integration prone to many security issues. Moreover, their homogeneous nature also leaves them prone to similar attacks with possibly cascading effects.
- *Management vulnerability* includes the lack of advised planning, security guidelines, procedures and policies.

3.3 Security threats

Robotics threats are growing, not only due to the concept of industrial competition, but also due spying and terrorism.

3.3.1 Threat source

Threats can originate from different sources [134], and can be part of cyber-crimes, cyber-warfare, cyber-espionage, or even cyber-terrorism. This paper lists the main ones as follows:

- *Insiders (or whistle-blowers)* are usually rogue or unsatisfied employees who aim to either steal robotic confidential information, or infiltrators that help outsiders to conduct their attack remotely through abuse of privilege. Insiders can also cause physical damage and destruction to robotic systems.
- *Outsiders* aim to gain access to a robotic system through the Internet. The external adversary's aim is to get access to information for malicious purposes [134], to cause malfunction or/and disrupt the system's services through the injection of either fake or malicious data.
- *Competitors* usually, rivals in the robotic industry aim to maintain a leading edge in this domain. Many methods can be adopted such as the reliance on insiders, or part of industrial espionage to leak confidential documents and damage the rival company's reputation [135].
- *Incompetent developers* include bad manufacturers and programmers who do not take into consideration the essential safety and security requirements upon the development of software for robots and machines.
- *Incompetent operators* include either ignorant users who do not know how to use well a robot or a machine, or malicious users who try to use the robot/machine for a malicious task.
- *Cyber criminals* including hackers whose aim is put their cyber-attack capabilities into action via scanning for security gaps or software/firmware vulnerability and exploiting them.
- *Organized criminals* unlike cyber criminals, they break into a given company and steal robotic components, parts, designs, or architecture plan in order to sell it into the black market to rival companies, or for their own personal gains.
- *Malicious manufacturers* leave, on purpose, a backdoor into the robotic system to track and monitor the activities of the robot and its operator without the owner's knowledge. Also, they can gather sensitive and confidential information about the user's device through key logging and root-kits. In fact, many manufacturers leave on purpose a design flaw or a misconfiguration as a backdoor in order to exploit it or to get quick access to the robotic system.
- *State-sponsored hackers* are usually recruited as a nation's cyber-army to perform defensive and offensive tasks to achieve political influence and gain. This can include hijacking military robots, leaking sensitive and confidential documents about lethal robot designs, or declassifying robotic documents and experiments.
- *Terrorists* also rely, in this domain, in the physical and cyber-world. Terrorists use robots and drones in their paramilitary operations. Also, cyber-terrorism is growing to retrieve details and gain insights about robotic systems to build their own versions.
- *Spies* are constantly being used to conduct (cyber) espionage and sabotage operations, typically between rival countries such as Iranian-Israeli cold cyber-war, which reached its height in May 2020, including cyber-attacks and sabotage operations [136–138]. A prime example is the "QuickSand" operation led by Iran's "MuddyWater" and Cyber "Avengers" that are linked to the Islamic Revolutionary Guard Corps (IRGC) targeting Israel's industrial infrastructure, followed by a series of ongoing Israeli counter-cyber-offensives, which reached their height in June, targeting Iran's infrastructure ports, electricity firms, covert nuclear labs, etc. In fact, the Iranian cyber-threat is growing with many Advanced Persistent Threat (APT) actors attacking Western targets such as: APT33 targeting aerospace and (petrochemical) energy, APT34 involving a long-term cyber espionage operation targeting financial, government, energy, chemical firms, APT35 (or Newscaster Team) targeting military, governmental, media and engineering firms, and APT39 targeting telecommunications sector and high-tech industry.

3.3.2 Threat nature

Despite the already listed issues, there are various threats [139] targeting Industrial IoT systems [23] that need to be

addressed before diving further into the security aspect of the robotic domain. These main threats are classified as follows:

- *Wireless jamming* robotic communications are prone to various availability attacks that can jam, disrupt or/and interrupt its connection via either de-authentication or jamming. This leads to the complete or partial loss of controlling the robot
- *Reconnaissance and scanning* robotic systems are also prone to various reconnaissance and scanning attacks that aim to evaluate their level of protection, the employed software, hardware, and operating systems, to search for a security vulnerability or gap that may be exploited in future attacks.
- *Information disclosure* can take place either via physical leaking of confidential documents, or remotely via a cyber-attack. Targeting both privacy and confidentiality of robotic manufacturers, businesses and industries.
- *Abuse of privilege* still remains a threat in the robotic domain whereby unauthorized users trespass physical and logical access controls to gain an unauthorized access or perform unauthorized tasks.
- *Information gathering* remains an essential threat, especially with personnel working in the robotic domain (operators, manufacturers, IT security, Chief Robotics Officers (CROs), etc.) lacking the right security training to overcome phishing and social engineering attempts.
- *Information interception* operating on different high frequencies allows manufacturers to communicate without interference. However, the lack of security protection and encryption over these channels leave them prone to various interception and delay attacks, which can result in a total breach of privacy, confidentiality and integrity.
- *Information modification* is a common threat that targets the AI aspect of robotics, with malicious modifications affecting the ability of AI to distinguish between pictures, for example, the accuracy of performing the intended tasks.
- *Physical damage* robots are also prone to physical damage, attack and theft by insiders (rogue employees) and intruders. This is mainly due to the lack of available security checks and tamper-resistant equipment.
- *Service disruption or denial* can be caused either by an employee's mistake or by malicious users who inject malicious data affecting the accuracy and performance of robotic systems, or via launching a (distributed) denial of service attack.
- *Sabotage and espionage* robotic systems are typically prone to industrial espionage operations, which can be further extended to become a sabotage operation resulting into hijacking, destroying or severely crippling the ability of robotic systems to properly perform their intended task(s) [140,141]. This can also be classified as an act of terrorism [142].
- *Tracking and monitoring* several robotic applications may include covert tracking systems that can monitor and track the robotic operators without their knowledge (i.e. iRobot cleaner) [143,144], all by secretly collecting information about them including personal details, devices in use, geographical locations, etc. [10].

In fact, threats also target the security goals that surround traditional and advanced Industrial Control Systems (ICSs), as well as the Cloud Computing (CC) domain associated with the robotic field [23].

- *Confidentiality threats* these include, in addition to the use of malware, passive traffic analysis (i.e. eavesdropping), sensitive data theft, malicious code injection (i.e. XSS or SQLi), exposure of sensitive information, side channel attacks, dumpster diving, and the adoption of social engineering or phishing techniques.
- *Integrity threats* include active traffic analysis (i.e. man/meet-in-the-middle), snooping, spoofing, data/information modification, malicious data or malware injection, false data injection, physical/logical compromise of robotic devices, back-doors, rootkits and elevation of privilege.
- *Availability threats* include service-data theft, service denial/disruption, disruption/interruption of network communications, exhaustion of resources and buffer overflow (i.e. Central Processing Unite (CPU), memory, battery consumption), jamming, malware types (i.e. Trojans, Botnets, etc.), physical damage to various equipment including routers and switches, replay attacks, and selective forwarding, as well as wormhole, blackhole and sinkhole attacks.
- *Authentication threats* include malicious third-party applications and services, social engineering and phishing techniques, abuse of privilege, key-stroke register, stealing sensitive documents, lack of proper (logical/physical) access controls, deployment of dummy/fake nodes, and spoofing.

3.4 Security risks

The rise of various robotic security and cyber-security issues, threats and vulnerabilities, in addition to their negative effects are presented as follows:

- *Security and system flaws* these risks affect the normal processing and performance of industrial robots, and could disrupt the production and industrial processes, leading to financial losses. More precisely, they could

result in a system blockage, data interception, extraction, and physical damage.

- *Back-doors* ill-configured robotic applications or applications with third-party access lead to various backdoor and rootkit attacks. This would expose robotic users by targeting their privacy first, and then by keeping them under constant surveillance, monitoring, and tracking, with possibility of registering keystrokes and capturing snapshots or even videos without their knowledge [10].
- *Remote-access* insecure and open wireless communications and communication ports, as well as unused ones if not closed, could lead to interception whereby attackers use them to gain remote access to a given robotic system to launch their cyber-attack, especially, robots relying on vulnerable LoRaWAN communications [145].
- *Device theft* robotic devices are also prone to physical theft or hijacking and control, a prime example is the de-authentication process that allows malicious users to disconnect legitimate owners and re-control them (i.e. robots and drones) [30].
- *Fake applications* many robotic applications are developed by third party vendors, some of which are fake applications masqueraded as legitimate apps. Such apps include various malware types attached to them such as ransomware, backdoor, spyware, botnet, worm, Trojan, and ransomware and can target the privacy, availability and authentication of robotic users.
- *Insecure backup and data storage* lack of proper and verified storage of data can lead to data loss or corruption. In fact, without proper data storage, any attack (i.e. ransomware) can cripple the ability of industrial organizations to safely operate, which may also affect the performance of the robotic systems and devices alike.
- *System failure* robotic systems, in case of cyber-events (i.e. attack or malfunctioning), are prone to various issues including major and cascading system failures, loss of power, and lack of operational availability.
- *Battery constraints* some robotic devices are resource-constrained and as such, they are prone to excessive battery consumption, battery power draining, battery life expectancy, and resource-exhaustion.
- *Inaccurate activity threshold* the lack of available robotic activity threshold risks having robots performing abnormal and deviating activities without them being detected. This might affect both operational and functional safety and security procedures that may endanger the life of their human operators.
- *Obstacle testing* robots that are not tested in their field of deployment are prone to various software/hardware and operating system issues. This may lead to system and hardware failures, disabling the robotic system, and bringing its production to a total halt, which is associated with financial losses.
- *Non-backed communication* can lead to the interception or loss of communication between the robotic system and its operator(s), which in turn, leads to loss of control. This occurs especially when the device goes beyond the (visual) line-of-sight. Hence, further work needs to be invested in this domain.
- *Supply-chain disruption* the disruption of semi- or fully automated supply chain systems may lead to drastic financial losses, significant time-to-repair, in addition to risking the availability of robotic services and activities [146].
- *Nature's disruption* without a backup plan to mitigate the threats imposed by natural disasters such as earthquakes, flooding, and so on, the operational services of robotic systems may come to a total halt, leading to high financial and economical losses related to the damage and destruction of hardware and software equipment, in addition to the loss of data.
- *Data transmission quality* the diversity of mitigation techniques deployed to protect robotic systems may affect the robotics' performance and data transmission quality [147].
- *Track and trace problems* can affect the real-time ability to locate robotic transits and deliveries. This may lead to supply chain poisoning and reduction of supply chain performance, especially, with the adoption of 5G technology [148].
- *Network connectivity* which is also linked to the cloud decentralization strategy helps reducing denial of service attacks. However, it comes at a cost of reduced resource elasticity and targeted attack behaviours [149]. Moreover, it also risks affecting the supply chain management and disrupts the agility of supply chains [148].

Figure 2 summarizes the different robot-related threats, their causes, and their consequences. In the next section, we discuss the occurrence of malicious attacks once these presented threats and vulnerabilities are met.

4 Robotic security attacks

There are various increasing attacks that are specifically targeting robotic systems, especially after their integration in domains such as Industrial IoT, Medical IoT and Battlefield IoT [150]. This resulted into various attacks being conducted targeting both robotics data and systems' security including confidentiality, integrity, availability, authentication and privacy. This section will present and discuss the main attacks that target the robotic field.

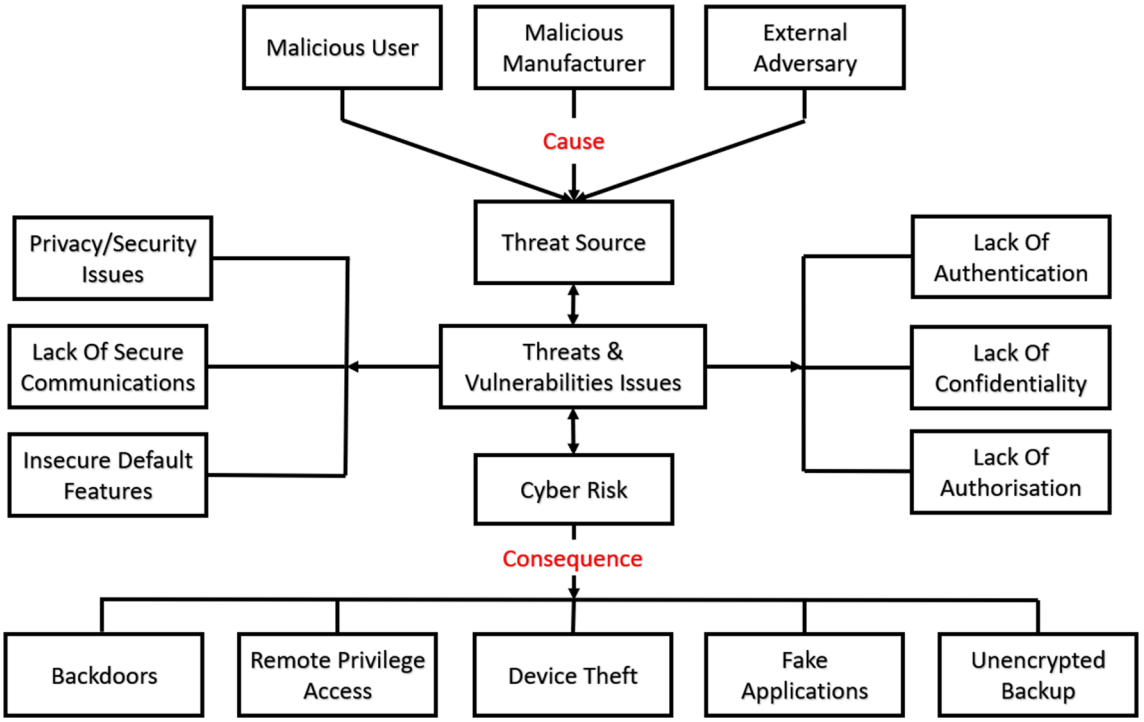

Fig. 2 A security robotic viewpoint

4.1 Robotic attacks: taxonomies and classification

The aim of this subsection is to identify and classify these attacks which target both robots and robotic systems. Moreover, the attack impact is also highlighted and discussed. For this reason, Fig. 3 is presented to summarize the main robot-related cyber-attacks, their structure and impact, along their cause and concerns. Lastly, the main risk assessment solutions are presented and analysed in order to ensure a quicker assessment of cyber risks, threats, vulnerabilities and attacks, followed by a qualitative risk assessment table being proposed.

4.1.1 Attacks on the robots hardware

These attacks can vary from least dangerous (e.g. phishing) to the most dangerous ones (e.g. hardware Trojans [151]). Such attacks can lead to the implementation of back-doors for the attacker to lead another attack by gaining unauthorized access to the robots being used, or during their maintenance [152]. In some cases, they can even have a full access to the hardware. Furthermore, robots are prone to implementation attacks such as side channel attacks or fault attacks that could possibly lead to sensitive data loss or system exploitation (depending on the attacker's target(s)).

4.1.2 Attacks on the robots firmware

The Operating System (OS) upgrades are achieved via internet connection, due to the presence of firmware codes that are usually stored on a flash memory [153]. However, with each upgrade, the OS might be vulnerable to new types of attacks. According to [154], the OS is prone to DoS and D-DoS attacks, along with the arbitrary code execution, and root-kit attacks.

On the other hand, since applications rely on running software programs to perform the required tasks, these software programs are vulnerable to application attacks, rendering the application itself prone to various types of attacks. This includes malware that including viruses, worms, software Trojans attacks, in addition to buffer overflow and malicious code injection attacks [154]. In the following, a set of these possible software attacks are described.

- *Worm attacks* aim to target the robotic systems by exploiting the vulnerabilities of their network's connected devices before self-propagation and self-replicating to infect other robotic devices, and target industrial control systems [155]. A prime example of that is the famous Stuxnet attack including its Stuxnet 2.0 and Stuxnet Secret Twin Variant [156]. This also included Flame, Gauss and Grayfish, Duqu, and Duqu 2.0 [157], which were initially designed by the joint US and Israel's SIGnal INTelligence (SIGINT) National Unit (ISNU), Unit

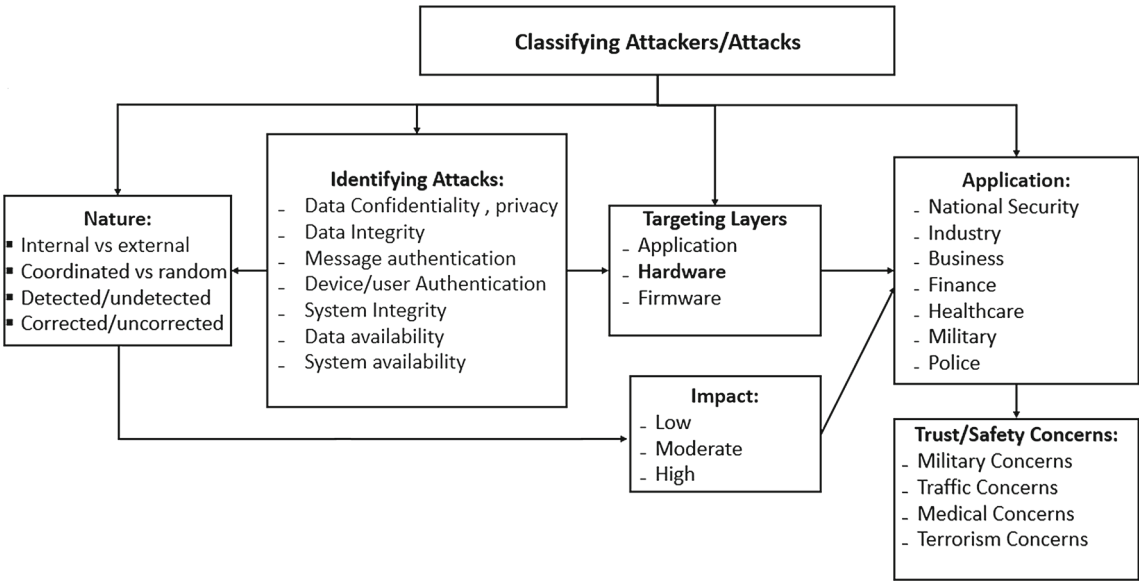

Fig. 3 Proposed attacks classification

8200 as part of "Operation Olympics" to target Iran's nuclear programassets [158,159].

- *Ransomware attacks* aim to encrypt all the data linked to robotic systems, devices and applications, as well as locking the backed up data while preventing legitimate users from re-accessing them without conducting a Bitcoin payment. Hence, the term of "Cryptoware", targeting robotic systems' and data confidentiality, integrity, availability, authentication and privacy. Many infamous ransomware attacks include CryptoLocker (2007), Troldesh (2015), Petya (2016), Locky (2016), Jigsaw (2016), WannaCry (2017), Bad Rabbit (2017), GoldenEye (2017), Ryuk (2018), GandCrab (2018) [160], LockerGoga (2019) and CovidLock (2020).
- *Trojans and random access trojan (RAT) attacks* Trojans are usually masqueraded in the form of a legitimate application and sometimes can be carried out via a phishing email or in a form of a Winlocker (i.e. police ransomware). RATs usually occur when an unauthorized access is gained by bypassing all the deployed security measures to protect robotic systems. It usually targets the authentication process, as well as data and robotic systems' privacy, confidentiality and integrity, and can be linked to Botnets to conduct DDoS attacks. Many Trojans include Storm Worm (2006), Zeus (2007), Plug X malware (2008), and Emotet (2018).
- *Rootkit attacks* allow a given attacker to have a privileged controlled access on an administrator level (i.e. Chief Robotic Officer) with the ability to have access to information and data related to robots and robotic systems. The aim is to alter robotic data and systems' logs, while leaving a backdoor for future attacks or installing a covert spyware, which affects the confidentiality, integrity, authentication and privacy aspects.
- *Botnet attacks* are usually employed as bots to conduct D-DoS attacks against medical and industrial robotic systems. Botnets can be based on malicious codes used to infect unprotected robotic devices. Botnets can also be linked to worms, ransomware and Trojans which allow them to conduct attacks against robotic systems' and data's privacy, confidentiality and integrity. This includes a variety of botnets such as Storm (2007), Cutwail (2007), Grum (2008), Kraken (2008), Mariposa (2008), Methbot (2016), Mirai (2016), and Glupteba (2019). This type of malware can affects the confidentiality, integrity, availability, authentication of data and robots.
- *Spyware attacks* the purpose is to gather information and data about the robot operator, the connected device and the robot in use to send this information to malicious third party, by simply installing this malware on a device controlling the robot. Thus, this results in being capable of monitoring the user's activity and consequently its robots activity.
- *Buffer overflow attacks* aim to exploit the ROS vulnerability to manipulate a robotics' device memory to control the robot and hijack it. Buffer overflow is based on two main types: stack-based, which is a continuous space in memory used to organize data associated with robotic function calls; and heap-based, which is where the amount of memory required is too large to fit on the stack. This attack type is used to affect different robotic security services such as robotic data and systems' authentication, availability and confidentiality.

- *Password cracking attacks* aim to target the authentication of the robotic systems, which later on can be further exploited to gain a full access privilege, targeting also the confidentiality, integrity and privacy of both data and robotic systems. Password cracking attacks can take many forms [161] including brute force attacks that guess and capture a user's password or personal identification number (PIN) [162], dictionary attack which uses a huge default word-set to try and guess the password. This also includes birthday attacks, online/offline password guessing, and Offline Password Guessing Attack (OPGA) [163].
- *Reverse engineering attacks* also known as a person-to-person attacks, are based on the attackers' ability to convince their victim(s) that they are legitimate users (i.e. IT firms, etc.) and luring them to retrieve useful information which the attacker needs to launch his attack against a given robotic system or device [164]. This targets both data and robotic systems' privacy, and integrity.
- *Surveillance attacks* include creating malicious robotic applications, third-party applications and anti-virus systems masqueraded as legitimate ones, and include also fake updates and pop-ups that urges robotic users from clicking on them to fulfil the update task. Malware can also be downloaded even if the user clicks on the "X" button. Once the malware is activated, all the user's private information and data is stored and covertly leaked to malicious parties, keeping robotics users and operators under a constantly covert surveillance with the ability to control and hijack the operational robot [165]. Thus, this type of attacks targets robotic data and systems' confidentiality, integrity, authentication and privacy.
- *Malicious code injection (MCI) attacks* or Remote Code Execution (RCE) attacks are based on an attacker's capability of executing malicious codes in order to perform an injection attack [166]. They are also capable of exploiting any coding vulnerabilities in the robotic software. This results in being able to exploit these vulnerabilities by injecting a malicious code script and running it without the user's knowledge. This led the authors in [167] to manage the use of such attack in order to test it on social robots to prove how insecure they are, as well as to highlight their lack of authentication.
- *Phishing attacks* are still ongoing with a variety of phishing attack types [168,169] targeting robotic employees and firms with different privileges and access level. This can lead to the exposure of their robotic devices in-use and lead to their compromising and loss of control. This can affect both robotics data and systems' privacy, integrity, availability and authentication processes.

4.2 Attacks on the robots communications

Robotic communications are also prone to different attacks that might affect different security services (i.e. authentication, confidentiality, and integrity), as stated in the following.

- *Jamming attacks* aim to interrupt and disrupt the robot-to-robot and robot-to-humans communication with the aim to suspend further robotic activities and jam any sort of communication and control. Thus, targeting both systems and data availability.
- *De-authentication attacks* aim to temporarily, periodically or disable the robotic devices from being able to connect back to their initial operator, disrupting the communication between them and the robotic devices and possibly preventing them from re-connecting back and hijacking the robot by gaining control. This aims to target the availability, authentication and integrity of both data and systems.
- *Traffic analysis attacks* since robotic systems are still relying on open wireless communications or communications with basic security measures, traffic analysis attacks can occur in a much more frequent manner. This includes listening to the ongoing traffic between the robots and their robot controllers, and retrieve vital information without being detected. This mainly affects the privacy and confidentiality of both robotic systems and data, and can lead to further future attacks.
- *Eavesdropping attacks* aim to passively monitor the transmitted robotic traffic over encrypted and un-encrypted open communication channels. This can help with the collection and extraction of sensitive information about the robotic systems and their current operators, targeting robotic data's confidentiality, and privacy. In fact, advanced eavesdropping can take the form of a "cloning and replay" attack, which recovers the data via an information gathering process, before conducting the eavesdropping attempt.
- *False data injection attacks* target the privacy and integrity of the robotic data and the availability of robots, by intercepting and modifying its payload [170]. This can be done through the initial interception of the ongoing robotic communication and altering it by injecting false data and information, which deviates the robots from performing their intended activity in an accurate manner, or leave them prone to response delays.
- *(Distributed) denial of service attacks* can be conducted locally or globally (distributed) in a simultaneous manner which aim to prevent legitimate users from accessing robotic systems and devices. DoS can be performed by sending excessive requests, that lead the network to re-authenticate requests that have invalid return addresses [171]. Other DDoS/DoS attacks include

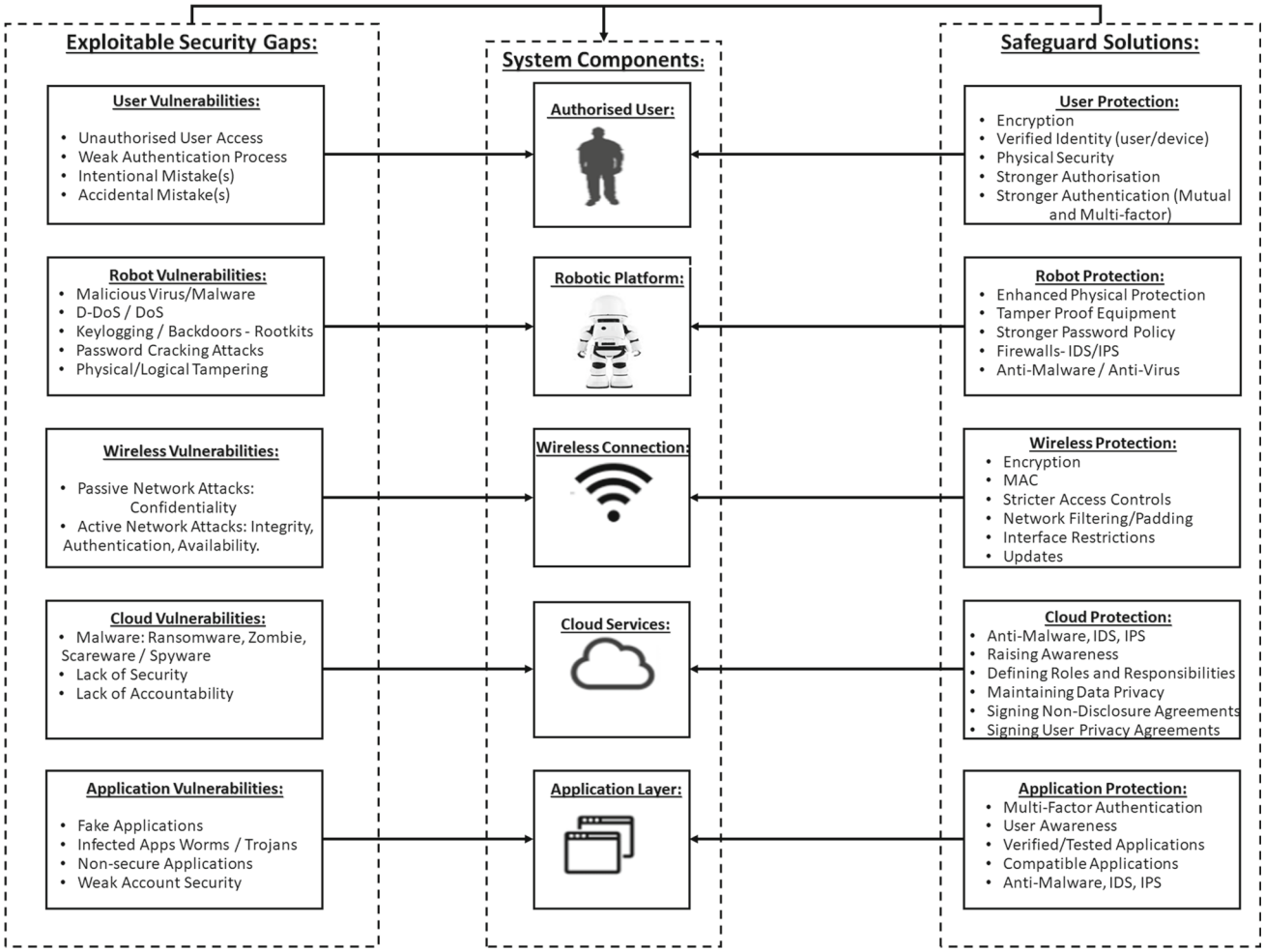

Fig. 4 Targeting layers classification

packet-dropping attack that targets different packets types located at the network layer or above [172], also Volume Based Attacks (UDP and ICMP (ping) floods), Protocol Attacks (SYN floods), Application Layer Attacks (low-and-slow attacks, and GET/POST floods), Ping of Death (POD) attack, Slowloris, HTTP/HTTPS flood, NTP amplification attacks, blackhole attacks, and finally Zero-day DDoS attacks including Mirai botnet [154].

- *Replay attacks* occur when a given adversary stores and replays at a later time the old messages sent between the robot and its operator to disrupt the ongoing traffic. The replay attack's mechanism is based on broadcasting the previous transmitted message to manipulate the location and the nodes' routing tables [11] to masquerade the identity of the attacker. Therefore, this affects the availability of both data and robotic systems.
- *Masquerading attacks* are ranked as one of the main electronic crimes perpetrated such malware attacks. The attacker (fake robot or controller) seems to be authentic since a valid identity is used, which is known as a mask. This is done by forming a blackhole or generating false messages which are then broadcast to the other robots. This attack has different objectives such as slowing down or up the speed of a robot, which may lead to an incident, or target its operational activity and performance. This type of attacks targets the robotic systems' availability and integrity by affecting its accuracy.
- *Man-in-the-Middle (MiMA) attacks* occur when an attacker is capable of actively listening and intercepting the communication between two robotic entities or nodes, alter the information and inject it without being detected. This allows the attacker to control the communication between these legitimated entities [173]. This mainly targets robotic data's confidentiality, integrity and authentication.
- *Meet-in-the-Middle (MITM) attacks* or plaintext attacks occur when the robotic communication is encrypted using a 2-DES, and now 3-DES key (168-bit) using a brute-force like technique to break the encrypted com-

munication channel and either actively or passively eavesdrop. This type of attacks targets robotic data's confidentiality, integrity and authentication.

- *Identity attacks* this type of attacks includes identity revealing attacks, which consists of retrieving the identity of the robot to put its operator's privacy at risk. Equally important, the attacker can track the robots location, which exposes all the needed information and geographical location about robotics systems along their users and devices.
- *Network impersonation attacks* aim to obtain the credentials of a legitimate entity in a given robotic network by claiming its network ID. This allows an attacker to advertise fake data which confuses other network entities, and to flood the robotic networks via DoS attacks.
- *Message tampering–fabrication–alteration attacks* aim to break the integrity of the exchanged messages, which is done by altering or creating fake messages, with both authentication and data integrity being affected in this case. This can lead to change the robot events log.
- *Illusion attacks* legally compromised robots are placed in the network to generate false data. As a result, false data can spread over the network. In this attack, the authentication countermeasure is not efficient, since the attacker is already authentic. In the robotics case, fake messages are capable of changing the decision of the robot controller.

Figure 4 summarizes the different attacks based on the targeted layer. As a result, based on the conducted research and perspective, this paper presents the main attacks that targets the main robotic layers. This includes their targeted layers and data security goals (confidentiality, integrity, availability, privacy and authentication alike). Therefore, they are classified and included in Table 1. In the next section, the effects of the listed attacks are discussed.

4.3 Robotic attacks: impact and concerns

The increasing number of attacks against robots and robotic systems has led to an increase in number of concerns [10]. This has raised many concerns surrounding this field along questioning the ability of effectively deploying in various domains and areas of operation.

- *On national security* the use of robots and robotics in domestic crimes and domestic terrorism has increased recently, not only through their use in the cyber field, but also in the physical field too. Robots can be re-modified to carry lethal weapons or can be re-programmed to perform an excessive use force which can lead to both human and material losses [200]. In fact, without a proper programming that ensures a safer and much more secure deployment and use of robots in police and law enforcement fields, robots may end up in a blue-on-blue engagement which may result in friendly fire, or engaging the wrong targets including civilians.
- *On battlefields* the use of robots in combat, especially on battlefields have proven to be very useful especially in counter-terrorism and counter-insurgency operations (Lebanon, Gaza, Syria, Iraq, Libya, Pakistan, Afghanistan, Yemen, Mali, Somalia, Nigeria, etc.), as well as military operations (i.e. Ukraine, Syria and Nagorno-Karabakh). However, their use by insurgents and terrorists alike, has proven to be also challenging especially with the use of explosive-laden autonomous drones and boats, and also using combat drones [114, 201,202].
- *On business and industry* the reliance on robots is offering a remarkable growth in the number of robots being deployed in the industrial fields with many business extensively relying on their use to ensure a faster productivity, in a less timely manner with a reduced cost and needed resources. However, robots can also be prone to technical and operational problems that threatens the safety of the working personnel [203], as well as cyber-attacks including the disclosure of secret business trades [10]. Such move can cause distrust among customers and the loss of many business trades related to the impractical safe and secure use of robots. In fact, robots are prone to (cyber) industrial espionage and sabotage operations especially caused by rival organizations or part of a state-sponsored campaign [204,205].
- *On economy and finance* the adoption of robots will surely boost productivity and economic growth, and creates new jobs and opportunities, especially in terms of creativity and social intelligence [206]. This includes an increase in labour's quality, increase in the Total Factory Productivity (TFP) and Capital Factory Productivity (CFP) and Multi-Factor Productivity (MFP) [207], which allows a further growth in terms of productivity and Gross Domestic Product (GDP). Despite the economic boost that the employment of robotics offer especially in industrial and manufacturing fields, except that it comes with a negative impact. Such employment is leading to many job losses worldwide, which is mainly affecting low-skilled workers and poorer local economies, leading to socio-political economic crisis [208,209]. Hence workforce skills must be developed by policy-makers and manufacturers to adapt to this growing robotic automation.
- *On health care* despite the known advantages of using robots in surgeries, medical robots were reported to have a negative impact on patients' lives due to inaccuracy mistakes and errors [210], or due to cyber-attacks (i.e. data exposure/leakage) such as the case of North Korea-Unit 180 (Lazarus) attack on UK's National Health Service

Table 1 Targeting security goals

Attack layers	Attack/vulnerability	Cause	Consequence	Countermeasure
Hardware	Social/reverse engineering	Lack of employees training/awareness	Stealing of confidential papers/documents	Further employee training/firmer access controls
	Backdoors [174,175]	Un-trusted hardware company	Infected hardware with malwares, gain unauthorized access	Trusted hardware companies/pen testing
	Cold-boot [176]	Unauthorized physical access to a given device to retrieve encryption keys from a running operating system after using a cold reboot to restart the device	Loss/alteration of data/information	Verified source and brand origin
	Physical memory	Physical damage or modification of hard drives/disks	Loss of information, alteration of data	Physical protection/privilege access
	Power disruption	Higher power voltage/loss of power	Disruption/denial of service	Additional backup computational devices, self-balancing robots [177]
	Insider [178]	Angry employee destroying a company, sabotage	Disruption/interruption of service	Physical protection/privileged access control [179]
Firmware	Malware types	Different malwares injected separately or combined	Further system/data damage is performed	Up-to-date intrusion detection/prevention, anti-viruses
	Ransomware [180]	Lack of physical/logical protection	Information disclosed, locked, deleted and modified, payment urged and needed	Key confidentiality, internal/external authentication [181]
	False data injection [170]	Data altered and modified	False information added, robotics performing unwanted tasks	Intrusion detection/prevention systems, access control policies, encryption
	Botnets [182]	Infected robotics devices used by an attacker	Resource exhaustion, loss of control	Anti-virus, anti-spyware always updated
	Wormhole [183]	WannaCry attack that targets and disrupt the availability and integrity alike	Privacy breached, availability disrupted, access blocked and locked, payment urged (ransomware)	Intrusion detection/prevention systems, honeypots, anti-viruses
	Default passwords	Easily broken and cracked	System breached, information disclosed, data altered	Access control policies, identification/verification and stronger passwords are required

Table 1 continued

Attack layers	Attack/vulnerability	Cause	Consequence	Countermeasure
	Unlocked devices [184]	Robotic devices (laptops, desktops, tablets) left unlocked	Devices destroyed, stolen, modified (key-logging, spyware, ransomware)	Devices locked, intrusion detection/prevention systems, encryption, privileged access, biometric techniques [185,186]
	Password cracking [187]	Weak passwords implementation	System breach, information disclosed	Strongly constantly changed passwords
	Spear-phishing [188]	Infected file sent by e-mail	Information gathering, disclosure of information, infected device	Intrusion detection/prevention systems, honeypots, firewalls
	Surveillance	Fake applications	Spyware, rootkit, RAT installed, privacy attacked	Verified applications, anti-virus, anti-spyware
	Malicious code injection	Lack of programming skills, weak coding	Accuracy attacked	Buffer overflow, input validation
Communication	Eavesdropping	Non-secure communication	Information gathering	Encryption and privacy-preserving techniques
	Distributed/Denial Of Service, side channel attack [189,190]	Jamming communication lines [191], exploiting crypt analysis and software bug	Servers down, service interrupted	Close unused ports, channel surfing, frequency hopping
	De-Authentication [192]	Targeting access points	Disruption of services between access points and robotic devices	Back Up servers, back up devices, frequency hopping
	Offline password guessing [193]	Capability to performing offline password attacks	Targets the robotic system offline	Firmer authentication and identification/verification processes
	Password cracking [194]	Lack of strong authentication measures	Unauthorized access, stealing of documents	Strong multi-factor authentication
	Authentication attack	Single-factor authentication	Unauthorized access, physical damage	Strong multi-factor authentication
	Man-in-the-Middle attacks [195], Rootkits [196], RATs [197]	Data alteration and interception	Loss of information, loss of robotic control, wrong orders issued	Stronger multi-tier encryption, Intrusion Detection System (IDS) [198,199]

(NHS) in 2017 [211,212]. As a result, medical concerns arose about the possibility of performing physical (i.e. loss of control) or logical (i.e. malicious data modification/injection) attack against a human patient [154], along the possibility of potentially performing assassination attempts (i.e. Vice President Dick Cheney) [213]. Moreover, the idea of knowing that robots will perform the surgical operation can scare many patients and affect their trust in a psychological manner [154].

- *On operations and functionality* both robotics and cloud robotics are descried as automated systems that rely on data to support their operations, and communicate via wireless networks. In fact, they are not integrated into a single stand-alone system [16], to ensure much more flexibility. This allows them to save battery consumption by offloading intensive tasks to the cloud services with the implementation of AI mechanisms. However, the reliance on cloud services and third party applications and open communication leads to causing network bottleneck, overhead and delays [214], as well as being prone to interception and alteration with lack of repudiation and accountability.
- *On humans* different issues arose with the reliance on robotics to perform human acts in various domains, especially in the industrial field to reduce the reliance on human labour. Table 2 presents real-case robotic incidents which resulted in a number of casualties and fatalities due to inaccuracies or fatal incidents related to the use of robots in various domains. In fact, traffic concerns also arose especially with fatal incidents related to autonomous driving cars were constantly being reported [154,215].

After reviewing the different security attacks that might compromise the robotics systems security. In the next section, we assess the risks associated with the listed attacks.

4.4 Robotic risks assessment

Robotic systems and platforms are vulnerable to various attack types, risking the disclosure, destruction, alteration and modification of sensitive information. Other risks are also associated with weak authentication and password cracking attacks, allowing attackers to gain a remote unauthorized access to the system to perform malicious tasks.

4.4.1 Qualitative risk assessment methods

Various risk assessment and management methods started emerging into the robotic field to maintain a secure robotic platform and communication. In fact, risks analysis was presented in [216], and is based on the Threat, Risk, Vulnerability Analysis (TVRA) methodology [217]. This methodology assesses the likelihood and impact of a given risk and attack. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) was presented in [218] and discussed in [219]. OCTAVE is used to evaluate risks based on a risk acceptance level without focusing on risk avoidance. Moreover, another method called "Méthode Harmonisée d'Analyse de Risque (MEHARI)" was presented in [220], to ensure a quantitative risk assessment of risk components, and is based on measuring the maturity of system level. Additionally, the CCTA Risk Analysis and Management Method (CRAMM), which is a resource exhaustive approach was used in [221] to identify and analyse risks using a software to implement a given method with its security measures. Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) [222] was used to identify different risks according to their severity level. However, EBIOS lacked the ability to indicate what security solution is needed to mitigate a given risk.

In fact, recently, various risk assessment solutions and frameworks were presented especially for Industrial IoT systems where robotics are mostly deployed. Here, this paper presents and discusses them. Suzen et al. examined the sources of cyber-security threats and vulnerabilities in the Industry 4.0 ecosystem [223]. Moreover, preventive cyber-defensive measures were also discussed along other defensive strategies which highlighted the lack of training and basic security measured applied by the concerned personnel. Brandstotter et al. presented a new and comprehensive safety concept for collaborative robotic systems that estimates and validates which changes on the system can be made without conducting a new risk assessment [224]. Komenda et al. presented the impact of modifications on collaborative robotic cells along how they influence the risk assessment in the concept of human–machine collaboration [225]. This advanced structured approach for safety assessment enables a safer implementation of modifications to a known extent. However, future work is still required to ensure an extensive comparison using real experimental setup. Chemweno et al. reviewed the ISO 15066 and ISO 10218 standards for collaborative robots systems and explored its gaps [226]. As a result, a framework based on the ISO 31000 for orienting design safeguards for collaborative robots to ensure a proper hazard, safety assurance, analysis and risk assessment. Wan et al. developed TOPSIS as an extended Failure Mode and Effects Analysis (FMEA) model that introduces environmental impacts as risk factors and evaluates the potential failure risk of robots to ensure their effectiveness and feasibility [227]. George et al. presented a multi-attacker multi-target graphical model for risk assessment which represents attackers, targets, and network's vulnerability [228]. Moreover, several risk mitigation strategies were also presented to secure edge devices in IoT networks. Huang et al. revised the Analytic Hierarchy Process (AHP) method and presented a

Table 2 Real-case robotic incidents

Incident	Date	Country	Casualty	Fatality
Golden state foods	July 21st, 2009	USA	0	1
Military incident	Oct, 2007	South Africa	14	9
SKH metals factory	August 13th, 2015	India	0	1
Shenzhen tech trade fair	Nov, 2016	China	1	0
Stanford shopping centre	Jul, 2016	USA	1	0
Medical	2001–2015	USA	1000+	144
Car-factory	June 2016	USA	0	1
Traffic	May, 2016	USA	0	1
Traffic-tesla model S	May 7th, 2016	USA	0	1
Counter-domestic terrorism	July 8th, 2016	USA	0	1
K5 robot incident	July 14th, 2016	USA	1	0
Ventra Ionia mains plant	March 14th, 2017	USA	0	1
Traffic-uber autonomous car	March 28th, 2018	USA	0	1

3-layer AHP-based risk assessment model (3aRAM) for an Industrial IoT cloud (PaaS platform) [229]. Two experiments were conducted to show the system's security benchmark to define the IIoT cloud's current status. Radanliev et al. presented a new model that included a design process with new risk assessment vectors for IoT cyber risks [230]. Moreover, an epistemological framework was used by applying the constructivism grounded theory methodology to draw on knowledge from existing cyber risk frameworks, models and methodologies to present a new model for IoT cyber risk impact assessment. Finally, Lv et al. presented a CPS trusted robust intelligent control strategy and a trusted intelligent prediction model which relies on the automatic online evaluation method of CPS reliability based on ML [231]. The AI-based CPS strategy aims to improve the response speed against various threats, while also improving the predictability and accuracy of risk prevention.

4.4.2 Proposed qualitative risk analysis

Assessing risks in a quantitative manner is not an easy to achieve, as it still remains a challenging complex task. Nonetheless, a new risk assessment is needed to quantify the security risks that surround the robotic domain. As a result, we present our Robotic Risk Assessment (RRS) method (Table 3), based on evaluating the likelihood and impact of a given attack (High/Very High, Damaging/Devastating) against the main system components presented earlier, along which security service the attack targets along its impact (critical, major, minor). Moreover, the system exposure level (i.e. high, medium, low) is also evaluated based on whether the system is secure, semi-secure or not secure at all, while various security measures are presented per attack.

In the light of the listed concerns, securing robotic system is of high importance. In this context, the next section presents the different countermeasures presented in order to prevent and help mitigating the discussed security attacks.

5 Securing robotics: presented solutions and effective countermeasures

It is essential to implement and maintain effective security countermeasures in order to secure the robotics systems. Therefore, the need for a strong multi-factor authentication process, along with the identification and verification processes (based on a strong access control policy and robot fingerprints measures), in addition to multi-factor confidentiality, are highly recommended. This allows the prevention of any malicious physical and/or logical unauthorized access. In fact, securing robots, robotics, and robot operating systems is not an easy task. However, it is not also an impossible task either. Therefore, different cryptographic, non-cryptographic and AI-based solutions were presented for this specific task. We highlight the various solutions presented by various authors and highlight their advantages and drawbacks.

5.1 Cyber threat intelligence

The Cyber Threat Intelligence (CTI) is based on the information gathered about robotic threats and threat actors which would help in mitigating harmful cyber-events based on the Advanced Persistent Threat (APT) concept through early detection and prevention. In fact, CTI sources include information gathered from HUMman INTelligence (HUMINT), Open Source INTelligence (OSINT), TECHnical INTelligence (TECHINT) and intelligence gathered from the dark web (silk road) [232,233]. This allows an enhancement in the robotic domain via an evidence-based malware analy-

Table 3 Proposed qualitative risk analysis for robotic systems

System		Impact on security services				Risk		Exposure system level			
Components	Attacks	Confidentiality	Integrity	Availability	Authentication	Likelihood W/O protection	Impact W/O protection	Protected	Semi-protected	Unprotected	Countermeasure
Authorized user	Unauthorized user	Major	Minor	Major	Critical	High	Damaging	Low	Medium	High	Stronger identification and physical security
	Weak authentication	Critical	Major	Major	Critical	High	Damaging	Medium	High	High	Multi-factor authentication
	Intentional accidents	Critical	Critical	Critical	Major	High	Devastating	High	High	High	Stronger verification/authorization
	Accidental mistakes	Minor	Minor	Major	Minor	Moderate	Less Damaging	Low	Low/medium	High	Verified backup/user training
Robotic platform	Malicious malware	Critical	Critical	Critical	Major	Very High	Devastating	Medium	High	High	Anti-malware, IDS
	DoS/DDoS	Minor	Minor	Critical	Minor	High	Damaging	Medium	High	High	Firewalls/IDS/secure backup
	Keylogging /backdoors	Critical	Critical	Major	Major	High	Damaging/devastating	High	High	High	Pen testing, vulnerability assessment, IDS
	Physical /logical tampering	Major	Critical	Major	Minor	Medium	Damaging	Low	Medium	High	Physical protection, tamper proof equipment
Wireless connection	Passive attacks	Critical	Major	Minor	Minor	High	Damaging /devastating	Low	Medium	High	Dynamic lightweight encryption
	Active attacks	Critical	Critical	Major	Minor	High	Devastating	High	High	High	Encryption, IDS/IPS

Table 3 continued

System		Impact on security services				Risk		Exposure system level			
Components	Attacks	Confidentiality	Integrity	Availability	Authentication	Likelihood W/O protection	Impact W/O protection	Protected	Semi-protected	Unprotected	Countermeasure
	Jamming	Minor	Minor	Critical	Minor	High	Damaging	Low	Medium	High	Frequency hopping, frequency shifting
	Stealing data	Critical	Critical	Major	Major	High	Devastating	Medium	High	High	IDS/IPS, Honeypot
Cloud services	Malware/botnet	Critical	Critical	Critical	Major	High	Devastating	High	High	High	IDS/IPS, honeypot, anti-malware & virus
	Side channel	Critical	Critical	Major	Minor	High	Damaging	Low	High	High	Secure system design, system protection
	Insider	Critical	Critical	Critical	Critical	Very High	Devastating	High	High	High	Employee screening, background check
	Service hijacking	Critical	Critical	Critical	Major	High	Damaging/devastating	Low	Medium/high	High	User awareness, anti-phishing and spamming
Application layer	Malware/spyware /botnet	Critical	Major/critical	Critical/major	Minor	High	Damaging/devastating	High	High	High	Anti-malware/spyware up-to-date, avoid free applications, IDS/firewalls
	Spoofing	Critical	Major	Critical	Minor	High	Damaging	Low	Medium	High	Encryption, anti-spoofing, Packet filtering
	Key log /rootkit	Critical	Critical	Major	Minor	High	Devastating	High	High	High	Vulnerability patching, Anti-virus, Hard-disk scan
	XSS/SQLi	Critical	Critical	Major	Minor	High	Damaging	Low	High	High	Vulnerability scan, web application firewall, mitigation and Discovery

sis, security incident's outcome utility, and data/information security controls.

CIT includes three intelligence types that can be described as follows:

- *Tactical CIT* assists in identifying threat actors.
- *Operational CIT* assists in identifying the threat actors' motives, used tools, techniques and tactics.
- *Strategic CIT* assists in developing high-level organizational strategy.

In fact, the reliance on CTI, especially in supply chains and Industry 4.0 [148], allows an enhanced and accurate alert assessment that allows a faster predictive and reactive Incident Response Service (IRS) [234] through cyber-threat detection, risk assessment, and log inspection/monitoring. This is achieved by combining the human–machine analytical capability to reach a higher level of INFOrmation SECurity (INFOSEC) by relying on human assistance and AI combined [235]. This benefits the robotic domain to boost its cyber-security levels by:

- *Development of proactive cyber-security* which bolster the overall risk assessment and risk management policies and procedures.
- *Development of predictive cyber-security* to ensure a higher level of threat detection in a much more accurate and timely manner with the least false-positive and false-negative rates.
- *Enhanced incident response systems* by combining both humans and machines assets, especially in detecting and responding to incident using ML and AI security measures before, during and after the event has taken place, through early detection, ongoing prevention, and lessons learnt, respectively.
- *Enhanced decision making* which is achieved with a much more accurate and timely manner based on the information collected about a cyber-event including an attack, intrusion, defence, etc.

5.1.1 Active security awareness

The Active Security Awareness (ASA) program requires being further extended and adopted since it can greatly reduce robotic risks that cannot be easily addressed to using robotic software and hardware devices. This requires an extensive focus on the security and safety of human elements business on the adoption of various security awareness programs, training, modules and (online) lessons to help growing an effective and affordable security awareness culture targeting all the personnel working in the robotic field and domain [236]. The advantage of applying ASA includes:

- *Solid security policies* which are developed in a professional way to enforce security to show a resilient commitment in achieving the needed robotic security and cyber-security.
- *Security requirement analysis* analyses the security requirements to formulate effective polices and management procedures to be applied in the robotic domain.
- *Defining formal security processes* which help in designing specifically secure solutions, especially in the non-cryptography domain, including the configuration and deployment of firewalls, honeypots, intrusion detection/prevention systems which are deployed on the Robotic Operating Systems (ROSs) and applications alike.
- *Reduced operational risks* which in turn would result into limiting the drain of financial resources and losses, while increasing a boost in terms of economy and investment.
- *Real-time security awareness* provides an up-to-date security awareness against security risks, threats and issues that surround the robotic domain.
- *Advanced employee education* promotes a higher real-time security awareness and knowledge related to employees' expected behaviour, activities and responsibilities to efficiently safeguard and protect any robotic information from being leaked.

5.1.2 Active response: detection and prevention

In active response, detective and preventive measures are essential to provide additional security protection through an easier and less complex implementation of detective and preventive security measures and platforms. This includes the adoption and deployment of centralized and decentralized hybrid, lightweight [237,238] and AI-based [239,240] intrusion detection and intrusion prevention systems, as well as antivirus mechanisms to trigger an automated response through a constant and continuous monitoring. Such adoption can bring many advantages to the robotic domain especially in the IIoT field.

- *AI-based detection* through the adoption of ML-based mechanisms to ensure a higher accuracy in a timely manner.
- *Hybrid detection* includes the combination of signature-based, behaviour-base and anomaly-based IDS/IPS patterns to cover a larger variety of robotic cyber-attacks and threats.
- *Constant vulnerability monitoring* through a constant vulnerability check, assessment, and management of the up-to-date systems, applications and security patches to ensure a higher level of detection and prevention.
- *Advanced activity monitoring* allows the continuous monitoring of a robotic device's behaviour over time and

compares it to check whether the behaviour threshold is different than the normal pattern (rogue device).
- *Easier deployment* ensures an easier integration around the robotic systems, including on networks, devices, software, firmware or even robotic operating systems, to ensure a constant detection and protection.
- *Easier management* to ensure a faster response for incident responders and (cyber) security professionals including security IT security.
- *Enhanced access management* which defines the right data classification and protection via enhanced authentication mechanisms such as a privileged account management, or via endpoint network encryption to secure robotic communications.

5.1.3 Active management: precaution and correction

The active management includes the adoption of both precautions and corrective measures. Precaution is essential in the early stages of any robotic design. In fact, other security precocious measures should also be taken into consideration during the early phases of robotic testing and design. This is essentially required to ensure that safety and security measures are taken into consideration by both manufacturers and integrators to ensure an efficient use. Moreover, robotic operators must also adhere to a certain degree of awareness and training, as well as a screening process to prevent its use for criminal or terrorist purposes. This can be further seen in Fig. 5. Additionally, corrective measures are also important as they are capable of allowing robotic systems of self-healing. Thus, being capable of autonomously restoring their operational capabilities without any serious interruption(s). Corrective measures can also be applied to isolate infected robotics systems, sensors and devices alike from the other operational devices to prevent further damage and attack escalation over a given system, especially if the attacks target the availability of robotic systems.

5.2 Robotic security protection

Despite the attacks that surround the embedded robotic systems' architecture, effective countermeasures can be adapted and employed to prevent security attacks [154]. These countermeasures can help with overcoming any exploitable vulnerability, and security gap. In the following, we list the main actions that should be taken to prevent robots security attacks.

- *Hardware protection* Robots have been prone to various types of hardware attacks, since their early stage of manufacturing and maintenance. As a result, hardware testing and monitoring are key to avoid any future exploitation [154]. In this context, many solutions have been presented [241]. This includes isolating Internet Protocol (IP) cores mechanisms [242], along with implementing solutions for payload detection [243], and the implementation of the Integrated Circuit (IC) fingerprinting technique [244].
- *Firmware protection* securing software requires taking into consideration the firmware aspect of robots. Hence, it is essential to ensure that the software patches are always updated, protected and always monitored and tested for any possibly suspicious activity. In order to protect the firmware, Clark et al. have suggested the adoption of a common standardized OS such as NuttX OS [154]. This prevents the exploitation of the firmware and reduces the likelihood of an attack. However, it is also recommended to add an authentication process to secure robots. Moreover, the use of message authentication and encryption mechanisms helps ensuring secure communications between robots and their control systems.
- *Application protection* It is essential to limit, reduce and overcome the likelihood of an application from being under the threat of any possible cyber-attack. Doing so would highly require the need to develop a well-built, well-defined, and well-secure application code, that prevents any possible code exploitation. Thus, this makes the robots control system less prone to malicious code injection or modification attempt(s) [154]. Moreover, before designing any application, each application must undergo a security testing phase to identify any possible vulnerability and/or security gap that can be found and detected. This helps by reducing and preventing further exploitation and future cyber-attack(s).

5.3 System hardening

Robotics' system issue has been ongoing for a while, as early as the design phase. However, recently, more light has been shed on overcoming this limitation with the focus on ensuring how to secure robotic system's software, hardware and communication. As a result, various solutions were recently presented. For this matter, two solutions were presented. One was presented by Pike et al. who managed to incorporate a Control Flow Integrity (CFI) check into the Real-Time Operating System (RTOS) [245]. The second one was presented by Abera et al. who managed to devise a Control-Flow Attestation for Embedded Systems Software (C-FLAT) to verify remotely the CFI on a given embedded device in [246]. In [139], Ahmad et al. analysed cyber-physical security threats that target the communication link between "Adept MobileRobots" platforms and their clients [247,248]. The authors analysed the existing vulnerabilities on the communication link used by robotic applications. Afterwards, the authors targeted the integrity, availability, and confidentiality, using an impact-oriented approach. This was done

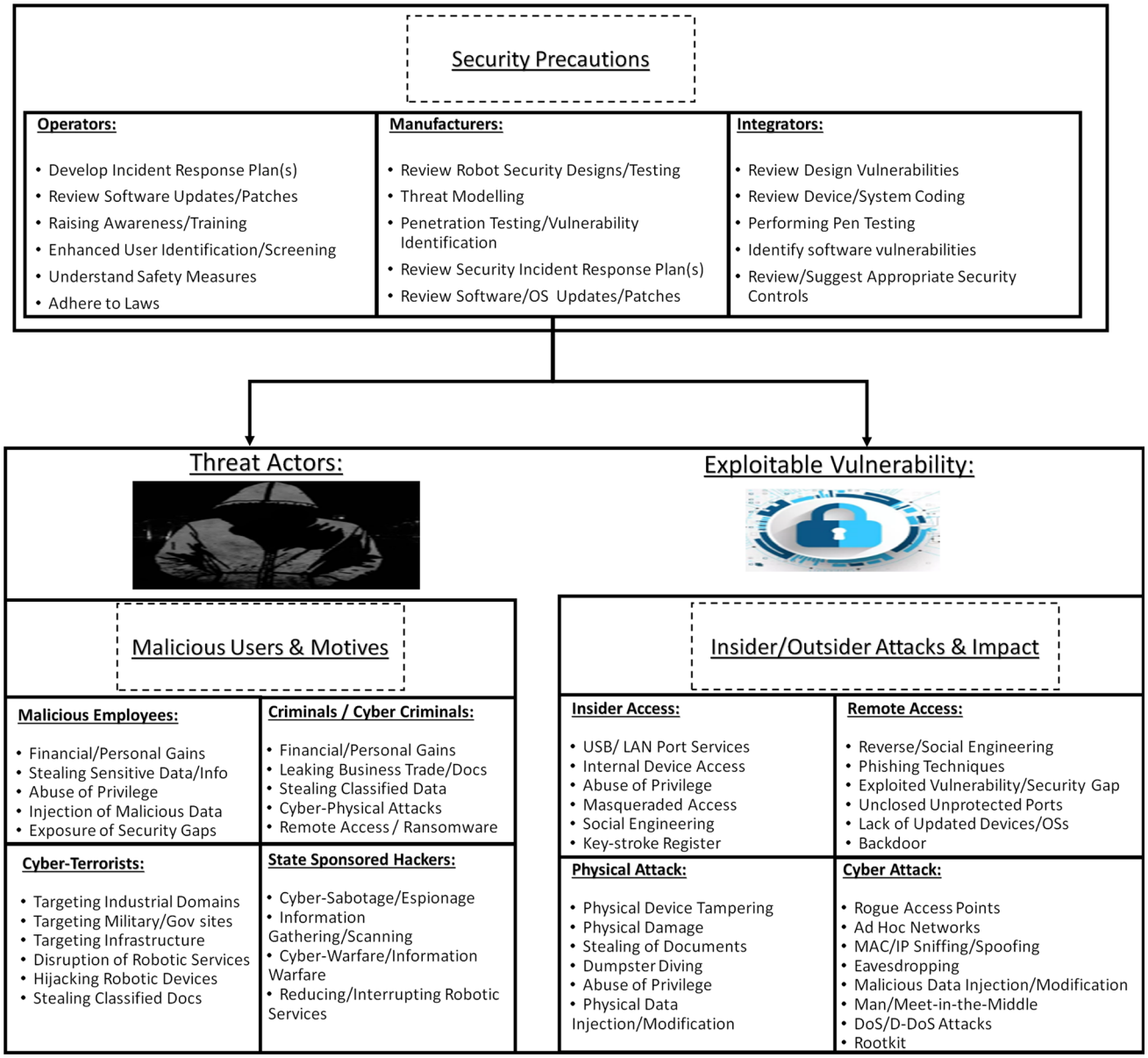

Fig. 5 Precocious robotic measures

by following the National Institute of Standards and Technology (NIST) adversarial risk assessment template [249]. The authors designed an open source Robot Attack Tool (RAT). Moreover, their performed attacks' risk level was qualitatively assessed with physically consequences being identified. The authors' goal is to improve both safety and security of robotic platform by raising awareness and increasing the understanding of new emerging threats. Moreover, as for risk assessment, Kriaa et al. presented a comprehensive survey of existing designs and risk assessment studies that took into consideration both security and safety for industrial infrastructures [250]. McLean et al. presented a new method that identifies the risks that surround mobile agent systems [251]. Guiochet et al. adapted a classic risk assessment approach to be applied during the initial phases of the development process for autonomous systems including service robots [252]. Their analysis was based on the guide-word-based collaborative method HAZOP (HAZard OPerability), which was applied to Unified Modelling Language (UML) models. This presented risk assessment approach was applied on an assisting robot, which provided assistance for standing up, sitting down and walking, and health-state monitoring. Vuong et al. investigated physical indicators of cyber-attacks on a rescue robot [11]. Their study found how an adversely can affect rescue robots' operation and impair an emergency

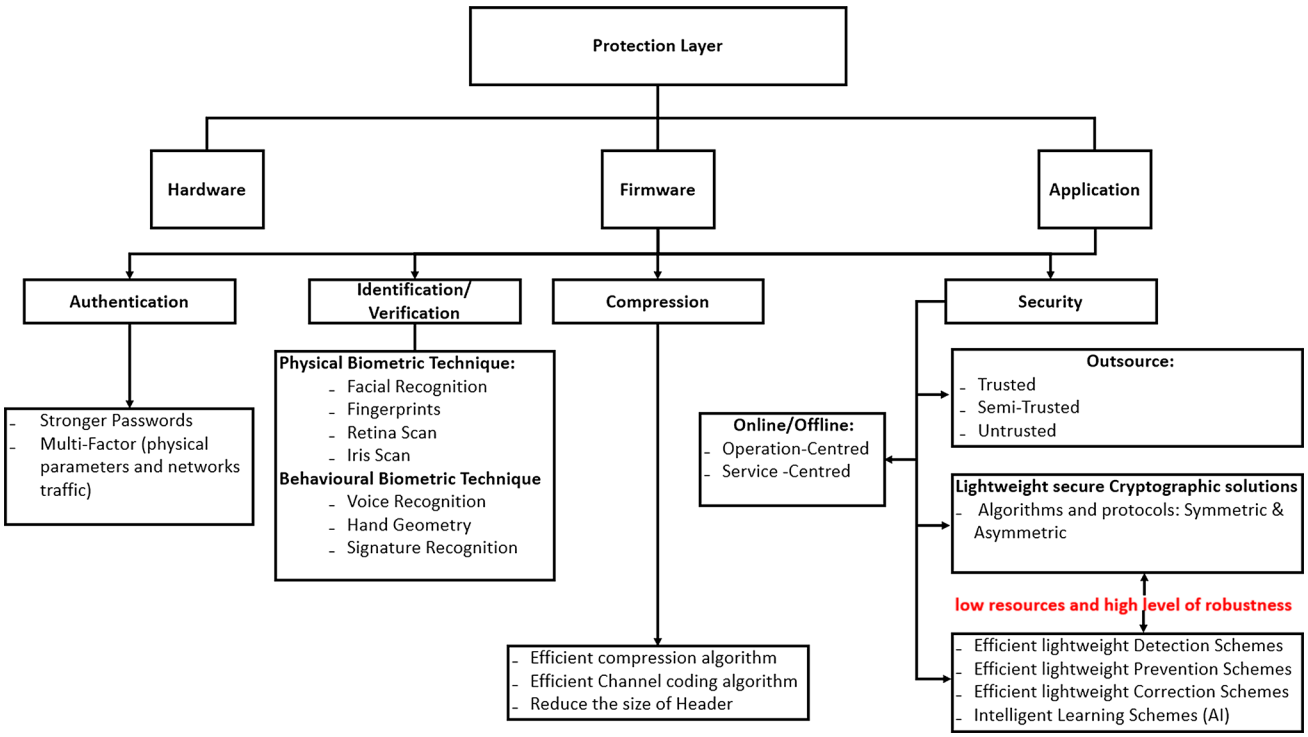

Fig. 6 Requirements to ensure security for robotics applications

response action. This paper summarizes the security measures at the application level in Fig. 6.

Moreover, Wagner et al. presented TIM, which is a large-scale flexible and transportable robotic timber construction platform [253]. TIM is location independent, reconfigurable and rapidly integrated, offering higher levels of quality and productivity. However, it lacked the security level testing, and requires further testing performance-wise. Diab et al. presented SkillMaN as a planning and execution framework using a module with experiential knowledge to integrate perception, planning, knowledge-based reasoning, and to execute various skills such as robot trajectories [254]. However, further study is also required from a cyber-security perspective. Choi et al. presented to recover robotic vehicles (RVs) from various (physical) sensor attacks, using a technique that builds a predictive state-space model based on the generic system identification technique and using sensor measurement prediction [255]. Upon attack, sensors can isolate and recover the compromised sensors to prevent further damage. The experimental results, conducted on a quad-rotor and a rover, reveal the ability to safely recover the vehicle from various attacks and prevent crashing. Beaudoin et al. presented an original software/hardware solution to obtain a universal low-level architecture for agile and easily replicable close-range remote sensing robots in different environments and on different platforms (land, surface, submarine and air) [256]. Beaudoin et al. also discussed the wise choice of Ardupilot as an autopilot and presented the ESP32 as an effective new hardware solution in terms of price and energy consumption. The experimental results revealed the easiness of tracking and achieving levels of autonomy except for flying devices. Huang et al. presented ScatterID as a lightweight system that attaches feather-light and battery-less back-scatter tags to single-antenna robots to overcome Sybil attacks [257]. The experimental results on the iRobot Create platform reveal a 96.4% accuracy level for identity verification.

5.4 Robotic system's: identification, verification and authentication

In a robotic system, both identification and verification are essential to prevent unauthorized access to the robots control machines. Hence, biometric systems and techniques are devoted to play a key role in this context. However, prior to the biometric system's set-up, there is also a need for a database to store the biometric templates safely. This allows the stored data to be used for future use [258]. Such a process is known as the enrolment process. In order to achieve identification and/or verification process, several biometric techniques are needed [259]. These biometric techniques can be divided into physical and behavioural biometric techniques [260]. Physical biometric techniques include facial recognition [261], fingerprint [262], retina [263] and iris

scan [264]. Behavioural biometric techniques are mainly based on voice recognition [260,264], hand geometry recognition [265,266] and signature recognition [260,263].

In fact, authentication is primarily used as a first defensive line that ensures the authentication of both, source and destination alike [267]. Authentication can also be based on either multi-factor authentication, where a second security mechanism is required in order to access a system in addition to the password or cryptographic first-factor authentication that requires only to enter a single password or a secret key. This makes the attack success probability low compared to only one single factor. In the following, we list several robot authentication schemes. In fact, Nguyen et al. did investigate the relationship between password protocols and other cryptographic primitives and realized that password-authenticated key exchange and public-key encryption are incomparable under black-box reductions in [268]. At first, Lamport [269] was the first to present a remote user authentication scheme using a password. Song et al. presented a dual-factor authentication scheme based on the use of smart cards [270]. Similar authentication approaches were presented for e-payment systems in [271]. He et al. presented an enhanced dual-factor user authentication scheme to protect Wireless Sensor Networks (WSNs) [272,273]. This scheme only uses hash function with a successful user authentication that uses three message exchanges. Both security and performance analysis state that it is more secure and efficient compared to other well-known authentication schemes. Das et al. presented the first smart-card-based password authentication scheme for WSNs [274]. However, the proposed solution lacks both mutual authentication and user anonymity [275]. In addition, different authentication-factor solutions have also been presented in [276], where Xue et al. presented a temporal-credential-based mutual authentication scheme among the user, Gateway Node (GWN) and the sensor node. Security and performance analysis state that this scheme offers more security features and high security level without any communication, computation and storage overhead. Moreover, Wang et al. presented a systematical evaluation framework for schemes to be assessed objectively in [277]. Evaluation results indicate that all existing schemes are not ideal. Hence, further work is required in this regard. Li et al. presented an advanced temporal credential-based security scheme with mutual authentication and key agreement for WSNs in [278]. By using lightweight one-way hashing computation, this authentication scheme significantly reduces the implementation cost against various attacks including insider attacks. Meanwhile, Gope et al. presented a realistic lightweight anonymous authentication protocol for securing real-time application data access for WSN [279]. This solution offers more security features with high security levels at a low communication and computation cost. Jiang et al. revealed that the initial temporal-credential-based authentication that was presented by Xue et al. was prone to various types of attacks, and presented a scheme that further cuts the computational cost [280]. Thus, reducing security flaws and improving performance, making them more suitable for WSN applications. Hence, Wu et al. presented an efficient two-factor authentication scheme for the single-gateway environment that achieves user anonymity, while preventing de-synchronization attacks in [281]. However, such models were not scalable enough in multi-gateway industrial WSNs, but proved to offer more security characters than Jiang et al. and Choi et al.'s schemes, especially for WSNs. As a result, Amin-Biswas presented a comprehensive lightweight user authentication and key agreement scheme for this specific purpose in [282]. Both security and performance analysis show that this scheme resists certain security weaknesses but achieves complete security requirements such as energy efficiency, user anonymity, mutual authentication, and user-friendly password change phase with more efficiency. However, this scheme is prone to spoofing attacks and offline password guessing attacks. Hence, Srinivas et al. proposed a scheme to overcome these problems in [283]. This scheme supports dynamic node addition and user friendly password change mechanisms using the BAN-logic, providing mutual authentication. The security analysis shows that this scheme is secure against the known attacks for authentication protocols including replay and man-in-the-middle attacks. However, González Muñiz and Laud stated that symmetric-key techniques were not enough to construct message recognition protocols in [284]. Moreover, the authors also presented a very strong evidence that Message Recognition Protocols (MRPs) cannot be built from "cheap" primitives using only hash functions and XORing. Hence, Kumar et al. attempted to develop a privacy-preserving two-factor authentication framework exclusively for WSNs to overcome various types of attacks in [285]. Despite this scheme having its own pros and cons, it can resist against popular attacks, and achieves better efficiency at low computation cost.

5.5 Cryptographic solutions and protocols

In fact, cryptographic protocols are used to authenticate user(s) or device(s) using cryptographic algorithms as a basic element. These elements can either be a hashing function (with or without key), or symmetric and asymmetric encryption algorithms. In fact, designing an efficient cryptographic algorithm would result in the reduction of the required latency and resources. Moreover, an efficient authentication protocol should reduce the required communication overhead. This is achieved by reducing the size of the communicated message during the authentication steps. However, improving the key management techniques and securing the ROS management layer can help to reach bet-

ter security level. In this context, symmetric cryptographic protocols are preferred since they are known to be more lightweight than asymmetric ciphers, especially with the Advanced Encryption Standard (AES) being faster than Elliptic-Curve Cryptography (ECC) in [286]. Furthermore, symmetric protocols are more energy efficient, especially when using the optimized AES block cipher. Different lightweight ciphers were presented recently and described in [19], including KATAN [287], KLEIN [288], mCrypton [289], Piccolo [290], PRESENT [291], TWINE [292], and EPCBC [293]. On the other hand, stream ciphers can be constructed by block ciphers using the Counter (CTR) and Output FeedBack (OFB) operation mode [294].

Breiling et al. presented a solution to secure Robot Operating Systems (ROS) communication channels using cryptographic methods [295]. In fact, this cryptographic method helps reducing DoS attacks. In [296], Hussein et al. introduced a Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) in the ROS core to secure the robot communication. This solution provides a fine-grained control over permissions to publish, subscribe or consume data. However, the authors did not secure the ROS master, which can be achieved via a secure channel or digital certificate [297].

Hussaini et al. presented an enhancement to the cybersecurity level of cloud data. This included the introduction of a new security model with optimal key selection, by clustering secret information with a K-Medoid clustering algorithm based on a data distance measure and encrypting the clustered data using Blowfish Encryption (BE) and stored in the cloud [298]. The testing results revealed the improved level of accuracy and maximum level of cyber-security that the confidentiality-based cloud storage framework present. Tian et al. presented a Cloud-Edge hybrid robotic system to enable dynamic, and compliant feedback control for physical human robot interactions (pHRIs) [299]. This solution was tested on various robots (i.e. Yumi, DoF, Igor and Pepper) and revealed its robustness in mitigating network latency within the Cloud-Edge perception feedback loop. Chavhan et al. presented a model that achieves mutual authentication and encryption mechanism to access to the hosted robotic services, using Kerberos module and the Elliptic Curve Integrated Encryption Scheme (ECIES) for data encryption [300]. The authors also performed a cryptanalysis test on their solution using the Proverif tool and revealed the ability of their system to overcome various security threats and attacks. Strobel et al. compared consensus protocols used in swarm robotics and showed how they fail in the presence of Byzantine (malicious) robots [301]. As a result, ARGoS–blockchain interface was presented to provide a secure robot swarm coordination via blockchain-based smart contracts as "meta-controllers", that also overcome Sybil attacks. However, further work is needed to ensure its efficiency against other robotic-related attacks. Lastly, Alcaraz et al. presented a three-layer-based interconnection architecture with a blockchain technology for Industry 4.0, to achieve a secure and reliable connection among entities [302]. Despite its advantages, it does not meet trade-off between operational performance and security, as well as the complexity in storing data.

5.6 Intrusion detection systems and firewalls

It is highly important to implement different methods of intrusion detection systems (hybrid solution). This helps increasing the level of protection and reaction against known (signature method) and unknown (specification and anomaly detection methods) threats that surround the robotic domain. In fact, different approaches were presented in this aim. This includes a synthesis technique used to build a distributed IDS to secure a class of multi-agents robots by Fagiolini et al. in [303]. Their IDS includes a decentralized monitoring mechanism and an agreement mechanism. The obtained testing results prove that the method is functional and can detect an intrusive behaviour with a good error rate (15% error). Such success is reinforced by similar systems, like the determination of behaviour in the use of credit card [304] using neural networks. This is achieved while allowing the administrators' knowledge to be easily introduced into the system in a way that new important information can be embedded to keep the data updated [305]. Another nonparametric density estimation approach was presented by Yeung et al. in [306], using Parzen-window estimators with Gaussian kernels to build an intrusion detection system using normal data only. The authors stated that despite its high computational demands during the testing phase, it does not require any training at all. Another approach named WebSTAT was presented by Vigna et al. in [307]. WebSTAT is a novel intrusion detection system that analyses web requests and searches for evidence of malicious behaviours, ensuring both flexibility and extensibility, along a much more effective web-based attack detection at a lower false positive rate. Experimental results indicate that this stateful intrusion detection can be performed on high-performance servers in a real-time manner. Onat et al. presented the mIDS, as a general methodology of an anomaly-based IDS that uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activities and to detect the malicious behaviour of the sensor node [308]. Evaluation results indicate a detection rate that ranges between 88 and 100% using routing layer attacks. This does not seem to be an ideal solution. Another approach was presented by Gudadhe et al. in [309]. This approach is a new network intrusion detection model using boosted decision trees. The generalized accuracy of the boosted decision tree was compared with different algorithms such as Naïve Bayes, k-nearest neighbour (kNN) and the testing results show that

this algorithm outperform existing algorithms when applied for real-world intrusion. Another hybrid IDS approach was presented by Om et al. in [310]. This approach combines the merits of anomaly and misuse detection to overcome the very high false alarm rate of anomaly detection. This hybrid IDS combines k-Means, K-nearest neighbour and Naïve Bayes for anomaly detection. The main drawback of their presented approach is that real-life datasets have a slightly small difference between normal and anomalous data.

In fact, the recently presented work by various authors reveals an enhanced protection version towards robotic domains. For example, Rath et al. presented a lively MANET-based automated convention called PD-ROBO with an IDS structure to overcome replay assault in mechanical based Mobile Adhoc Networks (MANETs) [311]. Results revealed its effectiveness in overcoming directing control overhead and achieving the right Quality of Service satisfaction in robotic communication. Rivera et al. presented ROS-Immunity as a solution that allows ROS users to harden their systems against attackers with low overhead, using robustness assessment, automatic rule generation, and distributed defence with a firewall [312]. This solution was also tested on a self-driving car, a swarm robotic system, and results revealed a low minimal overhead with 7–18% extra system power, a low false positive rate 8% and ability to react to stop attackers exploiting unknown vulnerabilities within 2.4 s. Zhou et al. presented a novel ensemble system based on the modified adaptive boosting with area under the curve (M-AdaBoost-A) algorithm to more effectively detect network intrusions [313]. Their mode was compared to already existing standard techniques, and it proves that it can achieve a higher performance for imbalanced multi-class data both 802.11 wireless intrusion detection and traditional enterprise intrusion detection. Gorbenko et al. discussed the problem of intrusion detection for zero-day deceptive attacks, and introduced an intrusion detection system based on an abnormal behavioural pattern detection technique for closed-loop robotic systems to detect zero-day deceptive attacks [314]. Experimental results reveal that it outperforms other solutions in detecting zero-day strictly deceptive attacks with high efficiency. Lastly, Almalawi et al. presented the Global Anomaly Threshold to Unsupervised Detection (GATUD) as an add-on anomaly threshold technique that identifies any abnormal deviation, and improves the performance of the Supervisory Control And Data Acquisition (SCADA) unsupervised anomaly detection approaches [315]. Experimental results indicate that it can achieve a significant improvement in the unsupervised anomaly detection algorithms. To resume the reviewed work, a summary is presented in Table 4.

5.7 Honeypots security solutions

Honeypots are very useful tools that supplement other security technologies in order to form a firm (see Table 5, and sophisticated defensive network security system [316]. Honeypots can be employed as a stand-alone system. In fact, they can also be employed in cooperation and collaboration with IDSs and firewalls alike, especially with their ability to detect, prevent and react.

This allows them to become a very useful deceptive tool that traps the attacker by sacrificing a given unneeded or unwanted system to server as a decoy [317]. In fact, if honeypots are employed with IDSes, they are capable of reducing both false positive and false negative rates. Moreover, they also ensure a high level of dynamicity and flexibility to respond to various types of attacks.

Therefore, different honeypot systems were presented in the literature. To solve robotic issues and problems, Irvene et al. introduced a "HoneyBot" [318]. This HoneyBot is based on a hybrid interaction honeypot which is designed specifically for robot systems. Unlike other honeypots, HoneyBot can accurately deceiving intelligent attackers through the reliance on HoneyPhy and techniques from traditional honeypots along with device models being in use. This allows the authors to fool the attackers into believing that their exploits were successful, while communication was logged to be used for attribution and threat model creation. Another type of honeypots was presented by R. Marcus, known as the Backofficer Friendly (BOF) [319]. This honeypot is a lightweight honeypot that is free for distribution. This approach ensures an accurate extraction of the essential meaning and most important aspects of honeypot's idea and insights. This allows BOF to have a clear view of the attack process, with the ability to collect logs, send alerts, in addition to responding with fake replies whenever a user connects to http, ftp, and telnet ports. Another honeypot approach was presented in [320] and is called "Specter" was developed and sold by a Swiss company called Netsec. This type of honeypots is used for commercial productions with the aim of detection. Specter is capable of simulating around roughly thirteen different OSes (including Windows and Linux), with the ability to offer around fourteen different network services and traps. This offers the chance to actively gather information about the attackers. In fact, Specter is a low interactive honeypot that fakes a given reply to the attacker's request. Another Honeypot approach named "Honeyd" was created by N. Provos and was presented in [321]. In [322], La et al. developed a game theoretic model that analyses deceptive attacks and defence problems in a honeypot enabled IoT network. Their approach uses a Bayesian belief update scheme in their repeated game. Their simulation results show that whenever facing a high concentration of active attackers, the defender's best interest was to heavily deploy honeypots.

Table 4 IDS approaches

IDS approaches	References	Advantages	Drawbacks	Characteristics
Synthesis technique used for distributed IDS	[303]	Detects new attacks, no loss of performance, reduced cost, and codifies new kinds of attack due to its good sensibility in detection of policy violation	Presence of malicious monitors that share false information that affects how systems monitor robots	Used to secure a class of multi-agents robotic, made of a decentralized monitoring mechanism and agreement mechanism
WebSTAT	[307]	Operates on multiple event streams, correlates network-level and operating system-level events with entries contained in server logs, ensures a more effective web-based attack detection at a lower false positive rate, ensuring a high performance in real-time	Possibility of higher false negative rates	Stateful IDS based on the extension of the STAT framework to detect web-based attacks, providing a sophisticated language describing multi-step attacks to ensure both flexibility and extensibility
Network IDS model	[309]	The generalized accuracy of the boosted decision tree outperformed the compared algorithms	Limited to network attacks, unsuitable for malware attacks	Network IDS model that uses boosted decision trees based on a learning technique that allows the combination of several decision trees
Parzen-Window	[306]	Does not require any training at all, can easily adapt to any data changes, along the ability to easily integrate new training examples into models without the need to retraining them from scratch	High Computational Demands	Similar characteristics to Ic-nearest-neighbour (Ic-NN) classifier
Hybrid IDS Approach	[310]	k-Means algorithm for clustering with a hybrid classifier used to overcome very high false alarm rates, fuzzy algorithms used to overcome the real-life dataset issue	Real-life datasets have a small difference between normal and anomalous data	Combines the merits of anomaly and misuse detection
Novel anomaly detection based security scheme	[308]	Low-complexity cooperative algorithms can possibly improve both detection and containment processes, nodes can effectively identify an intruder trying to impersonate a legitimate neighbour	Unable to detect different vulnerability types	Used for large scale sensor networks to exploit their stability in their neighbouring information

Table 5 Honeypots explained

Interaction level	Operational process	Deployment process	Risk level	Run process	Compromised level
Low interaction	Simulated services and applications	Simple deployment	Low risk	Not operational in any production system	Easy detection
High interaction	Relies on Operating Systems and applications alike	Complex deployment	High risk	Operational on production systems	Harder to detect
Hybrid interaction	Switching dynamically between simulators and real systems	Simple deployment	Medium risk	Operational within production systems	Harder to detect

This allows the defender to use a mixed defensive strategy that keeps the attacker's successful attack rate low. Furthermore, Honeyd is classified as an open source yet powerful honeypot production used for detection and reaction against a given attacker. Moreover, it is capable of hiding the guest's OS before the attacker detects it, with the ability to achieve or surpass 400 OS kinds at a given IP stack level. This reaches hundreds of computers and devices at a single machine use. Therefore, this allows the simulated reply to an attacker's request with the ability to customize the reply script to ensure much more flexibility against the attacker. Finally, another approach, called Honeynet, was presented by L. Spitzner in [323]. Honeynet can be modified to ensure better detection and reaction against a given attack, especially with new methods and techniques being employed and used to capture and control data. Therefore, it can ensure a higher flexibility and access control ability.

As a summary, these approaches are summarized in Table 6.

5.8 Artificial intelligence-based solutions

The choice of AI-based solutions was not only limited to perform highly accurate robotic tasks in a timely manner. In fact, the current work is now focusing on deploying AI into ensuring a highly secure robotic environment with the high accuracy and less overhead. Terra et al. presented the implementation of Fuzzy Logic System (FLS) and Reinforcement Learning (RL) to build risk mitigation modules for human–robot collaboration scenarios [324]. The testing results revealed that the presented risk mitigation strategies improve the safety aspect and the efficiency by 26% from the default setup. Wang et al. presented the main security threats for autonomous mobile robots and how to overcome them [325]. As a result, RoboFuzz was presented to automatically perform directed fuzzing sensor values at appropriate occasions, leading robots to a compromised state. The testing results indicate that concrete threats can be imposed to robots at a success rate of 93.3%, with a loss of work efficacy reaching 4.1% in mitigation mode. Bykovsky presented the minimization of Multiple-Valued Logic (MVL) functions for the analysis of aggregated objects [326]. To ensure the full use of MVLs, a heterogeneous network architecture was also presented using three allocated levels of AI such as logic modelling for discrete multiple-valued logic, Boolean logic, and fuzzy logic. This solution aims to provide additional secret coding, data aggregation, data protection and communications for network addressing and the targeted control of robotic devices. Alamer presented a Secure Anonymous Tracing (SAT) fog-assisted method that supports the tracing of Internet of Robotic Things (IoRT) through a Fog Computing (FC) network system [327]. SAT is based on the Counting Bloom Filter (CBF) method and the Elliptic Curve Cryptography (ECC) technique. Both analysis and evaluation results reveal the effectiveness of SAT especially in terms of false positive rate, memory cost and query running time consumption in a secure manner.

6 Security requirements, recommendations, and future research directions

Based on the reviewed works, we found that various security requirements are still needed to be studied, conducted and analysed to enhance the discussed security countermeasures and the recommendations for future research directions. A very limited number of presented work included managing the security aspect of robotics during the design phase, and many focused on how to maintain the privacy and confidentiality through encryption without taking into consideration the source authentication and data integrity part through the use of strong keyed hash mechanism (e.g. HMAC) or by using authentication operation mode such as Cipher-based Message Authentication Code (CMAC) and Galois Message Authentication Code (GMAC) [328].

On the other hand, only a handful number of papers discussed the use of forensics [329,330]. Consequently, a further advanced attention is required to reveal the event prior the exploitation of a given robotic system through the conduction of a specialized robotic digital forensic investigation. No research was based on the adoption of self-healing robotic system to overcome any possible power/system failure with systems serving as back up. Therefore, many aspects require further studies and deeper understanding to secure robotic systems in all forms, aspects and domains. Therefore, in this section, we include the main requirements for ensuring the robotics domain security. In addition, we present our recommendations for possible security enhancements and future research directions.

6.1 Security requirements

It is essential to ensure the security of robot's wireless communications through the implementation of various security mechanisms. This maintains secure communication and ensures authentication, integrity, confidentiality, and availability [331].

6.1.1 Adaptive security

This paper found that it is important to ensure and implement an active and adaptive security solution. This adaptive security solutions can be divided into two main types, threat-centred or data-centred to know what data to secure, and against whom the data must be secured [332].

Table 6 Presented honeypot approaches

Honeypot approaches	References	Advantages	Drawbacks	Characteristics
HoneyBot	[318]	Accurately deceives intelligent attackers	Limited to users with no physical or visual access to the robotic system	Hybrid interaction, specifically designed for robotic systems
Backofficer friendly	[319]	Having a clear view of the attack process, collecting logs, sending alerts and fake replies to the attacker	Limited to detecting attacks on seven ports only	Lightweight honeypot, free for distribution
Specter	[320]	Simulates thirteen different OSs, and offers fourteen different networks services and traps, actively gather information about the attackers and fakes a given reply to their request	Limited detection activity on only 14 TCP ports, prone to IP/Port Snorting	low interactive honeypots used for commercial productions for detection purposes
Honeyd	[321]	Reporting bugs and source code, creates virtual hosts on a network, where hosts can be configured to run arbitrary services	Adversary never gains access to a complete system despite compromising a simulated service	Open source virtual yet powerful honeypot production used for detection and reaction against a given attacker
Honeynet	[323]	Can be modified to ensure a better detection and reaction against a given attack, with new methods to capture and control data	Attackers can fingerprint the honeynet and launch attacks in the outbound limits	Highest honeypot research level, and high interaction honeypot

- *Threat-centred* evaluates threats in order to employ the right security measures. If there is no risk, security measures should not be applied in order to reduce unnecessary resources cost. In fact, [19] presented a threat-centred adaptive security solution.
- *Data-centred* this approach ensures that data sensitivity must be evaluated first, focusing on which data needs to be secured instead of evaluating the threat level [19].

6.1.2 Outsource security

Outsource security delegates heavy operations to powerful devices, while also using cryptographic aiders. Moreover, it can ensure three main assistance modes including trusted assistance, semi-trusted assistance, and untrusted assistance. As a result, applications using this security type rely on the environmental deployment by assisting devices that are available and accessible to the constrained node [19,333]. In fact, the use of aiders helps computing expensive operations by carrying intensive computations and reducing energy consumption, or by dividing the execution of cryptographic algorithm to be done locally by being less intensive.

6.1.3 Trusted assistance outsource security

Trusted assistance outsource security relies on trusted assistants, where heavy operations can be assigned to a specific assistant by preserving security and privacy to maintain the systems availability [19]. This includes relying on Rivest–Shamir–Adleman (RSA) and Extended Tiny Encryption Algorithm (XTEA) protocols [334], along the use of Trusted Platform module (TPM) for WSNs [335,336]. However, such operations can be really expensive in terms of cost and maintenance.

6.1.4 Semi-trusted assistance outsource security

"Semi-trusted" is based on an entity that correctly performs its assigned task to maintain confidentiality by preventing the disclosure of sensitive information. It includes the ability to learn more about the essential information that should be secured, where nodes rely on unconstrained accessible devices due to the unavailability of hardware equipment. This allows storing the encrypted data in a remote server [337, 338] using Key Ciphertext-Policy Based Encryption (CP-ABE) [333] and Key Police-Attribute Based Encryption (KP-ABE) [339].

6.1.5 Untrusted assistance outsource security

The main objective of this approach is to ensure the systems' accuracy. However, the main challenges are based on the possibility of a robot or device being prone to misconfiguration or software bugs. This may lead to inaccurate results as an outcome. Therefore, the aim is to ensure the results' accuracy by detecting any possible failure [340].

6.1.6 Online/offline security

Online/Offline security concept is based on transforming cryptographic schemes into two main phases [19]. The first phase is the offline phase, where the message is encrypted before initiating the security service and before identifying the destination. This phase reduces the online cryptographic overhead by producing the ciphertexts and storing them. This, consequently, reduces the required online latency. The second phase is performed online, using the stored results in the offline phase. Thus, this phase should be fast [341,342]. However, the online/offline approach might be difficult to employ and apply, especially with heavy operations being related to unknown and unidentified data.

6.1.7 Low power security

Low-power security protocols offer an alternative solution for heavy cryptosystems, since they provide the necessary basis to build up energy-efficient security services. Thus, they reduce energy consumption by relying on low-power protocols [19]. As a result, various optimized low-power asymmetric cryptosystems were presented in [343–345] including the use of Elliptic-Curve Cryptography (ECC) and the open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data (NTRU) operations. However, designing an efficient lightweight and robust cryptographic protocol for robotic applications, that require low communication, delay, and resources overheads, is not a straightforward task (trade-off between security level and performance).

6.1.8 Physical layer security

A new approach has emerged in the physical layer research domain towards benefiting from it to enhance security [19, 346,347]. In fact, Physical Layer Security (PLS) is an emerging paradigm employed to enhance wireless network security without relying on hnoura2021secureigher-layer encryption techniques. PLS enables legitimate users to exchange confidential messages over a secure wireless medium. This is done by utilizing the main properties and characteristics of the wireless channel. The main objective is to apply security approaches at the physical layer with lesser energy consumption. Therefore, PLS is very suitable for resource-constrained networks, such as in the Industrial IOT (IIoT) and IoT cases in [348,349].

Physical layer encryption schemes were presented in [350–352] and a dynamic key is obtained by hashing the

mixing of a nonce obtained from the hash of certain physical parameters and a secret key to produce a dynamic key. This solution introduces the dynamicity into physical cryptographic algorithms by updating cryptographic primitives for each new input frame. This can be applied to design new lightweight cryptographic primitives at the physical layer, which is useful for robots as the connection between robots and network server can be realized by wireless communication means (star topology).

6.2 Recommendations

In order to enhance the level of robots security, it is essential to take the following cyber-security measures into account:

- *Securing robots by design* manufacturers should take security as a key component in the development of any firmware, hardware and application. Such a move should be achieved by the implementation of strongly secure cryptographic mechanisms.
- *Enhanced policies* the adoption of authorization and authentication policies prevents unauthorized entities from accessing the robotic system, which makes it less prone to insider threats.
- *Real-time isolation* the need to implement mechanisms that instantly disconnect or/and turn off the robot once a security threat is detected. This can ensure that robots will not be controlled by an adversary, which prevents any damage from occurring, as well as avoids injuries or/and death. To do so, there is a need for a self-destructive chip to be implemented in each robot, which can either be software or hardware.
- *Enhanced testing phase* robots must undergo a regular testing phase in order to evaluate their security threat level on human's life. This is the case when robots fall into the wrong hands.
- *Application testing* the security of the applications that control the robots must be tested. This helps detecting any exploitable vulnerability or security gap, and fixing it as soon as possible. In fact, this can be realized by designing automated robotic penetration tests.
- *Enhanced forensics* ROS forensics are not being given a great importance in order to trace back and reconstruct any possible attack event(s) [329,353,354]. This also includes network forensics analysis to match patterns, identify streams and examine data [330].
- *Safer robotic designs* robots and robotics must undergo a safety test before and after achieving the required design to reduce the occurrence of any potential risk that may prove being harmful or lethal against any human operator(s).
- *Smarter robotic designs* smarter designs must be adopted to reduce any false negatives and false positives that may affect the accuracy of the assigned task(s), and to ensure that tasks are performed in a real-time manner with no latency.
- *Quantum powered robots* may be adopted in the near future. This can be done via the emergency of cloud-based quantum computing services and Quantum Co-Processors (QPUs) to operate with classic CPUs for the development of more "intelligent" robots.
- *Simpler designs* must also be adopted to prevent any design complexity that renders the robotics' use as either complex for human operators, or/and difficult to adopt on a given system.
- *By-customers design* robots must be designed and developed in a manner that allows their adoption as an answer to the customers' need(s) to enhance productivity, reduce cost and reduce wasted time.
- *Efficient robotic deployment* is required based on the lessons learnt from previous experiences especially in industrial, agricultural, military/law enforcement and medical fields. This primarily includes how to ensure an efficient adoption and use of robots to combat pandemics via early detection, disinfection and protection (i.e. H1N1 and H3N2 influenza viruses, Zika, Ebola, and COVID-19 or SARS-CoV-2).
- *Smart self-healing processing* must be adopted by-design phase or added at a later development stages to ensure that robots are then capable of overcoming a variety of attacks in a "smart" manner that allows them to recover and re-operate normally by identifying the affected node and isolating it to prevent further damage.
- *Multi-tasking robots* Robots should perform a variety of tasks and not limited to a single aspect to allow them to further operate and cover wider activities which are deemed by humans as repetitive and labour-intensive.
- *Human–machine interaction* must be adopted to ensure a much more balanced cooperation and equal collaboration between both humans and machines to ensure a higher rate of high quality production in a safe and timely manner.

In Fig. 7, we summarize the security requirements and recommendations.

6.3 Future research directions

In addition to AI, the advanced information and communication technology has revolutionized robotic domains. Security is a serious requirement, since a given attacker (i.e. hacker) can maliciously exploit these robots, which in turn, can lead to a complete or partial control of robots or robotic systems. Therefore, we present several potential research directions in the following to improve robotic security :

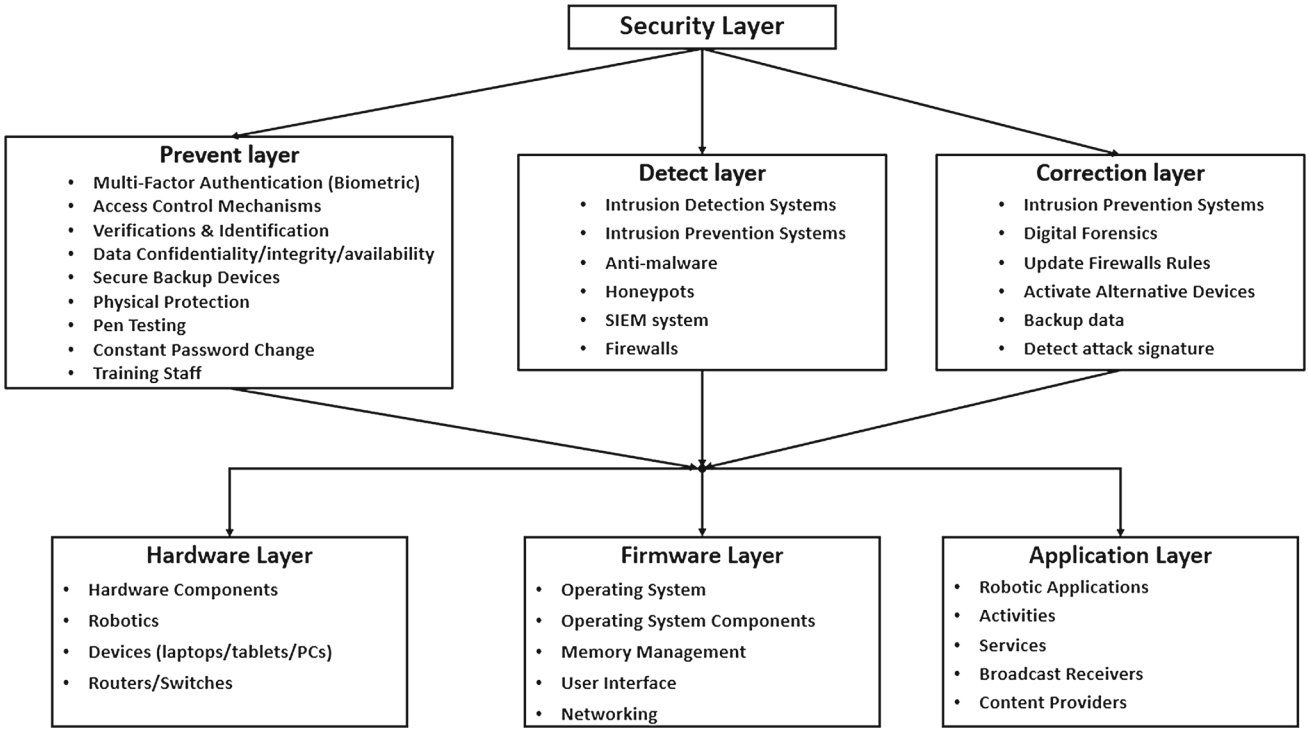

Fig. 7 Recommended security layer

(1) *New lightweight host/network IDS/IPS* developing a lightweight efficient IDS that employs anomaly-based techniques, as a part of the detection method, is crucial to detect unknown attacks in the robotic context. These lightweight IDS techniques can be used to make prompt decisions in a resource-constrained environment or real-time applications such as robotic applications. Without an efficient IDS, robots could be compromised leading to drastic consequences for individuals, companies, cities, and even countries. This has raised a huge security concern about current robotics deployments and the necessity for having a lightweight and robust IDS that can combine hybrid anomaly detection techniques (statistical and ML approaches) in addition to signature-based and specification-based detection methods. This can help the IDS to make the right decisions, especially for real-time robotics applications. More research work should focus on designing new efficient anomaly classification that can reach a good balance between performance and detection accuracy.

(2) *New lightweight multi-factor authentication scheme* the most widely used authentication mechanism in robotic systems is the one-factor authentication scheme, that is based on existing cryptographic authentication key approaches. These approaches include pre-shared, asymmetric, and public-key infrastructure (PKI). However, the asymmetric key techniques might not be practical in the context of limited robotic devices. Additionally, the pre-shared password suffers from different security issues. Accordingly, any weakness in the identification/authentication schemes would allow a compromised robot to launch dangerous attacks (e.g. data injection), which can potentially lead to drastic effects on the functions of the robotic system.
To solve such issues, a combination between lightweight cryptographic and non-cryptographic-based authentication protocols should be used to avoid any potential illegal access as presented in [355,356]. More research work should focus on designing new efficient multi-factor authentication that reach best balance between performance and authentication accuracy.

(3) *Lightweight multi-factor cryptographic algorithms (block cipher and hash function)* in fact, designing a multi-factor cryptographic algorithms for robotic communications would lead to increase the data confidentiality, integrity and source authentication level [352,357,358], since any legal entity should have all factors (for example to encrypt/decrypt) the communicated data. Moreover, recent approaches use common channel parameters as "you know" factor and the secret key as "you have" factor [350,351]. These factors are used to produce a dynamic key since wireless channel parameters change in a random manner. Moreover, the proposed cipher should require low latency and resources. This can be attained by using the one round cipher approach, where cipher requires only one round and with a minimum

number of operations [359–363]. We think that modern cryptographic algorithms should use the dynamic cryptographic primitives approach to reach a good balance between security and performance level [364]. New research work should be presented towards reaching the best balance between performance, security and real implementations [365].

(4) *Lightweight crypto-compression* since a huge amount of real-time data is being constantly transmitted between a robot and the control centre or cloud services using open wireless communications, compression is mandatory for any communication system since it reduces the size of transmitted or stored data. In fact, three main crypto-compression techniques exist in the literature, which are: pre-compression, in-compression, and post-compression. In fact, the pre-compression class degrades the compression efficiency. While in-compression class depends on the compressor and requires a modification in the standard, the post-compression class is more efficient since it preserves the compression efficiency independently of the compressor. Moreover, a recent post-selective image crypto-compression scheme was presented in [366,367]. It consists of selecting randomly (uniform distribution) only 5% of the compressed data to reach a high visual degradation.

(5) *Intelligent security* while AI can play an essential role in enabling innovative robotics applications, it is devoted to play also a key role in securing robot network communications. AI-based IDS and traffic classification schemes have been presented in the literature. Recently, a non-cryptographic device authentication scheme was presented in [368,369] and it is based on the network generated traffic. The presented solution uses an intelligent authentication factor ("you are"), that can help in reducing the false positive detection rate (illegal access probability), if combined with another factor(s) ("you know" and "you have"). Moreover, different security solutions can benefit from AI to enhance robots security level. In fact, AI can be used for different modern security functions in the robotics domain, and it is not only limited to user/device authentication and IDS-anomaly detection solutions.

7 Conclusion

Nowadays, robotic systems are being deployed and used in different domains that are based on critical infrastructures. However, robotic systems suffer from several security vulnerabilities that can be exploited to launch dangerous attacks, which may have drastic consequences on these infrastructures escalating from economical losses all the way to the loss of human lives. Such attacks are possible due to the lack of security by design of robotic systems and the reliance on open wireless communication channels. As such, it is highly recommended to protect robots from any possible attack and by all means necessary. This includes detecting and preventing attackers from breaching into these systems to inject malicious malware or/and data to cause either chaos and havoc in the robots' operation, or to leak sensitive information (industrial espionage). Therefore, the authentication process should be designed to reach the highest possible security level by employing mutual multi-factor authentication scheme. This helps in reducing the illegal access to robots/users. On the other hand, lightweight cryptographic algorithms and protocols at the network and/or at the physical layer are mandatory to ensure secure wireless communication with minimal overhead in terms of delay and required resources. Moreover, privacy-preserving techniques should be used to ensure the privacy of legal entities. Moreover, non-cryptographic solutions such as lightweight intrusion detection or prevention systems should be designed to better protect the robotics applications. At the end of this paper, we have discussed the security requirements and have presented several recommendations for such requirements within robotic systems. As part of future work, we plan to shed more light over the main topics that are yet to be covered, including the design of anti-forensic solutions to maintain the integrity of availability of evidences.

Funding This research is supported by the Maroun Semaan Faculty of Engineering and Architecture at the American University of Beirut and by the EIPHI Graduate School (Contract "ANR-17-EURE-0002").

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., Harnisch, M.: Industry 4.0: the future of productivity and growth in manufacturing industries. Boston Consult. Group **9**(1), 54–89 (2015)
2. Bahrin, M.A.K., Othman, M.F., Nor Azli, N.H., Talib, M.F.: Industry 4.0: a review on industrial automation and robotic. J. Teknol. **78**(6–13), 137–143 (2016)
3. Pfeiffer, S.: Robots, industry 4.0 and humans, or why assembly work is more than routine work. Societies **6**(2), 16 (2016)
4. Shyvakov, O.: Developing a security framework for robots. Master's thesis, University of Twente (2017)
5. Simoens, P., Dragone, M., Saffiotti, A.: The internet of robotic things: a review of concept, added value and applications. Int. J. Adv. Robot. Syst. **15**(1), 1729881418759424 (2018)

6. Chui, M., Manyika, J., Miremadi, M.: Where machines could replace humans-and where they can't (yet). McKinsey Q. **7**, 1–6 (2016)
7. Kirschgens, L.A., Ugarte, I.Z., Uriarte, E.G., Rosas, A.M., Vilches, V.M.: Robot hazards: from safety to security (2018). arXiv preprint arXiv:1806.06681
8. Guerrero-Higueras, Á.M., DeCastro-Garcia, N., Matellan, V.: Detection of cyber-attacks to indoor real time localization systems for autonomous robots. Robot. Auton. Syst. **99**, 75–83 (2018)
9. Petit, J., Shladover, S.E.: Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. **16**(2), 546–556 (2015)
10. Cerrudo, C., Apa, L.: Hacking robots before skynet. Cybersecurity Insight, IOActive Report, Seattle, USA (2017)
11. Vuong, T., Filippoupolitis, A., Loukas, G., Gan, D.: Physical indicators of cyber attacks against a rescue robot. In: 2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 338–343. IEEE (2014)
12. Dash, P., Karimibiuki, M., Pattabiraman, K.: Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. J. Digit. Threats Res. Pract. **2**(1), 1–25 (2021)
13. Chowdhury, A., Karmakar, G., Kamruzzaman, J.: Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In: Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications, pp. 1426–1441. IGI Global (2019)
14. Lacava, G., Marotta, A., Martinelli, F., Saracino, A., La Marra, A., Gil-Uriarte, E., Vilches, V.M.: Current research issues on cyber security in robotics (2020)
15. Mitchell, R., Chen, I.-R.: A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. (CSUR) **46**(4), 55 (2014)
16. Kehoe, B., Patil, S., Abbeel, P., Goldberg, K.: A survey of research on cloud robotics and automation. IEEE Trans. Autom. Sci. Eng. **12**(2), 398–409 (2015)
17. Chowdhury, A., Karmakar, G., Kamruzzaman, J.: Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In: Detecting and Mitigating Robotic Cyber Security Risks, pp. 284–299. IGI Global (2017)
18. Jeong, S.-Y., Choi, I.-J., Kim, Y.-J., Shin, Y.-M., Han, J.-H., Jung, G.-H., Kim, K.-G.: A study on ros vulnerabilities and countermeasure. In: Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human–Robot Interaction, pp. 147–148. ACM (2017)
19. Hellaoui, H., Koudil, M., Bouabdallah, A.: Energy-efficient mechanisms in security of the internet of things: a survey. Comput. Netw. **127**, 173–189 (2017)
20. Guiochet, J., Machin, M., Waeselynck, H.: Safety-critical advanced robots: a survey. Robot. Auton. Syst. **94**, 43–52 (2017)
21. Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., Schartner, P.: Security for the robot operating system. Robot. Auton. Syst. **98**, 192–203 (2017)
22. Alcaraz, C., Cazorla, L., Lopez, J.: Cyber-physical systems for wide-area situational awareness. In: Cyber-Physical Systems, pp. 305–317. Elsevier (2017)
23. Rubio, J.E., Alcaraz, C., Roman, R., Lopez, J.: Current cyber-defense trends in industrial control systems. Comput. Secur. **87**, 101561 (2019)
24. Jahan, F., Sun, W., Niyaz, Q., Alam, M.: Security modeling of autonomous systems: a survey. ACM Comput. Surv. (CSUR) **52**(5), 1–34 (2019)
25. Chen, J., Li, K., Zhang, Z., Li, K., Yu, P.S.: A survey on applications of artificial intelligence in fighting against covid-19 (2020). arXiv preprint arXiv:2007.02202
26. Brem, A., Viardot, E., Nylund, P.A.: Implications of the coronavirus (covid-19) outbreak for innovation: which technologies will improve our lives? Technol. Forecast. Soc. Change **163**, (2020)
27. Khan, F.N., Khanam, A.A., Ramlal, A., Ahmad, S.: A review on predictive systems and data models for covid-19. In: Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis, pp. 123–164. Springer (2020)
28. Fan, D., Li, Y., Liu, W., Yue, X.-G., Boustras, G.: Weaving public health and safety nets to respond the covid-19 pandemic. Saf. Sci. **134**, 105058 (2020)
29. Bokolo Anthony Jnr: Use of telemedicine and virtual care for remote treatment in response to covid-19 pandemic. J. Med. Syst. **44**(7), 1–9 (2020)
30. Yaacoub, J.-P.A., Noura, H.N., Salman, O., Chehab, A.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things **11**, 100218 (2020)
31. Wang, H., Cheng, H., Hao, H.: The use of unmanned aerial vehicle in military operations. In: International Conference on Man–Machine–Environment System Engineering, pp. 939–945. Springer (2020)
32. Kamel, M.A., Yu, X., Zhang, Y.: Formation control and coordination of multiple unmanned ground vehicles in normal and faulty situations: a review. Annu. Rev. Control **49**, 128–144 (2020)
33. Nandyal, A.A., Adithya, D.M., Karthik, K., Manikantan, G., Sudha, P.N.: A literature survey on "unmanned underwater vehicle for monitoring aquatic ecosystem". Int. J. Eng. Appl. Sci. Technol. **5**(2), 599–601 (2020). (**ISSN: 2455-2143**)
34. He, Y., Wang, D.B., Ali, Z.A.: A review of different designs and control models of remotely operated underwater vehicle. Meas. Control, p. 0020294020952483 (2020)
35. Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M.: Cyber-physical systems security: limitations, issues and future trends. Microprocess. Microsyst. **77**, 102019 (2020)
36. Yaacoub, J.P.A., Fernandez, J.H., Noura, H.N., Chehab, A.: Security of power line communication systems: issues, limitations and existing solutions. Comput. Sci. Rev. **39**, 100331 (2021)
37. Yaacoub, J.-P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., Chehab, A.: Securing internet of medical things systems: limitations, issues and recommendations. Future Gener. Comput. Syst. **105**, 581–606 (2020)
38. Gogu, G., Ray, P., Neagoe, M., Gogu, G., Diaconescu, D., Pocola, A.G., Pop, D.O., Petra, C.: Robotics and manufacturing. In: Talaba, D., Roche, T. (eds.) Product Engineering: Eco-Design, Technologies and Green Energy, p. 348. Springer, Cham (2006)
39. Kadir, M.A.: Role of telemedicine in healthcare during covid-19 pandemic in developing countries. Telehealth Med, Today (2020)
40. Beasley, R.A.: Medical robots: current systems and research directions. J. Robot. (2012)
41. Rosen, J., Hannaford, B.: Doc at a distance. IEEE Spectr. **43**(10), 34–39 (2006)
42. Cheein, F.A.A., Carelli, R.: Agricultural robotics: unmanned robotic service units in agricultural tasks. IEEE Ind. Electron. Mag. **7**(3), 48–58 (2013)
43. Murphy, R.R., Tadokoro, S., Nardi, D., Jacoff, A., Fiorini, P., Choset, H., Erkmen, A.M.: Search and rescue robotics. In: Siciliano, B., Khatib, O. (eds.) Springer Handbook of Robotics, pp. 1151–1173. Springer, Berlin (2008)
44. Murphy, R.R., Tadokoro, S., Kleiner, A.: Disaster robotics. In: Siciliano, B., Khatib, O. (eds.) Springer Handbook of Robotics, pp. 1577–1604. Springer, Berlin (2016)
45. Stager, P.: Visual search capability in search and rescue(sar) (1974)
46. McKirdy, E.: Thailand cave rescue: boys appear in new video, 'i am healthy' (2018)

47. Naghsh, A.M., Gancet, J., Tanoto, A., Roast, C.: Analysis and design of human–robot swarm interaction in firefighting. In: The 17th IEEE International Symposium on Robot and Human Interactive Communication, 2008. RO-MAN 2008, pp. 255–260. IEEE (2008)
48. Hong, J.H., Matson, E.T., Taylor, J.M.: Design of knowledge-based communication between human and robot using ontological semantic technology in firefighting domain. In: Robot Intelligence Technology and Applications, vol. 2, pp. 311–325. Springer (2014)
49. Mansour, H., Bitar, E., Fares, Y., Makdessi, A., Maalouf, A., El Ghoul, M., Mansour, M., Chami, A., Khalil, M., Jalkh, A., et al.: Beirut port ammonium nitrate explosion. SSRN (2020)
50. Cheaito, M.A., Al-Hajj, S.: A brief report on the beirut port explosion. Mediterr. J. Emerg. Med, Acute Care (2020)
51. Oxford Analytica. Beirut blast could bring hunger, disease and fury. Emerald Expert Briefings (2020)
52. Stennett, C., Gaulter, S., Akhavan, J.: An estimate of the TNT-equivalent net explosive quantity (NEQ) of the Beirut port explosion using publicly-available tools and data. Propellants Explos, Pyrotech. **45**(11), 1675–1679 (2020)
53. Thielman, S.: Use of police robot to kill Dallas shooting suspect believed to be first in US history. The Guardian (2016)
54. Ringrose, K., Ramjee, D.: Watch where you walk: law enforcement surveillance and protester privacy. Calif. L. Rev. Online **11**, 349 (2020)
55. Schulte, P.: Future war: Ai, drones, terrorism and counterterror. In: Handbook of Terrorism and Counter Terrorism Post 9/11. Edward Elgar Publishing (2019)
56. Zych, J.: The use of weaponized kites and balloons in the Israeli-Palestinian conflict. Secur. Def. Q. **27**(5), 71–83 (2019)
57. Engberts, B., Gillissen, E.: Policing from above: drone use by the police. In: The Future of Drone Use, pp. 93–113. Springer (2016)
58. Shachtman, N.: Military stats reveal epicenter of us drone war. Wired. com **9** (2012)
59. Wilson, C.: Improvised explosive devices in Iraq: effects and countermeasures. In: CRS Report for Congress, Library of Congress Washington DC Congressional Research Service (2005)
60. Lesley-Dixon, K.: Northern Ireland: the troubles: from the provos to the det, 1968–1998. Pen and Sword (2018)
61. Miller, D.: Rethinking Northern Ireland: Culture. Ideology and Colonialism. Routledge, London (2014)
62. Krishnan, A.: Killer Robots: Legality and Ethicality of Autonomous Weapons. Routledge, London (2016)
63. Barboza, A.R.: The Irish Republican Army: an examination of imperialism, terror, and just war theory. Master's thesis, California Polytechnic State University, San Luis Obispo (2020)
64. Karnozov, V., et al.: Russia and Turkey put their latest equipment to the test in Syria. Def. Rev. Asia **14**(2), 20 (2020)
65. Zoltán, Ő.: Special features of the Russian-Ukrainian armed conflict. Hadmérnök **15**(1), 207–220 (2020)
66. Okpaleke, F., Burton, J.: 9 US grand strategy and the use of unmanned aerial vehicles during the George W. Bush administration. In: Emerging Technologies and International Security: Machines, the State, and War, p. 153 (2020)
67. Scipanov, L.V., Dolceanu, D.: The opportunity for using remotely operated underwater vehicles in support of naval actions. Bull. Carol I Natl. Def. Univ. **9**(3), 62–68 (2020)
68. Siwek, M., Wacławik, K.: Legal aspects of production and operation of autonomous combat robots. Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa, **11** (2020)
69. Thornton, R., Miron, M.: Towards the 'third revolution in military affairs' the Russian military's use of AI-enabled cyber warfare. RUSI J. **165**, 1–10 (2020)
70. Abiodun, T.F., Taofeek, C.R.: Unending war on boko haram terror in northeast Nigeria and the need for deployment of military robots or autonomous weapons systems to complement military operations. Journal DOI **6**(6) (2020)
71. Westerheijden, V.R.: Remote warfare comes home: an inquiry in the Dutch government's development of discourse on airstrikes and drones between 1998–2020. Master's thesis, Utrecht University (2020)
72. Oxford Analytica: Uae's bolstering of Libya's haftar is a risky policy. Emerald Expert Briefings (oxan-db) (2020)
73. Milan, F.F., Tabrizi, A.B.: Armed, unmanned, and in high demand: the drivers behind combat drones proliferation in the Middle East. Small Wars Insurgencies **31**(4), 730–750 (2020)
74. Gallagher, K.: Killer optics: exports of Wescam sensors to Turkey (2020)
75. Clark, M., Yazici, E.: Erdogan seeks to upend kremlin-backed status quo in Nagorno-Karabakh. Institute for the Study of War, p. 1 (2020)
76. Tol, T., et al.: Transitions online_around the bloc-Tuesday, 27 October 2020. Transitions Online (11/02):9–11 (2020)
77. Khan, N., Fahad, S., Naushad, M., Faisal, S.: Analysis of Arminia and Azerbijan war and its impact on both countries economies. Available at SSRN 3709329 (2020)
78. Jenzen-Jones, N.R.: Understanding the threat posed by cots small UAVs armed with CBR payloads. In: 21st Century Prometheus, pp. 179–204. Springer (2020)
79. Kaya, E.K.: Walking a fragile path: assessing the idlib demilitarization deal (2018)
80. Sadat, S.A.: Iran ties to the Palestinian Islamic resistance movement with emphasis on the Islamic Jihad Movement (PIJ), pp. 77–105 (2016)
81. Bendett, S.: Battle robots rivalry and the future of war (2019)
82. Brookes, P.: The growing Iranian unmanned combat aerial vehicle threat needs us action. Herit. Found. Backgr. **3437** (2019)
83. Sims, A.: The rising drone threat from terrorists. Georget. J. Int. Aff. **19**, 97–107 (2018)
84. Rossiter, A.: Bots on the ground: an impending UGV revolution in military affairs? Small Wars Insurgencies **31**(4), 851–873 (2020)
85. Chávez, K., Swed, O.: Off the shelf: the violent nonstate actor drone threat. Air Space Power J. **29**, 29 (2020)
86. Vogiatzis, D.: The way to the promised land or the door to Armageddon: how severe are the threats against the physical security of israeli offshore gas platforms? Naval Postgraduate School, Monterey, CA. Ph.D. thesis (2020)
87. Borg, S.: Assembling Israeli drone warfare: loitering surveillance and operational sustainability. Security Dialogue, p. 0967010620956796 (2020)
88. Benjamin, G.: Drone culture: perspectives on autonomy and anonymity. AI & SOCIETY, pp. 1–11 (2020)
89. Popister, F., Steopan, M., Pusca, A.: Surveillance robot for military use. Acta Tech. Napocensis-Ser. Appl. Math. Mech. Eng. **63**(3) (2020)
90. Fishman, J., Kuperwasser, Y.: Willful blindness and the mistake of underestimation: the Oslo gamble. Natl. Resili. Polit. Soc. **2**(1), 9–50 (2020)
91. Marcus, R.D.: Learning 'under fire': Israel's improvised military adaptation to Hamas tunnel warfare. J. Strateg. Stud. **42**(3–4), 344–370 (2019)
92. Michael, K., Dostri, O.: The Hamas military buildup. The crisis of the Gaza strip: a way out (Tel Aviv: INSS, 2017), pp. 49–60 (2019)
93. White, J.: The combat performance of Hamas in the Gaza war of 2014. CTC Sentin **7**(9), 9–13 (2014)
94. Gillespie, P.G.: Weapons of choice: the development of precision guided munitions. The University of Alabama Press, Tuscaloosa (2006)

95. Fink, A.H., Wilson, W.A., Holte, R.T.: System and methods for countering satellite-navigated munitions, December 20 2016. US Patent 9,523,773
96. Ahner, D., McCarthy, A.: Response surface modeling of precision-guided fragmentation munitions. J. Def. Model. Simul. **17**(1), 83–97 (2020)
97. O'Donohue, Commander Mark: Autonomous underwater vehicles. Niobe Papers **9**(11) (2020)
98. Keane, J., Joiner, K.: Experimental test and evaluation of autonomous underwater vehicles. Aust. J. Multi-Discip. Eng. **16**(1), 67–79 (2020)
99. Nasu, H., Letts, D.: The legal characterization of lethal autonomous maritime systems: warship, torpedo, or naval mine? Int. Law Stud. **96**(1), 4 (2020)
100. Mvelle, G.: Fighting piracy in the gulf of guinea: small states' pursuit of strategic autonomy. Revue internationale et strategique **2**, 35–46 (2020)
101. Broohm, D.A., Wang, G., Gao, J.: Maritime security: a new strategy for merchant shipping to avoid piracy in the Gulf of Guinea. Open J. Soc. Sci. **8**(5), 392–410 (2020)
102. Grasso, R., Braca, P., Osler, J., Hansen, J.: Asset network planning: integration of environmental data and sensor performance for counter piracy. In: 21st European Signal Processing Conference (EUSIPCO 2013), pp. 1–5. IEEE (2013)
103. Karahalios, H.: Appraisal of a ship's cybersecurity efficiency: the case of piracy. J. Transp. Secur. **13**, 1–23 (2020)
104. AU African Union, COIN Counterinsurgency, and CT Counterterrorism. Ctf counter terrorist financing ctf 150 combined task force 150 cwc chemical weapons convention dfg deutsche forschungsgemeinschaft/German research foundation
105. Beccaro, A.: Isis in mosul and sirte: differences and similarities. Mediterr. Polit. **23**(3), 410–417 (2018)
106. Bunker, R.J.: Keshavarz. Terrorist and insurgent teleoperated sniper rifles and machine guns, Alma (2016)
107. Beccaro, A.: Isis in Libya and beyond, 2014–2016. J. N. Afr. Stud. 1–20 (2020)
108. Gibbons-Neff, T.: Isis drones are attacking us troops and disrupting airstrikes in Raqqa, officials say. Washington Post **14** (2017)
109. Hoenig, M.: Hezbollah and the use of drones as a weapon of terrorism. Public Interest Rep. **67**(2) (2014)
110. Stalinsky, S., Sosnow, R.: A decade of jihadi organizations' use of drones—from early experiments by Hizbullah, Hamas, and Al-Qaeda to emerging national security crisis for the west as ISIS launches first attack drones. MEMRI-The Middle East Media Research Institute. February, 21 (2017)
111. Shay, S.: The Houthi Maritime Threats in the Red Sea Basin, vol. 9. Institute for Policy and Strategy (2017)
112. Rossiter, A.: Drone usage by militant groups: exploring variation in adoption. Def. Secur. Anal. **34**(2), 113–126 (2018)
113. Sana'a Center. Drone wars (2019)
114. Archambault, E., Veilleux-Lepage, Y.: Drone imagery in Islamic state propaganda: flying like a state. Int. Aff. **96**(4), 955–973 (2020)
115. Naudé, W.: Artificial intelligence vs covid-19: limitations, constraints and pitfalls. Ai & Society, p. 1 (2020)
116. Moon, M.J.: Fighting COVID-19 with agility, transparency, and participation: Wicked policy problems and new governance challenges. Public Adm. Rev. **80**(4), 651–656 (2020)
117. Yakas, B.: Faa investigating" anti-covid-19 volunteer drone" filmed admonishing people in nyc (2020)
118. Scott, J.E., Scott, C.H.: Models for drone delivery of medications and other healthcare items. In: Unmanned Aerial Vehicles: Breakthroughs in Research and Practice, pp. 376–392. IGI Global (2019)
119. Ye, J.: The role of health technology and informatics in a global public health emergency: practices and implications from the covid-19 pandemic. JMIR Med. Inform. **8**(7), e19866 (2020)
120. Abubakar, A.I., Omeke, K.G.,Öztürk, M., Hussain, S. and Imran, M.A.: The role of artificial intelligence driven 5G networks in COVID-19 outbreak: opportunities, challenges, and future outlook. Front. Comms. Net. (2020)
121. Nair, V.V.: Drones as futuristic crime prevention strategy: situational review during covid-19 lockdown. J. Soc. Sci. **64**(1–3), 22–29 (2020)
122. Jat, D.S., Singh, C.: Artificial intelligence-enabled robotic drones for covid-19 outbreak. In: Intelligent Systems and Methods to Combat Covid-19, pp. 37–46. Springer (2020)
123. Oguamanam, C.: Covid-19 and Africa: does one size fit all in public health intervention? Vulnerable: The Policy, Law and Ethics of COVID-19.University of Ottawa Press, Ottawa (2020) (**Forthcoming in 2020**)
124. Vafea, M.T., Atalla, E., Georgakas, J., Shehadeh, F., Mylona, E.K., Kalligeros, M., Mylonakis, E.: Emerging technologies for use in the study, diagnosis, and treatment of patients with covid-19. Cell. Mol. Bioeng. **13**(4), 249–257 (2020)
125. Zeng, Z., Chen, P.-J., Lew, A.A.: From high-touch to high-tech: Covid-19 drives robotics adoption. Tour. Geogr. **22**, 1–11 (2020)
126. Bhaskar, S., Bradley, S., Sakhamuri, S., Moguilner, S., Chattu, V.K., Pandya, S., Schroeder, S., Ray, D., Banach, M.: Designing futuristic telemedicine using artificial intelligence and robotics in the covid-19 era. Front. Public Health **8**, 708 (2020)
127. Odekerken-Schröder, G., Mele, C., Russo-Spena, T., Mahr, D., Ruggiero, A.: Mitigating loneliness with companion robots in the covid-19 pandemic and beyond: an integrative framework and research agenda. J. Serv. Manag. (2020)
128. Bhardwaj, A., Avasthi, V., Goundar, S.: Cyber security attacks on robotic platforms. Netw. Secur. **2019**(10), 13–19 (2019)
129. Wang, C., Carzaniga, A., Evans, D., Wolf, A.: Security issues and requirements for internet-scale publish-subscribe systems. In: HICSS, p. 303. IEEE (2002)
130. Esposito, C., Ciampi, M.: On security in publish/subscribe services: a survey. IEEE Commun. Surv. Tutor. **17**(2), 966–997 (2015)
131. Dzung, D., Naedele, M., Von Hoff, T.P., Crevatin, M.: Security for industrial communication systems. Proc. IEEE **93**(6), 1152–1177 (2005)
132. Laitinen, A., Niemelä, M., Pirhonen, J.: Demands of dignity in robotic care: recognizing vulnerability, agency, and subjectivity in robot-based, robot-assisted, and teleoperated elderly care. Tech. Res. Philos. Technol. **23**(3), 366–401 (2019)
133. Choi, H., Kate, S., Aafer, Y., Zhang, X., Xu, D.: Cyber-physical inconsistency vulnerability identification for safety checks in robotic vehicles. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 263–278 (2020)
134. Atamli, A.W., Martin, A.: Threat-based security analysis for the internet of things. In: 2014 International Workshop on Secure Internet of Things (SIoT), pp. 35–43. IEEE (2014)
135. Hou, T., Wang, V.: Industrial espionage-a systematic literature review (slr). Comput. Secur. **98**, 102019 (2020)
136. Siman-Tov, D., Even, S.: A new level in the cyber war between Israel and Iran. INSS Insight (1328) (2020)
137. Losa, L.: The impact of cyber capabilities on the Israeli–Iranian relationship (2020)
138. Kaye, D.D., Efron, S.: Israel's evolving Iran policy. Survival **62**(4), 7–30 (2020)
139. Yousef, K.M.A., AlMajali, A., Ghalyon, S.A., Dweik, W., Mohd, B.J.: Analyzing cyber-physical threats on robotic platforms. Sensors **18**(5), 1643 (2018)

140. Eun, Y.-S., Aßmann, J.S.: Cyberwar: taking stock of security and warfare in the digital age. Int. Stud. Perspect. **17**(3), 343–360 (2016)
141. Geerts, M.: Digitalization combined with organizational process innovation. The solution to the risk of industrial espionage? (2020)
142. Klebanov, L.R., Polubinskaya, S.V.: Computer technologies for committing sabotage and terrorism. RUDN J. Law **24**(3), 717–734 (2020)
143. Astor, M.: Your roomba may be mapping your home, collecting data that could be shared—the New York times. https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html (2017)
144. Sollins, K.R.: Iot big data security and privacy vs. innovation. IEEE Internet Things J. **6**, 1–1 (2019)
145. Noura, H.N., Hatoum, T., Salman, O., Yaacoub, J.-P., Chehab, A.: Lorawan security survey: issues, threats and possible mitigation techniques. Internet of Things, p. 100303 (2020)
146. Salamai, A., Hussain, O.K., Saberi, M., Chang, E., Hussain, F.K.: Highlighting the importance of considering the impacts of both external and internal risk factors on operational parameters to improve supply chain risk management. IEEE Access **7**, 49297–49315 (2019)
147. Priyadarshini, I.: Cyber security risks in robotics. In: Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 1235–1250. IGI Global (2018)
148. Sobb, T., Turnbull, B., Moustafa, N.: Supply chain 4.0: a survey of cyber security challenges, solutions and future directions. Electronics **9**(11), 1864 (2020)
149. Sha, K., Yang, T.A., Wei, W., Davari, S.: A survey of edge computing-based designs for IoT security. Digit. Commun. Netw. **6**(2), 195–202 (2020)
150. Gaikwad, N.B., Ugale, H., Keskar, A., Shivaprakash, N.C.: The internet of battlefield things (IoBT) based enemy localization using soldiers location and gunshot direction. IEEE Internet of Things J. **7**(12), 11725–11734 (2020)
151. Tehranipoor, M., Koushanfar, F.: A survey of hardware Trojan taxonomy and detection. IEEE Des. Test Comput. **27**(1), 10–25 (2010)
152. Wang, X., Mal-Sarkar, T., Krishna, A., Narasimhan, S., Bhunia, S.: Software exploitable hardware Trojans in embedded processor. In: 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 55–58. IEEE (2012)
153. Elmiligi, H., Gebali, F., El-Kharashi, M.W.: Multi-dimensional analysis of embedded systems security. Microprocess. Microsyst. **41**, 29–36 (2016)
154. Clark, G.W., Doran, M.V., Andel, T.R.: Cybersecurity issues in robotics. In: 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), pp. 1–5. IEEE (2017)
155. Falliere, N., Murchu, L.O., Chien, E.: W32. stuxnet dossier. White paper, Symantec Corp., Security Response **5**(6), 29 (2011)
156. Goyal, R., Sharma, S., Bevinakoppa, S., Watters, P.: Obfuscation of stuxnet and flame malware. Latest Trends Appl. Inform. Comput. **150**, 154 (2012)
157. Bencsáth, B., Pék, G., Buttyán, L., Felegyhazi, M.: The cousins of stuxnet: Duqu, flame, and gauss. Future Internet **4**(4), 971–1003 (2012)
158. Kamiński, M.A.: Operation "olympic games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. Secur. Def. Q. **29**(2), 63–71 (2020)
159. Horschig, D.: Cyber-weapons in nuclear counter-proliferation. Def. Secur. Anal. **36**(3), 352–371 (2020)
160. Fruhlinger, J.: What is wannacry ransomware, how does it infect, and who was responsible (2017)
161. Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson, Upper Saddle River (2017)
162. Monikandan, S., Arockiam, L.: Confidentiality technique to enhance security of data in public cloud storage using data obfuscation. Indian J. Sci. Technol. **8**(24), 1 (2015)
163. Bellovin, S.M., Merritt, M.: Encrypted key exchange: password-based protocols secure against dictionary attacks. In: 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 1992. Proceedings, pp. 72–84. IEEE (1992)
164. Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., Pu, C.: Reverse social engineering attacks in online social networks. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 55–74. Springer (2011)
165. Khan, M.H., Shah, M.A.: Survey on security threats of smartphones in internet of things. In: 2016 22nd International Conference on Automation and Computing (ICAC), pp. 560–566. IEEE (2016)
166. Kc, G.S., Keromytis, A.D., Prevelakis, V.: Countering code-injection attacks with instruction-set randomization. In: Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 272–280. ACM (2003)
167. Miller, J., Williams, A.B., Perouli, D.: A case study on the cybersecurity of social robots. In: Companion of the 2018 ACM/IEEE International Conference on Human–Robot Interaction, pp. 195–196. ACM (2018)
168. Shahbaznezhad, H., Kolini, F., Rashidirad, M.: Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? J. Comput. Inf. Syst. 1–12 (2020)
169. Alabdan, R.: Phishing attacks survey: types, vectors, and technical approaches. Future Internet **12**(10), 168 (2020)
170. Mo, Y., Garone, E., Casavola, A., Sinopoli, B.: False data injection attacks against state estimation in wireless sensor networks. In: 2010 49th IEEE Conference on Decision and Control (CDC), pp. 5967–5972. IEEE (2010)
171. Senie, D., Ferguson, P.: Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. Network (1998)
172. Gu, Q.: Packet-dropping attack. In: Encyclopedia of Cryptography and Security, pp. 899–902. Springer (2011)
173. Navas, R.E., Le Bouder, H., Cuppens, N., Cuppens, F., Papadopoulos, G.Z.: Do not trust your neighbors! a small IoT platform illustrating a man-in-the-middle attack. In: International Conference on Ad-Hoc Networks and Wireless, pp. 120–125. Springer (2018)
174. Chen, X., Liu, C., Li, B., Lu, K., Song, D.: Targeted backdoor attacks on deep learning systems using data poisoning (2017). arXiv preprint arXiv:1712.05526
175. Alemzadeh, H., Chen, D., Li, X., Kesavadas, T., Kalbarczyk, Z.T., Iyer, R.K.: Targeted attacks on teleoperated surgical robots: dynamic model-based detection and mitigation. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 395–406. IEEE (2016)
176. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold-boot attacks on encryption keys. Commun. ACM **52**(5), 91–98 (2009)
177. Blackwell, T., Casner, D., Nelson, B., Wiley, S.: Self-balancing robot including an ultracapacitor power source, October 18 2011. US Patent 8,041,456
178. Abomhara, M., Køien, G.M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber Secur. **4**(1), 65–88 (2015)
179. Rajendran, J., Kanuparthi, A.K., Zahran, M., Addepalli, S.K., Ormazabal, G., Karri, R.: Securing processors against insider attacks: a circuit-microarchitecture co-design approach. IEEE Des. Test **30**(2), 35–44 (2013)

180. Larson, S.: Ransomware experiment shows the dangers of hacking robots. https://money.cnn.com/2018/03/09/technology/robots-ransomware/index.html (2018)
181. Mansor, H., Markantonakis, K., Akram, R.N., Mayes, K.: Don't brick your car: firmware confidentiality and rollback for vehicles. In: 2015 10th International Conference on Availability, Reliability and Security (ARES), pp. 139–148. IEEE (2015)
182. Feily, M., Shahrestani, A., Ramadass, S.: A survey of botnet and botnet detection. In: Third International Conference on Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09, pp. 268–273. IEEE (2009)
183. Yih-Chun, H., Perrig, A., Johnson, D.B.: Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 370–380 (2006)
184. Baccelli, E., Hahm, O., Gunes, M., Wahlisch, M., Schmidt, T.C.: Riot os: Towards an os for the internet of things. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 79–80. IEEE (2013)
185. Azar, C., Brostoff, G.: System and method for providing secure access to an electronic device using continuous facial biometrics, February 5 2013. US Patent 8,370,639
186. Azar, C., Brostoff, G.: System and method for providing secure access to an electronic device using both a screen gesture and facial biometrics, January 7 2014. US Patent 8,627,096
187. Tasevski, P.: Password Attacks and Generation Strategies. Tartu University, Faculty of Mathematics and Computer Sciences, Tartu (2011)
188. Hoelscher, P.: Phishing networks. https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-attack-overview/phishing-networks/#gref
189. Neumann, P.G.: Denial-of-service attacks. Commun. ACM **43**(4), 136–136 (2000)
190. Side-Channel Attacks. Side-channel attacks
191. Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H.M., Rowe, J., Levitt, K.: Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun. Mag. **53**(6), 126–132 (2015)
192. Chesaux, J.: Wireless access point spoofing and mobile devices geolocation using swarms of flying robots. Master optional semester project, Spring (2014)
193. Kaufman, C.W., Pearlman, R.J., Gasser, M.: System for increasing the difficulty of password guessing attacks in a distributed authentication scheme employing authentication tokens, February 13 1996. US Patent 5,491,752
194. Barcena, M.B., Wueest, C.: Insecurity in the internet of things. Security Response, Symantec (2015)
195. Kumar, R., Pattnaik, P.K., Pandey, P.: Detecting and Mitigating Robotic Cyber Security Risks. IGI Global, Hershey (2017)
196. Schultz, E.E., Ray, E.: Rootkits: the ultimate malware threat. Inf. Secur. Manag. Handb. **2**, 175 (2008)
197. Denning, T., Matuszek, C., Koscher, K., Smith, J.R., Kohno, T.: A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th International Conference on Ubiquitous Computing, pp. 105–114. ACM (2009)
198. Jiang, D., Omote, K.: An approach to detect remote access trojan in the early stage of communication. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA), pp. 706–713. IEEE (2015)
199. Maglaras, L.A., Jiang, J.: Intrusion detection in Scada systems using machine learning techniques. In: Science and Information Conference (SAI), 2014, pp. 626–631. IEEE (2014)
200. Block, J.: A laws of war review of contemporary land-based missile defence system 'iron dome'. Sci. Mil. S. Afr. J. Mil. Stud. **45**(2), 105–128 (2017)
201. Schneider, P., IFSH Hamburg: Recent trends in global maritime terrorism. Marit. Secur. Count. Terror. Lessons Marit. Piracy Narc. Interdiction **150**, 187 (2020)
202. Patterson, D.A., Bridgelall, R.: Attack risk modelling for the San Diego maritime facilities. Mar. Policy 104210 (2020)
203. Morris, I.: War! what is it good for?: conflict and the progress of civilization from primates to robots. Farrar, Straus and Giroux (2014)
204. Button, M.: Economic and industrial espionage (2020)
205. Oruc, A., Sc MIET MIMarEST, M.: Claims of state-sponsored cyberattack in the maritime industry
206. Cellan-Jones, R.: Robots 'to replace up to 20 million factory jobs' by 2030. https://www.bbc.com/news/business-48760799 (27.01.2020) (2019)
207. Vermeulen, B., Pyka, A., Saviotti, P.P.: A taxonomic structural change perspective on the economic impact of robots and artificial intelligence on creative work. In: The Future of Creative Work. Edward Elgar Publishing (2020)
208. Cooper, A.: How robots change the world; what automation really means for jobs and productivity. Technical report (Tech. Rep.). Oxford Economics, Oxford (2019)
209. Acemoglu, D., Restrepo, P.: Robots and jobs: evidence from US labor markets. J. Polit. Econ. **128**(6), 2188–2244 (2020)
210. Alemzadeh, H., Raman, J., Leveson, N., Kalbarczyk, Z., Iyer, R.K.: Adverse events in robotic surgery: a retrospective study of 14 years of FDA data. PloS one **11**(4), e0151470 (2016)
211. Bloomfield, R.E.G.: Bullets to bytes: defending the United Kingdom in cyberspace (2019)
212. Rotjan, R.D., Blum, J., Lewis, S.M.: Shell choice in pagurus longicarpus hermit crabs: does predation threat influence shell selection behavior? Behav. Ecol. Sociobiol. **56**(2), 171–176 (2004)
213. Peterson, A.: Yes, terrorists could have hacked Dick Cheney's heart. Washington Post (2013)
214. Senthilkumar, K.S., Pirapaharan, K., Julai, N., Hoole, P.R.P., Othman, A.-H., Harikrishnan, R., Hoole, S.R.H.: Perceptron ANN control of array sensors and transmitters with different activation functions for 5g wireless systems. In: 2017 International Conference on Signal Processing and Communication (ICSPC), pp. 107–111. IEEE (2017)
215. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al.: Comprehensive experimental analyses of automotive attack surfaces. In: USENIX Security Symposium, pp. 77–92. San Francisco (2011)
216. Turner, A., Glantz, K., Gall, J.: A practitioner-researcher partnership to develop and deliver operational value of threat, risk and vulnerability assessment training to meet the requirements of emergency responders. J. Homel. Secur. Emerg. Manag. **10**(1), 319–332 (2013)
217. Moalla, R., Labiod, H., Lonc, B., Simoni, N.: Risk analysis study of its communication architecture. In: 2012 Third International Conference on the Network of the Future (NOF), pp. 1–5. IEEE (2012)
218. Alberts, C.J., Behrens, S.G., Pethia, R.D., Wilson, W.R.: Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst (1999)
219. Zahra, B.F., Abdelhamid, B.: Risk analysis in internet of things using EBIOS. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–7. IEEE (2017)
220. Méthode Harmonisée d'Analyse de Risques. Mehari. CLUSIF, France (2007)
221. Barber, B., Davey, J.: The use of the CCTA risk analysis and management methodology Cramm in health information systems. Medinfo **92**, 1589–1593 (1992)

222. Secrétariat Général Défense Nationale. Ebios-expression des besoins et identification des objectifs de sécurité (2004)
223. Süzen, A.A.: A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. Int. J. Comput. Netw. Inf. Secur. **12**(1) (2020)
224. Brandstötter, M., Komenda, T., Ranz, F., Wedenig, P., Gattringer, H., Kaiser, L., Breitenhuber, G., Schlotzhauer, A., Müller, A., Hofbaur, M.: Versatile collaborative robot applications through safety-rated modification limits. In: International Conference on Robotics in Alpe-Adria Danube Region, pp. 438–446. Springer (2019)
225. Komenda, T., Steiner, M., Rathmair, M., Brandstötter, M.: Introducing a morphological box for an extended risk assessment of human-robot work systems considering prospective system modifications. Gra, In: Joint Austrian Computer Vision and Robotics WorkshopAt (2019)
226. Chemweno, P., Pintelon, L., Decre, W.: Orienting safety assurance with outcomes of hazard analysis and risk assessment: a review of the ISO 15066 standard for collaborative robot systems. Saf. Sci. **129**, 104832 (2020)
227. Wan, N., Li, L., Ye, C., Wang, B.: Risk assessment in intelligent manufacturing process: a case study of an optical cable automatic arranging robot. IEEE Access **7**, 105892–105901 (2019)
228. George, G., Thampi, S.M.: Vulnerability-based risk assessment and mitigation strategies for edge devices in the internet of things. Pervasive Mob. Comput. **59**, 101068 (2019)
229. Huang, Y.-L., Sun, W.-L., Tang, Y.-H.: 3aram: a 3-layer AHP-based risk assessment model and its implementation for an industrial IoT cloud. In: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 450–457. IEEE (2019)
230. Radanliev, P., De Roure, D.C., Nurse, J.R.C., Montalvo, R.M., Cannady, S., Santos, O., Burnap, P., Maple, C., et al.: Future developments in standardisation of cyber risk in the internet of things (iot). SN Appl. Sci. **2**(2), 169 (2020)
231. Lv, Z., Yang, H., Singh, A.K., Manogaran, G., Lv, H.: Trustworthiness in industrial IoT systems based on artificial intelligence. IEEE Trans. Ind. Inform. (2020)
232. Afzaliseresht, N., Miao, Y., Michalska, S., Liu, Q., Wang, H.: From logs to stories: human-centred data mining for cyber threat intelligence. IEEE Access **8**, 19089–19099 (2020)
233. Koloveas, P., Chantzios, T., Tryfonopoulos, C., Skiadopoulos, S.: A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence. In: 2019 IEEE World Congress on Services (SERVICES), vol. 2642, pp. 3–8. IEEE (2019)
234. Xu, Z., Parizi, R.M., Hammoudeh, M., Loyola-González, O.: Cyber Security Intelligence and Analytics: Proceedings of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), vol. 2, 1147. Springer (2020)
235. Gupta, S., Sabitha, A.S., Punhani, R.: Cyber security threat intelligence using data mining techniques and artificial intelligence. Int. J. Recent Technol. Eng. **8**, 6133–6140 (2019)
236. De Cubber, G., Doroftei, D., Rudin, K., Berns, K., Matos, A., Serrano, D., Sanchez, J., Govindaraj, S., Bedkowski, J., Roda, R., et al.: Introduction to the use of robotic tools for search and rescue (2017)
237. Davahlia, A., Shamsib, M., Abaeic, G.: A lightweight anomaly detection model using SVM for WSNs in IoT through a hybrid feature selection algorithm based on GA and GWO. J. Comput. Secur. **7**(1), 63–79 (2020)
238. Pham, V., Seo, E., Chung, T.-M.: Lightweight convolutional neural network based intrusion detection system. J. Commun. **15**(11) (2020)
239. He, H., Gray, J., Cangelosi, A., Meng, Q., McGinnity, T.M., Mehnen, J.: The challenges and opportunities of artificial intelligence in implementing trustworthy robotics and autonomous systems. In: 3rd International Conference on Intelligent Robotic and Control Engineering (2020)
240. Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R., Sakurai, K.: Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features. Electronics **9**(1), 144 (2020)
241. Sethumadhavan, S., Waksman, A., Suozzo, M., Huang, Y., Eum, J.: Trustworthy hardware from untrusted components. Commun. ACM **58**(9), 60–71 (2015)
242. Huffmire, T., Brotherton, B., Wang, G., Sherwood, T., Kastner, R., Levin, T., Nguyen, T., Irvine, C.: Moats and drawbridges: an isolation primitive for reconfigurable hardware based systems. In: 2007 IEEE Symposium on Security and Privacy (SP), pp. 281–295. IEEE (2007)
243. Waksman, A., Sethumadhavan, S.: Tamper evident microprocessors. In: 2010 IEEE Symposium on Security and Privacy (SP), pp. 173–188. IEEE (2010)
244. Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P., Sunar, B.: Trojan detection using ic fingerprinting. In: IEEE Symposium on Security and Privacy, 2007. SP'07, pp. 296–310. IEEE (2007)
245. Pike, L., Hickey, P., Elliott, T., Mertens, E., Tomb, A.: Trackos: a security-aware real-time operating system. In: International Conference on Runtime Verification, pp. 302–317. Springer (2016)
246. Abera, T., Asokan, N., Davi, L., Ekberg, J.-E., Nyman, T., Paverd, A., Sadeghi, A.-R., Tsudik, G.: C-flat: control-flow attestation for embedded systems software. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 743–754. ACM (2016)
247. Wang, H., Zhang, C., Song, Y., Pang, B.: Robot arm perceptive exploration based significant slam in search and rescue environment. Int. J. Robot. Autom. **33**(4) (2018)
248. Romero, M., Frey, B., Southern, C., Abowd, G.D.: Brailletouch: designing a mobile eyes-free soft keyboard. In: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, pp. 707–709. ACM (2011)
249. Joint Task Force Transformation Initiative et al.: Guide for conducting risk assessments. Special Publication (NIST SP)-800-30 Rev 1 (2012)
250. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. **139**, 156–178 (2015)
251. McLean, I., Szymanski, B., Bivens, A.: Methodology of risk assessment in mobile agent system design. In: Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, pp. 35–42. IEEE (2003)
252. Guiochet, J., Martin-Guillerez, D., Powell, D.: Experience with model-based user-centered risk assessment for service robots. In: 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering (HASE), pp. 104–113. IEEE (2010)
253. Wagner, H.J., Alvarez, M., Kyjanek, O., Bhiri, Z., Buck, M., Menges, A.: Flexible and transportable robotic timber construction platform-tim. Autom. Constr. **120**, 103400 (2020)
254. Diab, M., Pomarlan, M., Beßler, D., Akbari, A., Rosell, J., Bateman, J., Beetz, M.: Skillman-a skill-based robotic manipulation framework based on perception and reasoning. Robot. Auton. Syst. **134**, 103653 (2020)
255. Choi, H., Kate, S., Aafer, Y., Zhang, X., Xu, D.: Software-based realtime recovery from sensor attacks on robotic vehicles. In: 23rd International Symposium on Research in Attacks, Intrusions and Defenses (*RAID* 2020), pp. 349–364 (2020)
256. Beaudoin, L., Avanthey, L., Villard, C.: Porting ardupilot to esp32: towards a universal open-source architecture for agile and easily replicable multi-domains mapping robots. Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci. **43**, 933–939 (2020)

257. Huang, Y., Wang, W., Wang, Y., Jiang, T., Zhang, Q.: Lightweight sybil-resilient multi-robot networks by multipath manipulation. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, pp. 2185–2193. IEEE (2020)
258. Wallhoff, F.: Fgnet-facial expression and emotion database. Technische Universität München (2004)
259. Johnson, N.F., Jajodia, S.: Exploring steganography: seeing the unseen. Computer **31**(2), 26–34 (1998)
260. Douglas, M., Bailey, K., Leeney, M., Curran, K.: An overview of steganography techniques applied to the protection of biometric data. Multimed. Tools Appl. **77**(13), 17333–17373 (2018)
261. Woodward, J.D., Jr., Horn, C., Gatune, J., Thomas, A.: Biometrics: a look at facial recognition. Technical report, Rand Corp Santa Monica, CA (2003)
262. Taupin, J.M.: Using forensic DNA evidence at trial: a case study approach. CRC Press, Boca Raton (2016)
263. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)
264. George, J.P.: Development of efficient biometric recognition algorithms based on fingerprint and face. Ph.D. thesis, Christ University (2012)
265. Al-Ani, M.S., Rajab, M.A.: Biometrics hand geometry using discrete cosine transform (DCT). Sci. Technol. **3**(4), 112–117 (2013)
266. Jain, A.K., Kumar, A.: Biometric recognition: an overview. In: Second Generation Biometrics: The Ethical, Legal and Social Context, pp. 49–79. Springer (2012)
267. Wei, X., Wang, T., Tang, C., Fan, J.: Collaborative mobile jammer tracking in multi-hop wireless network. Future Gener. Comput. Syst. **78**, 1027–1039 (2018)
268. Nguyen, M.-H.: The relationship between password-authenticated key exchange and other cryptographic primitives. In: Theory of Cryptography Conference, pp. 457–475. Springer (2005)
269. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(11), 770–772 (1981)
270. Song, R.: Advanced smart card based password authentication protocol. Comput. Stand. Interfaces **32**(5–6), 321–325 (2010)
271. Chaudhry, S.A., Farash, M.S., Naqvi, H., Sher, M.: A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electron. Commer. Res. **16**(1), 113–139 (2016)
272. He, D., Gao, Y., Chan, S., Chen, C., Jiajun, B.: An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc Sens. Wirel. Netw. **10**(4), 361–371 (2010)
273. Yeh, H.-L., Chen, T.-H., Liu, P.-C., Kim, T.-H., Wei, H.-W.: A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors **11**(5), 4767–4779 (2011)
274. Chen, T.-H., Shih, W.-K.: A robust mutual authentication protocol for wireless sensor networks. ETRI J. **32**(5), 704–712 (2010)
275. Kim, J., Lee, D., Jeon, W., Lee, Y., Won, D.: Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. Sensors **14**(4), 6443–6462 (2014)
276. Xue, K., Ma, C., Hong, P., Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. **36**(1), 316–323 (2013)
277. Wang, D., Li, W., Wang, P.: Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Ind. Inform. (2018)
278. Li, C.-T., Weng, C.-Y., Lee, C.-C.: An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors **13**(8), 9589–9603 (2013)
279. Gope, P., Hwang, T., et al.: A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans. Ind. Electron. **63**(11), 7124–7132 (2016)
280. Jiang, Q., Ma, J., Xiang, L., Tian, Y.: An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-peer Netw. Appl. **8**(6), 1070–1081 (2015)
281. Fan, W., Lili, X., Kumari, S., Li, X.: A new and secure authentication scheme for wireless sensor networks with formal proof. Peer-to-Peer Netw. Appl. **10**(1), 16–30 (2017)
282. Amin, R., Biswas, G.P.: A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Netw. **36**, 58–80 (2016)
283. Srinivas, J., Mukhopadhyay, S., Mishra, D.: Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Netw. **54**, 147–169 (2017)
284. González Muñiz, M., Laud, P.: On the (im) possibility of perennial message recognition protocols without public-key cryptography. In: Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1510–1515. ACM (2011)
285. Kumar, P., Choudhury, A.J., Sain, M., Lee, S.-G., Lee, H.-J.: Ruasn: a robust user authentication framework for wireless sensor networks. Sensors **11**(5), 5020–5046 (2011)
286. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.: A survey of lightweight-cryptography implementations. IEEE Des. Test Comput. **6**, 522–533 (2007)
287. De Canniere, C., Dunkelman, O., Knežević, M.: Katan and ktantan—a family of small and efficient hardware-oriented block ciphers. In: Cryptographic Hardware and Embedded Systems-CHES 2009, pp. 272–288. Springer (2009)
288. Gong, Z., Nikova, S., Law, Y.W.: Klein: a new family of lightweight block ciphers. In: International Workshop on Radio Frequency Identification: Security and Privacy Issues, pp. 1–18. Springer (2011)
289. Lim, C.H., Korkishko, T.: mcrypton—a lightweight block cipher for security of low-cost rfid tags and sensors. In: International Workshop on Information Security Applications, pp. 243–258. Springer (2005)
290. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: an ultra-lightweight blockcipher. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp. 342–357. Springer (2011)
291. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: Present: an ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp. 450–466. Springer (2007)
292. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: A lightweight block cipher for multiple platforms. In: International Conference on Selected Areas in Cryptography, pp. 339–354. Springer (2012)
293. Yap, H., Khoo, K., Poschmann, A., Henricksen, M.: Epcbc-a block cipher suitable for electronic product code encryption. In: International Conference on Cryptology and Network Security, pp. 76–97. Springer (2011)
294. Dworkin, M.: Recommendation for block cipher modes of operation. Methods and techniques. Technical report, National Inst of Standards and Technology, Gaithersburg, MD, Computer Security Div (2001)
295. Breiling, B., Dieber, B., Schartner, P.: Secure communication for the robot operating system. In: 2017 Annual IEEE International Systems Conference (SysCon), pp. 1–6. IEEE (2017)
296. Hussein, A., Elhajj, I.H., Chehab, A., Kayssi, A.: Securing diameter: comparing tls, dtls, and ipsec. In: 2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1–8. IEEE (2016)

297. Dieber, B., Kacianka, S., Rass, S., Schartner, P.: Application-level security for ros-based applications. In: 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 4477–4482. IEEE (2016)
298. Hussaini, S.: Cyber security in cloud using blowfish encryption. Int. J. Inf. Technol. (IJIT), **6**(5) (2020)
299. Tian, N.: Cloud-edge hybrid robotic systems for physical human robot interactions. Ph.D. thesis, UC Berkeley (2020)
300. Chavhan, S., Doriya, R.: Secured map building using elliptic curve integrated encryption scheme and kerberos for cloud-based robots. In: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 157–164. IEEE (2020)
301. Strobel, V., Ferrer, E.C., Dorigo, M.: Blockchain technology secures robot swarms: a comparison of consensus protocols and their resilience to byzantine robots. Front. Robot. AI **7**, 54 (2020)
302. Alcaraz, C., Rubio, J.E., Lopez, J.: Blockchain-assisted access for federated smart grid domains: coupling and features. J. Parallel Distrib. Comput. (2020)
303. Fagiolini, A., Pellinacci, M., Valenti, G., Dini, G., Bicchi, A.: Consensus-based distributed intrusion detection for multi-robot systems. In: IEEE International Conference on Robotics and Automation, 2008. ICRA 2008, pp. 120–127. IEEE (2008)
304. Reategui, E.B., Campbell, J.: A classification system for credit card transactions. In: European Workshop on Advances in Case-Based Reasoning, pp. 280–291. Springer (1994)
305. Bonifacio, J.M., Cansian, A.M., De Carvalho, A.C.P.L.F., Moreira, E.S.: Neural networks applied in intrusion detection systems. In: The 1998 IEEE International Joint Conference on Neural Networks Proceedings, 1998. IEEE World Congress on Computational Intelligence, vol. 1, pp. 205–210. IEEE (1998)
306. Yeung, D.-Y., Chow, C.: Parzen-window network intrusion detectors. In: Object Recognition Supported by User Interaction for Service Robots, vol. 4, pp. 385–388. IEEE (2002)
307. Vigna, G., Robertson, W., Kher, V., Kemmerer, R.A.: A stateful intrusion detection system for world-wide web servers. In: Null, p. 34. IEEE (2003)
308. Onat, I., Miri, A.: An intrusion detection system for wireless sensor networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking And Communications, 2005.(WiMob'2005), vol. 3, pp. 253–259. IEEE (2005)
309. Gudadhe, M., Prasad, P., Wankhade, L.K.: A new data mining based network intrusion detection model. In: 2010 International Conference on Computer and Communication Technology (ICCCT), pp. 731–735. IEEE (2010)
310. Om, H., Kundu, A.: A hybrid system for reducing the false alarm rate of anomaly intrusion detection system. In: 2012 1st International Conference on Recent Advances in Information Technology (RAIT), pp. 131–136. IEEE (2012)
311. Rath, M., Pattanayak, B.K.: Security protocol with ids framework using mobile agent in robotic manet. Int. J. Inf. Secur. Privacy (IJISP) **13**(1), 46–58 (2019)
312. Rivera, S., Iannillo, A.K., et al.: Ros-immunity: integrated approach for the security of ros-enabled robotic systems (2020)
313. Zhou, Y., Mazzuchi, T.A., Sarkani, S.: M-adaboost-a based ensemble system for network intrusion detection. Expert Syst. Appl. **162** (2020)
314. Gorbenko, A., Popov, V.: Abnormal behavioral pattern detection in closed-loop robotic systems for zero-day deceptive threats. In: 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp. 1–6. IEEE (2020)
315. Almalawi, A., Fahad, A., Tari, Z., Khan, A.I., Alzahrani, N., Bakhsh, S.T., Alassafi, M.O., Alshdadi, A., Qaiyum, S.: Add-on anomaly threshold technique for improving unsupervised intrusion detection on scada data. Electronics **9**(6), 1017 (2020)
316. Spitzner, L.: Honeypots: Tracking Hackers, vol. 1. Addison-Wesley, Reading (2003)
317. Zhang, F., Zhou, S., Qin, Z., Liu, J.: Honeypot: a supplemented active defense system for network security. In: Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003, pp. 231–235. IEEE (2003)
318. Irvene, C., Formby, D., Litchfield, S., Beyah, R.: Honeybot: a honeypot for robotic systems. Proc. IEEE **106**(1), 61–70 (2018)
319. Ranum, M.: Backofficer friendly (bof)
320. Spitzner, L.: Specter: a commercial honeypot solution for windows. Acesso em **26**(08) (2003)
321. Provos, N.: Honeyd-a virtual honeypot daemon. In: 10th DFN-CERT Workshop, Hamburg, Germany, vol. 2, p. 4 (2003)
322. La, Q.D., Quek, T.Q.S., Lee, J.: A game theoretic model for enabling honeypots in IoT networks. In: 2016 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2016)
323. Spitzner, L.: The honeynet project: trapping the hackers. IEEE Secur. Privacy **99**(2), 15–23 (2003)
324. Terra, A., Riaz, H., Raizer, K., Hata, A., Inam, R.: Safety vs. efficiency: Ai-based risk mitigation in collaborative robotics. In: 2020 6th International Conference on Control, Automation and Robotics (ICCAR), pp. 151–160. IEEE (2020)
325. Wang, C., Tok, Y.C., Poolat, R., Chattopadhyay, S., Elara, M.R.: How to secure autonomous mobile robots? an approach with fuzzing, detection and mitigation. J. Syst. Archit. 101838 (2020)
326. Bykovsky, A.Y.: Heterogeneous network architecture for integration of AI and quantum optics by means of multiple-valued logic. Quantum Rep. **2**(1), 126–165 (2020)
327. Alamer, A.: A secure anonymous tracing fog-assisted method for the internet of robotic things. Library Hi Tech (2020)
328. Szalachowski, P., Ksiezopolski, B., Kotulski, Z.: Cmac, ccm and gcm/gmac: advanced modes of operation of symmetric block ciphers in wireless sensor networks. Inf. Process. Lett. **110**(7), 247–251 (2010)
329. Abeykoon, I., Feng, X.: 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), pp. 851–857. IEEE (2017)
330. Erbacher, R.F., Christiansen, K., Sundberg, A., et al.: Visual network forensic techniques and processes. In: 1st Annual Symposium on Information Assurance: Intrusion Detection and Prevention, p. 72 (2006)
331. Noura, H.N., Melki, R., Chehab, A., Fernandez, J.H.: Efficient and robust data availability solution for hybrid plc/rf systems. Comput. Netw. **185**, 107675 (2021)
332. Chigan, C., Li, L., Ye, Y.: Resource-aware self-adaptive security provisioning in mobile ad hoc networks. In: 2005 IEEE Wireless Communications and Networking Conference, vol. 4, pp. 2118–2124. IEEE (2005)
333. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, 2007. SP'07, pp. 321–334. IEEE (2007)
334. Needham, R.M., Wheeler, D.J.: Tea extensions. Report (Cambridge University, Cambridge, UK, 1997) Google Scholar (1997)
335. Hu, W., Corke, P., Shih, W.C., Overs, L.: secfleck: a public key technology platform for wireless sensor networks. In: European Conference on Wireless Sensor Networks, pp. 296–311. Springer (2009)
336. Hu, W., Tan, H., Corke, P., Shih, W.C., Jha, S.: Toward trusted wireless sensor networks. ACM Trans. Sens. Netw. (TOSN) **7**(1), 5 (2010)
337. Touati, L., Challal, Y., Bouabdallah, A.: C-cp-abe: cooperative ciphertext policy attribute-based encryption for the internet of

things. In: 2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS), pp. 64–69. IEEE (2014)
338. Touati, L., Challal, Y.: Collaborative kp-abe for cloud-based internet of things applications. In: 2016 IEEE International Conference on Communications (ICC), pp. 1–7. IEEE (2016)
339. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and communications security, pp. 89–98. ACM (2006)
340. Hohenberger, S., Lysyanskaya, A.: How to securely outsource cryptographic computations. In: Theory of Cryptography Conference, pp. 264–282. Springer (2005)
341. Even, S., Goldreich, O., Micali, S.: On-line/off-line digital signatures. J. Cryptol. **9**(1), 35–67 (1996)
342. Laih, C.-S., Kuo, W.-C.: New signature schemes based on factoring and discrete logarithms. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **80**(1), 46–53 (1997)
343. Courtois, N.T., Finiasz, M., Sendrier, N.: How to achieve a Mceliece-based digital signature scheme. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 157–174. Springer (2001)
344. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)
345. Hoffstein, J., Pipher, J., Silverman, J.H.: Ntru: a ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium, pp. 267–288. Springer (1998)
346. Noura, H.N., Melki, R., Chehab, A.: Efficient data confidentiality scheme for 5g wireless NOMA communications. J. Inf. Secur. Appl. **58** (2021)
347. Noura, H.N., Melki, R., Kanj, R., Chehab, A.: Secure MIMO d2d communication based on a lightweight and robust PLS cipher scheme. Wirel. Netw. **27**(1), 557–574 (2021)
348. Trappe, W., Howard, R., Moore, R.S.: Low-energy security: limits and opportunities in the internet of things. IEEE Secur. Privacy **13**(1), 14–21 (2015)
349. Mukherjee, A.: Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. Proc. IEEE **103**(10), 1747–1761 (2015)
350. Noura, H.N., Melki, R., Chehab, A., Mansour, M.M., Martin, S.: Efficient and secure physical encryption scheme for low-power wireless m2m devices. In: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 1267–1272. IEEE (2018)
351. Melki, R., Noura, H.N., Mansour, M.M., Chehab, A.: An efficient OFDM-based encryption scheme using a dynamic key approach. IEEE Internet of Things J. **6**(1), 361–378 (2018)
352. Noura, H.N., Melki, R., Chehab, A., Hernandez Fernandez, J.: Efficient and secure message authentication algorithm at the physical layer. Wirel. Netw. 1–15 (2020)
353. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In: Annual International Cryptology Conference, pp. 1–15. Springer (1996)
354. Noura, H.N., Salman, O., Chehab, A., Couturier, R.: Distlog: a distributed logging scheme for IoT forensics. Ad Hoc Netw. **98**, 102061 (2020)
355. Melki, R., Noura, H.N., Chehab, A.: Lightweight multi-factor mutual authentication protocol for IoT devices. Int. J. Inf. Secur. **19**, 1–16 (2019)
356. Noura, H.N., Melki, R., Chehab, A.: Secure and lightweight mutual multi-factor authentication for IoT communication systems. In: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), pp. 1–7. IEEE (2019)
357. Noura, H.N., Salman, O., Couturier, R., Chehab, A.: Novel one round message authentication scheme for constrained IoT devices. J. Ambient Intell. Hum. Comput. 1–17 (2021)
358. Noura, H.N., Noura, M., Salman, O., Couturier, R., Chehab, A.: Efficient & secure image availability and content protection. Multimed. Tools Appl. **79**, 22869–22904 (2020)
359. Noura, H.N., Chehab, A., Sleem, L., Noura, M., Couturier, R., Mansour, M.M.: One round cipher algorithm for multimedia IoT devices. Multimed. Tools Appl. **77**, 1–31 (2018)
360. Noura, H., Chehab, A., Couturier, R.: Lightweight dynamic key-dependent and flexible cipher scheme for IoT devices. In: 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–8. IEEE (2019)
361. Noura, H.N., Couturier, R., Pham, C., Chehab, A.: Lightweight stream cipher scheme for resource-constrained IoT devices. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1–8. IEEE (2019)
362. Noura, H.N., Chehab, A., Couturier, R.: Overview of efficient symmetric cryptography: dynamic vs static approaches. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–6. IEEE (2020)
363. Noura, H.N., Melki, R., Malli, M., Chehab, A.: Lightweight and secure cipher scheme for multi-homed systems. Wirel. Netw. 1–18
364. Noura, H.N., Salman, O., Chehab, A., Couturier, R.: Preserving data security in distributed fog computing. Ad Hoc Netw. **94**, 101937 (2019)
365. Noura, H.N., Salman, O., Kaaniche, N., Sklavos, N., Chehab, A., Couturier, R.: Tresc: Towards redesigning existing symmetric ciphers. Microprocess. Microsyst. 103478 (2020)
366. Fawaz, Z., Noura, H.N., Mostefaoui, A.: Securing jpeg-2000 images in constrained environments: a dynamic approach. Multimed. Syst. **24**(6), 669–694 (2018)
367. Mostefaoui, A., Noura, H.N., Fawaz, Z.: An integrated multimedia data reduction and content confidentiality approach for limited networked devices. Ad Hoc Netw. **32**, 81–97 (2015)
368. Salman, O., Elhajj, I.H., Chehab, A., Kayssi, A.: A multi-level internet traffic classifier using deep learning. In: 2018 9th International Conference on the Network of the Future (NOF), pp. 68–75 (2018)
369. Salman, O., Chaddad, L., Elhajj, I.H., Chehab, A., Kayssi, A.: Pushing intelligence to the network edge. In: 2018 Fifth International Conference on Software Defined Systems (SDS), pp. 87–92 (2018)