POLITECNICO DI TORINO

DIPARTIMENTO DI INGEGNERIA GESTIONALE

Tesi di Laurea Magistrale

Cybersecurity Issues For Companies Employing Mobile Manipulators.

Relatore
Prof. Dario ANTONELLI

Candidate
Jad Al Saket
Matr.275527

July 2022

ABSTRACT

Nowadays, which are the period of the digital revolution robots are widely used due to this evolution. Robot is now an important part of our lives, which can be seen almost everywhere in industry, hospitals, military, logistic etc. Robots are connected to a control device (usually a computer) via Internet WiFi or Ethernet, or a local network. The mobile manipulator is a robot that is connected via the precedent network types to provide remote access. Providing a remote access born some issues with such big importance as maintaining the safety of the data collected by the mobile manipulator, worker safety, and security access. The increasing use of mobile manipulators in the industry gives a new problem which leads to some critical damage of its consequences may be catastrophic and may cause immediate physical damage to the robot, serious human injuries, economic/financial loss, and data leakage, those problems are caused by a malicious attack by hacking and controlling the mobile manipulator. In this thesis, we will discuss Cybersecurity issues for companies employing Mobile Manipulators by listing the threats which may result in a complete/partial prevention access and impact of the attack, and we study the risks caused by this hack/attack. While we provide some solutions to prevent the hack and enhance the mobile manipulator security, or any robot system using the same communication criteria so it’s subjected to the same risks. So after, we see that using a mobile manipulator is beneficial to the industry because it reduces labor costs and time only if we take into consideration all the security measures in order to benefit from its advantages and not convert them into a catastrophe in this industry.

Acknowledgement

I dedicate this thesis to the soul of my father, who could not comprehend this day. I hope you will be proud of your son of what I did and I will do, as you are the one who made me here.
It would like to express a deep thanks from all of my heart to Professor Dario Antonelli, because without his availability, and support support the completion of this thesis was so difficult, thanks for reading my numerous revisions and helped me in making senses for the confusion. Also, thanks to my family, and friends who supported my from the begging of my study since my childhood till today while I am finishing my Master Degree.

Thanks to Polytecnico Di Torino which fulfill me on the whole duration of this course usefull information that makes the base of my career and facilitate my future by having such this pleasure to graduate from this high ranking university.

Contents

Symbols 6

List Of Figures: 9

Chapter 1: Introduction. 11

1.1 What is the Mobile Manipulator: 11

1.2 Component and their interaction. 12

1.2.1 How does the mobile manipulator see and grasp an object 14

1.3 Where the mobile manipulator can be used? 16

1.4 Intro to the problem: 20

Chapter 2: Sources And Types Of Hacks 21

2.1- Hacking sources: 21

2.2: Nature of attack 23

2.3: Negative effects of the hack. 26

Chapter 3: Attacks Classification And Explanation. 29

3.1- firmware attacks. 29

3.2- Communication attacks. 33

3.3- Hardware attacks. 36

Chapter 4: Risk Study For Implementing The Mobile Manipulator. 37

4.1 Risk Modeling 37

Qualitative risk analysis. 38

4.2- Quantitative Risk Assessment Determination: 40

4.3 Solutions and countermeasures. 43

4.3.1 Cyber threats intelligence 43

4.3.2. Active security awareness 44

4.3.3 Active response: detection and prevention 45

4.3.4 Active management: precaution and correction 46

4.3.5 Robotic security protection 46

4.3.6 System hardening 47

4.3.7 Robotic systems: identification, verification, and authentication 49

4.3.8 Cryptographic solutions and protocols 51

4.3.9 Intrusion detection systems and firewalls 52

4.3.10 Honeypots security solutions 54

4.3.11 Artificial intelligence-based solutions 55

4.4 Security requirements: 59

Chapter 5: Conclusion 61

Symbols

6-DOF
Six Degree Of Freedom

RGB-D
Red Green Blue And Depth

IMU
Inertial Measurement Unit

DWM
Dynamic Window Approach

SSD
Single Shot Multibox Detector

AP
The average precision

IOU
Intersection Over Union

ROS
Robotic Operations Systems.

IT
Information Technology

CROs
Chief Robotics Officers

XSS
Cross Site Scripting

SQL
Structured Query Language

LoRaWAN
Low-power, wide area networking protocol

DDoS
Distributed Denial of Service

DoS
Denial of Service

OPGA
Offline Password Guessing Attacks

MCI
Malicious code injection

RCE
Remote Code Execution

FDIA
False Data Injection Attacks

IP
Internet Protocol

MiMA

Man-in-the-Middle

MITM

Meet-in-the-Middle

TRA

Threat Risk Assessment

FMEA

Failure Mode & effect analysis

RA

Router Advertisement

CTI

Cyber Threat Intelligence

APT

Advanced Persistent Threat

HUMINT

Human Intelligence

INT

Open Source intelligence

TECHINT

Technical Intelligence

CIT

Cyber International techonolgy

IRS

Incident Response Service

ML

Machine Learning

AI

Artificial Intelligence

ASA

Active Security Awareness

CFI

Control Flow Integrity

RTOS

Real-Time Operating System

C-FLAT

Control-Flow Attestation for Embedded Systems Software

UML

Unified Modeling Language

GWN

The Gateway Node

WSNs

Wirless Sensor Networks

MRPs

Message Recognition Protocols

AES

Advanced Encryption Standard

ECC

Elliptic-Curve Cryptography

DTLS

Datagram Transport Layer Security

TLS

Transport Layer Security

ECIES

Elliptic Curve Integrated Encryption Scheme

BLR

Binary Logistic Regression

KNN

K-Nearest Neighbor

BOF

Back Officer Friendly

CMAC

Cryptography-based Message Authentication Code

PLS

Physical layer security

List Of Figures:

Figure 1: Shows the manipulator’s arm 11
Figure 2 Shows the mobile manipulator and its components. 12
Figure 3 Shows the user-friendly software shows the chain scheme done by a person to define the work of the mobile manipulator. 13
Figure 4 This Shows the interaction between the components. 14
Figure 5 Shows the communication structure in the robot firmware to execute the mission... 16
Figure 6 Shows mobile manipulator in warehouse/industry 17
Figure 7 shows a mobile manipulator in a space exploration mission. 18
Figure 8 Shows a mobile manipulator used in a rescue mission. 19
Figure 9 Shows a mobile manipulator discovering unexploded ordnance. 19
Figure 10 Shows the motive of the thief to attack or stole some data from a ROS 23
Figure 11 shows the map drawn via software taken by the laser scanner for the operation site that map can be leaked by cyber-attack 25
Figure 12 Shows how the Trojan Attack the device 30
Figure 13 Shows the ransomware attack 31
Figure 14 Shows the Cyber Security Scenarios source and it’s targets 40
Figure 15 42
Figure 16 Protection Requirements for the Mobile Manipulaor 49

Chapter 1: Introduction.

1.1 What is the Mobile Manipulator:

Like any technology in the world, the mobile manipulator passed through a lot of phases and periods to become as we know it now. First, it was a static manipulator that cannot move, then they invented a dynamic robot that move in a specific way on a black line drawn before its main role was to deliver tools/products from one line to another it does not contain a manipulator, these two technologies combined with some innovative ideas to booted the mobile manipulator.

Manipulator is the first appearance of the industrial robot is the first modern robot, a manipulator is a fixed automatic operating device that can imitate certain movements of the hand and arm, and it can be used to grab and carry objects or operate tools in a fixed procedure. It can replace the labor to achieve the automation and production of mechanization, which is widely used in machinery manufacturing, metallurgy, electronics, light industry, atomic energy, and other departments.

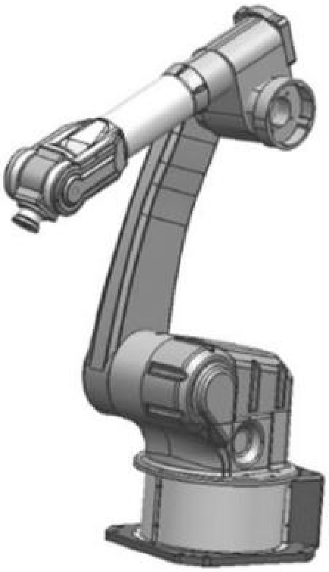


Figure 1: Shows the manipulator's arm

.

A mobile manipulator refers to a robot system that is composed of a single or plurality of manipulator arms [Fig1] mounted on a mobile platform that moves without limitation in the workspace which gives unlimited access to the manipulator. Such systems offer the advantages of mobility offered by a mobile platform and brilliantly offered by the manipulator robotic the combination of two systems reduces their drawbacks. The manipulator has the function of movement and operation, and these advantages make it superior to the mobile robot and the traditional manipulator. He has many uses that will be covered in the following section.

1.2 Component and their interaction.

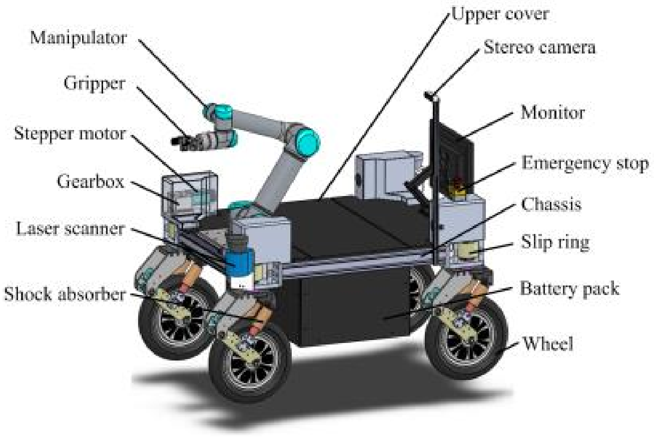
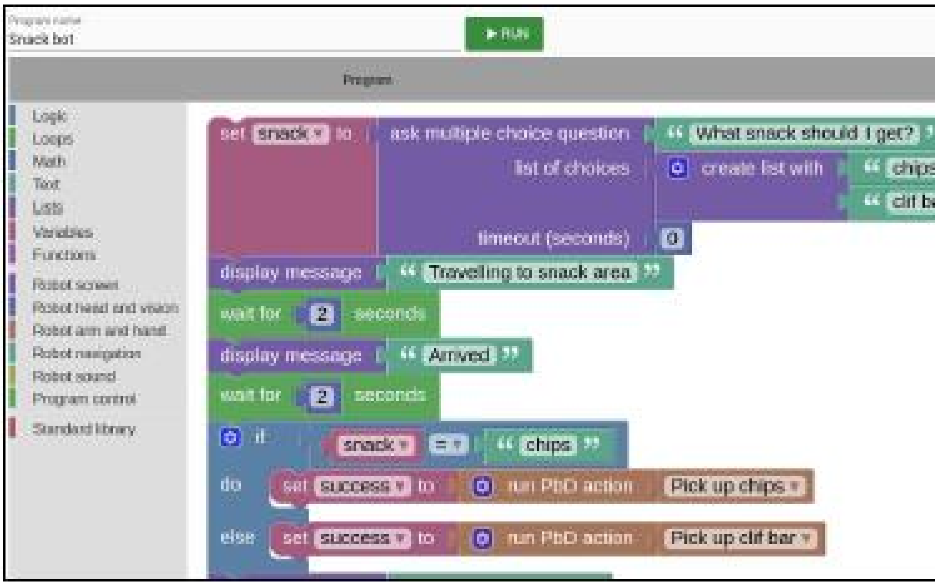


Figure 2 Shows the mobile manipulator and its components.

The mobile manipulator can perform a variety of missions in other words it's an adaptive robot that can perform a variety of tasks not only for 1 specific task during its lifetime like the ironing robot its only mission is ironing on specific points in a specific shape, so how can a mobile manipulator be modified to kept pace with the needed mission. It's not needed to be professional in programing to use a mobile manipulator because it is controlled via a user-friendly application/website so it is sufficient to know the needed task so you can go and make a chain of schemes for what you need of the mobile manipulator to do, and from this platform, you can control and check everything in the robot's like the battery life, accounts, live collected data. Knowing every robot has software and hardware so the component and the software interact to accomplish the mission.



```
set snack to  ask multiple choice question  "What snack should I get? "
              list of choices  create list with  "chips
                                                 "clif b
              timeout (seconds)  0
display message  "Travelling to snack area"
wait for 2 seconds
display message  "Arrived"
wait for 2 seconds
if     snack = "chips"
do     set success to  run PbD action  Pick up chips
else   set success to  run PbD action  Pick up clif bar
```

Figure 3 Shows the user-friendly software shows the chain scheme done by a person to define the work of the mobile manipulator.

The mobile manipulator consisted of the following component:

-The chassis where all the parts are assembled on it

-A mobile manipulator is composed of 4 wheels that can move freely at 6-DOF

-The manipulator is the robotic arm responsible for doing the task.

-Gripper The end effector must be selected to suit the item to be manipulated it is like the fingers or hand of the mobile manipulator.

-The mobile manipulator has 1 or 2 laser scanners to scan the surroundings and analyze if there is any obstacle.

-The camera takes an RGB-D image to analyze the object or the surrounding which gives a real-time image to the mobile manipulator computer to analyze it and give the right command with the right distance.

- Monitor that shows some message and from it, you can touch the screen to give the simple command (It may not be applied).

- Memory to store the important information needed for the robot it is usually not a big memory to store files- images like the memory for phones or laptops but it is essential for robot function and task accomplishment.

- Emergency stop to switch off the robot in case of urgent or malfunction.

-Battery like any electrical device the robot needs a battery to store the energy and transform the electrical energy into a mechanical one using the motor which is responsible for robot movement.

- Inertial Measurement Unit An inertial measurement unit, called “IMU”, is an electronic device used to measure and report a body's orientation and force. An IMU can be used to operate a GPS receiver when GPS signals are unavailable. It can also work when electronic interference is detected.

Those components communicate with each other in a specific way as shown in fig

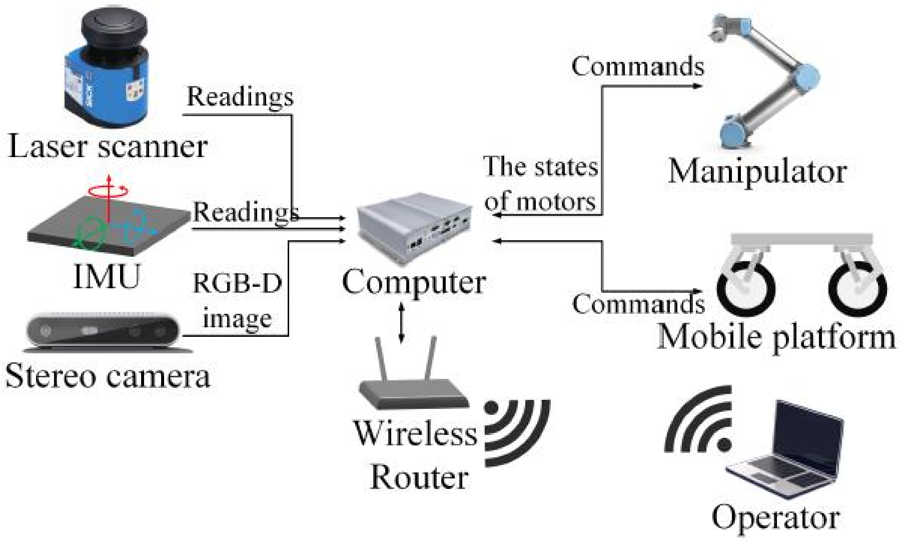


Figure 4 This Shows the interaction between the components.

.

1.2.1 How does the mobile manipulator see and grasp an object.

We can divide the processes into three phases:
Detecting and positioning, motion planning, and grasping. To grasp the objective, the robot needs to recognize the objects and locate them concerning the mobile manipulator so how is that done?
First simultaneous localization and mapping (SLAM) is the procedure to build up a map of the surroundings and localize itself and it can estimate the 6-DOF in addition to the laser scanner on the 2D map. The data collected and read from the IMU and the laser scanner with the grip map those data using the Dijkstra algorithm [1] with the dynamic window approach (DWA) for some local path planning [2]
For grasping an object the mobile manipulator needs to recognize and locate the object this operation is done using the stereo camera that catches RGB-D images of the surroundings but

how he recognizes the object knowing that it may be more than once and it may vary with the shape, size, color… usually it is used the single shot multibox detector (SSD) approach [3] because of its performance of accuracy and speed. The object detection takes inputs from RGB images and returns a list of the object proposals. Each proposal has a label and a 2D position of the object in the image. The proposals are sorted in descending order of the confidences decided by the mobile manipulator. The ranking of the proposal determines the order of the object being grasped. A bounding box is an abstract rectangle that acts as a reference point for object detection and produces so as a bounding box the mobile manipulator encloses an object, the center of the bounding box is treated as the estimation of the center of the object The 2D position of the object in the RGB images is transferred into a 2D position in the Euclidean [4] coordinate respect to the base of the manipulator which is the reference axis. The other dimension is obtained by transferring the depth value. The object detection module influences the ability to position the object of the mobile manipulator. The average precision (AP) metric is to evaluate the performance of the object detection module. What is Average precision (AP): is a popular evaluation metric for object detection, where detection is declared as a true positive if the detection box and the ground truth box overlap with IOU (intersection over union) greater than or equal to 0.5.[5]

The 3D position and the label are the inputs of the motion planning module, a series of parameterized templets of motion are designed for different categories of the objects. The motion instantiated from a templet of motion is combined by four segments: approach, contact, retreat and put down.

The algorithm takes the 3D position and the label as input and then chooses the grasping strategies base on the label of the candidate done by the specific mobile manipulator software. The algorithm figures out four key points of the end-effector based on the parameterized templets, and the motion planning module generates a motion plan to connect the key points.

The first key point is the position of the stereo camera where it can capture the whole area without being blocked out by the manipulator. To grasp the object, the manipulator does not reach the 3D position of the object directly. The second key point is the algorithm next to the 3D position of the object with a given distance based on the grasping strategies and the gripper heads to the object. The third key point is the 3D position of the object. And the fourth key point is the right place to put down the object. As the path is generated, the manipulator executes the path and at last returns to the first key point to wait for the next command.

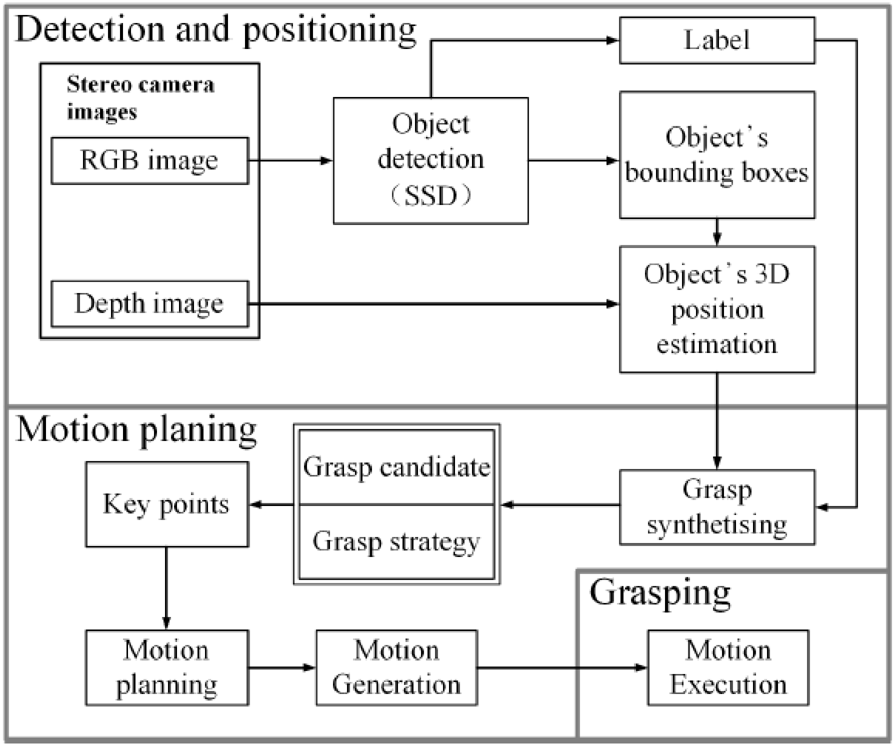


Figure 5 Shows the communication structure in the robot firmware to execute the mission.

1.3 Where the mobile manipulator can be used?

Mobile manipulation is a growing field that is subject of major focus in research environments and development, and it's being widely used in various applications, such as space exploration, military operations, homecare, health care, warehouses, manufacturing, and disaster field.

-The warehouse & distribution segment held the biggest sector that uses the mobile manipulator in 2021 and is anticipated to grow at a CAGR of 11.5% by revenue through the forecast period 2022-2027[6], owing to the increasing demand for mobile manipulators in the warehouse & distribution sector. The changes necessary to the warehouse infrastructure are relatively minimal and less expensive.

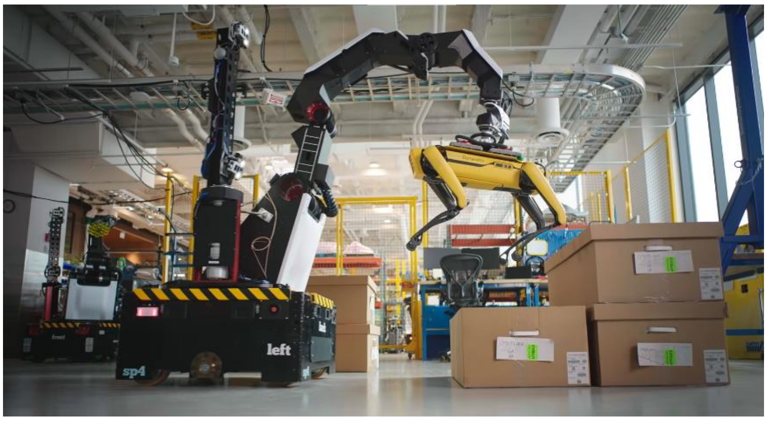


Figure 6 Shows mobile manipulator in warehouse/industry

-The manufacturing segment held the largest share in the mobile manipulators market in 2021 and is anticipated to grow at a CAGR of 12.9% by revenue through the forecast period 2022-2027 [7]. owing to the increasing application and utilization of mobile manipulators in the manufacturing industry. Modern industrial manufacturing relies heavily on flexible production. Autonomous mobile manipulators can perform a variety of tasks, including logistics, pick and place, and handling. As a result, autonomous robotic systems have the potential to improve the flexibility of existing manufacturing environments.

-First, it aided in the growth of medical professional mobile manipulator robots, as it helped augment critical infrastructure staff and alleviate supply chain stresses. And it performs nursing tasks, like checking the patient blood pressure or changing the serum, giving medical pills, and delivering medical. Because in this thesis we are dedicated to the industrial sector we can mention the critical physical consequence in the medical field which is the loss of availability in this scenario is delaying or preventing the robot from delivering urgent medical supplies to the hospital operations room, in addition to critical consequence is for the right medication to be maliciously replaced by bad medication which may cause loss of human life.

-In recent years, mobile manipulation is getting more attention in the field of space exploration. Future space robots play a critical role in collecting, distributing, and maintaining components in extraterrestrial environments. The advantage of a mobile manipulator is not only the increased workspace of the robot but also the capability to place itself in a position that provides a collision-free environment for the manipulator, in addition to the independency of the oxygen-like human.

Figure 7 shows a mobile manipulator in a space exploration mission.

-Homecare the mobile manipulator nowadays is used to help in houses he can be used to give the disabled/gaffer medicine, water, and food. He can be used to do some housekeeping missions.

-Disaster field the mobile manipulator as mentioned has 6 DOF which offers a high level of flexibility and multi-terrain use so he can be used in case of a disaster he offers aid support and supplies, searches and rescue missions, risk assessment the mobile manipulator enter first in the disaster field and give a clear live image and using its manipulator he can give support in those cases.

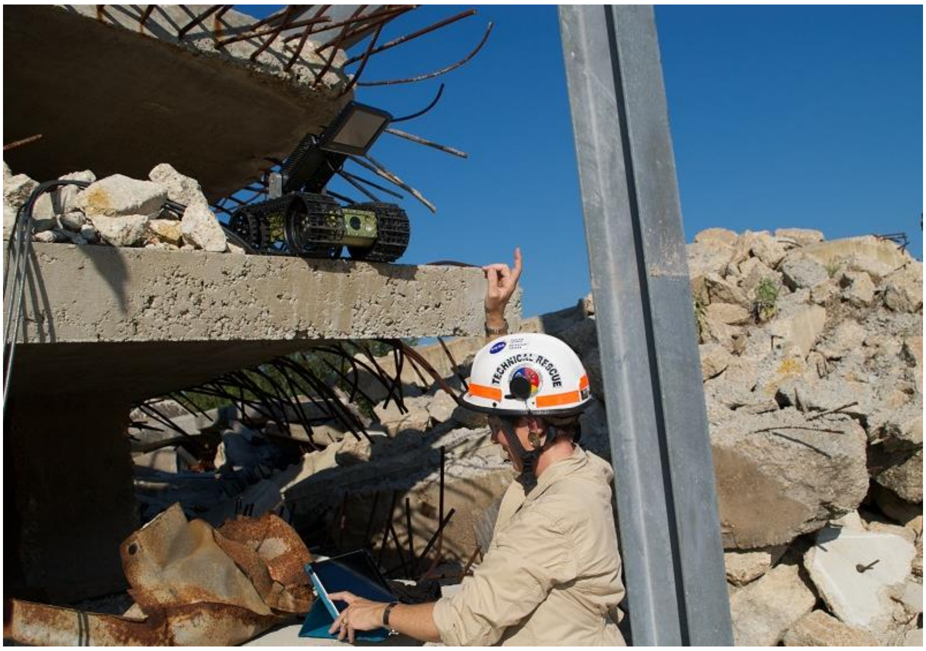


Figure 8 Shows a mobile manipulator used in a rescue mission.

-In the Military field due to its high accuracy and the 6 DOF which allows it to move freely and remotely the mobile manipulator is used in the military field especially in discovering unexploded ordnance and in case of war he can provide aid/supply for the army, logistics support, and in the front rows in discovering and infiltrate the enemies.

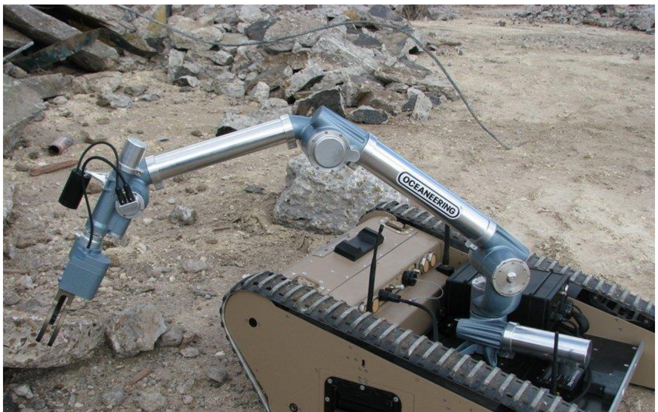


Figure 9 Shows a mobile manipulator discovering unexploded ordnance.

On the other hand, the market for industrial mobile manipulator robots was hampered due to the production constraints in the automotive and electrical/electronic industries, although the needs for intelligent and flexible automation are present. A reason for this is that the manufacturing industries act traditionally and, therefore, have a reluctance in taking risks by implementing new technologies. Also, within the field of industrial mobile manipulation, the center of attention has been on the optimization of the individual technologies, especially robot manipulators and tooling, while the integration, use, and application have been neglected

1.4 Intro to the problem:

The mobile manipulator is widely used and start to enter new sectors: this is due to an increase in demand for products/services in the manufacturing, distribution, and warehouses sector. Now he become beyond products/services so he is now used in space exploration, military field, disasters, and healthcare. Mobile manipulator is like any other product in life he has advantages and disadvantages. In this thesis, we will focus on the hacking effect of the mobile manipulator which can lead to serious damage and/or leakage of sensitive data which leads to critical damage in some cases because depending on where it is used and how, as mentioned before the mobile manipulator has a camera and laser scanner which send live data that can be leaked, or he can be subjected to serious modification of the duty, especially he is controlled and tracked using an Online(Internet)/Offline(Ethernet) platform application using a computer or mobile which in turn also can be hacked.

Chapter 2: Sources And Types Of Hacks

In the past, all the robotic operations systems (ROS) were operated in isolation from all types of networks, and communication the only risk was physical damage from humans. But the evolution in the robotic field inserted a lot of communication technology using network, signal, and computer software for robot communication and performance/task monitoring. Those innovations with their complexity facilitate the hacking of the robot system by benefiting from the vulnerability of robotic security in this chapter we will cover the possible threat source the nature of attacks in other words how it can happen, and the risk consequences of this hack.

2.1- Hacking sources:

There are many possibilities of potential danger sources which can happen from many sources, not only the people operating in the operation zone of the robot in our case the mobile manipulator. Below we will try to cover all the possible threat sources affecting the mobile manipulator:

- Worker and/or insider: here we should take into consideration the physical attack which can be done by an unsatisfied/mad employee. The damage is not trapped only on physical damage he can also steal some critical information or by facilitating the attack done by someone else throw the abuse of privilege regarding his/her post or job.

- Outsiders: the risk is not only from worker inside the company but it’s highly from an outsider that gets access to the robot through the internet if it’s connected or a visit from competitor. The aim is to have access to information or to cause the robot to malfunction through the injection of fake data or physical damage.

- The employees of the producing company: As mentioned before generally the producing company creates similar and simple credentials for the whole production which intend that the workers in the robotic domain (operators, manufacturers, IT security, Chief Robotics Officers (CROs) can have easy access to the robot.

The threats above generally should have a physical encounter with the robot or operate in its zone so here the attack is not only subjected just to physical damage it also can be stealing documents using a USB/LAN port services or having access using an internal device.

- Cybercriminals: Are the hackers that do it for business purposes either extortion of the hacked company by asking them money for not publishing data (usually on the dark web like that the hackers stayed as anonymous and cannot be recognized), or by selling the leaked data to competitors. The hack is done by gaps in software/firmware vulnerability, and usually, the payment is done via a Bitcoin wallet.

- Wannabes: are normal people that are learning hacking tricks. Usually, they do the hack for training, fun, or showing off to friends.

- Malicious manufacturers: usually some small robotic manufacturers leave a backdoor purpose on their product in order to track the activities of the robot without letting the owner know so they can have an access to some sensitive confidential information through keylogging and root-kits because usually, they come with a simple password which matches the user name. Sure not all robotics manufacturing does it.

Those threat sources don't need to have a physical encounter with the robot. If it's connected to the internet or a specific weak platform the hack here is done remotely via:

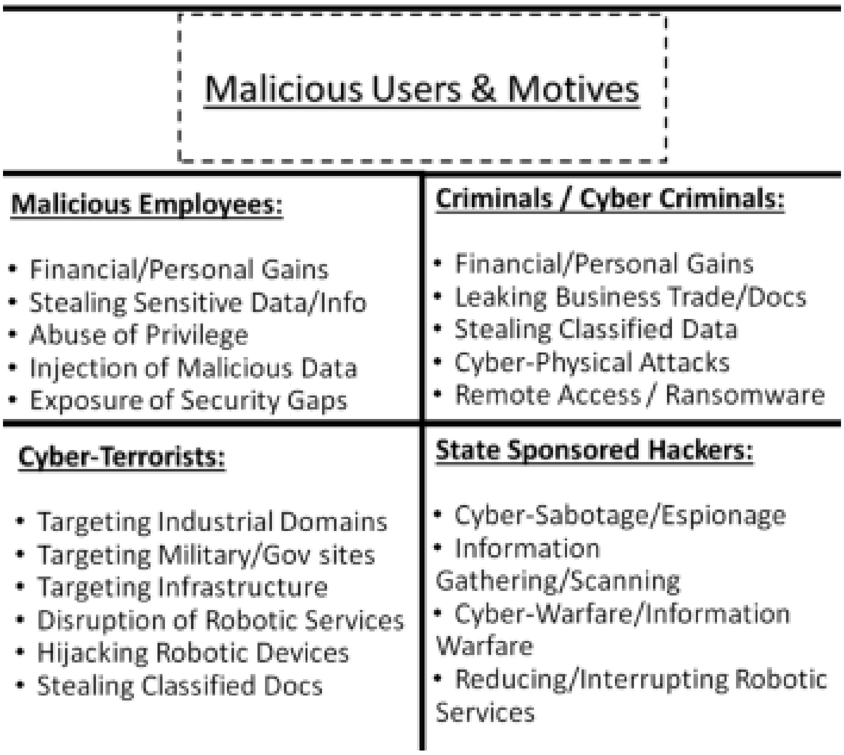
- Some competitors: resort to unfair competition especially in this period because the first who releases his invention wins, so they try some unfair competition method like this. That can be done using the help of an insider or to leak confidential documents and damage the company's reputation.

- Inexperienced/malicious operators: includes employees who don't have sufficient experience to use mobile manipulators or do it on purpose.

- Inexperienced program developers: maybe they are not well trained, experienced, or careless in essential safety and security requirements for robot software development that can be seen by the credential created by some mobile manipulator which is in some cases the password is the same as the username.

- 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. [8]

- Spies: if the mobile manipulator is used for military missions. The spies are constantly being used to conduct (cyber) espionage and sabotage operations, typically between rival countries such as the Iranian-Israeli cold cyber-war.



Malicious Users & Motives

Malicious Employees: • Financial/Personal Gains • Stealing Sensitive Data/Info • Abuse of Privilege • Injection of Malicious Data • Exposure of Security Gaps	**Criminals / Cyber Criminals:** • Financial/Personal Gains • Leaking Business Trade/Docs • Stealing Classified Data • Cyber-Physical Attacks • Remote Access / Ransomware
Cyber-Terrorists: • Targeting Industrial Domains • Targeting Military/Gov sites • Targeting Infrastructure • Disruption of Robotic Services • Hijacking Robotic Devices • Stealing Classified Docs	**State Sponsored Hackers:** • Cyber-Sabotage/Espionage • Information Gathering/Scanning • Cyber-Warfare/Information Warfare • Reducing/Interrupting Robotic Services

Figure 10 Shows the motive of the thief to attack or stole some data from a ROS

2.2: Nature of attack

In this section, we will cover the different possibilities of attacks

- Wireless jamming: this type of attack is done on the communication of the robot it is subjected to various attacks that can be done by disrupting, jamming, and interrupting the connection are done via de-authentication or jamming which leads to the complete/partial loss of mobile manipulator control.

- Surveillance and checking automated frameworks: are too inclined to different surveil lance and filtering assaults that point to assess their level of assurance, the utilized program, equipment, and operating frameworks, to look for security powerlessness or crevice which will be misused in future assaults.

- Information disclosure: as mentioned before the mobile manipulator has a laser scanner, and cameras which make any leak of data critical but the information disclosure can happen physically by (internal workers, or external guests) or via cyber-attack from cybercriminals.

- Information gathering: remains a critical danger, 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 capture attempts working on diverse tall frequencies permit producers to communicate without impedances clearing out them inclined to different capture attempts and delay assaults, which can result in an add up to breach of protection, secrecy, and judgment.

- Information modification: is one of the common threats because it targets the artificial intelligence part of robotics via some modification affecting the performance of AI to distinguish in our case of mobile manipulator it can affect the camera and the sensors so the robot loses the accuracy in performing the task like grabbing with the manipulator arm which needs to be accurate to hold the object and analyze it.

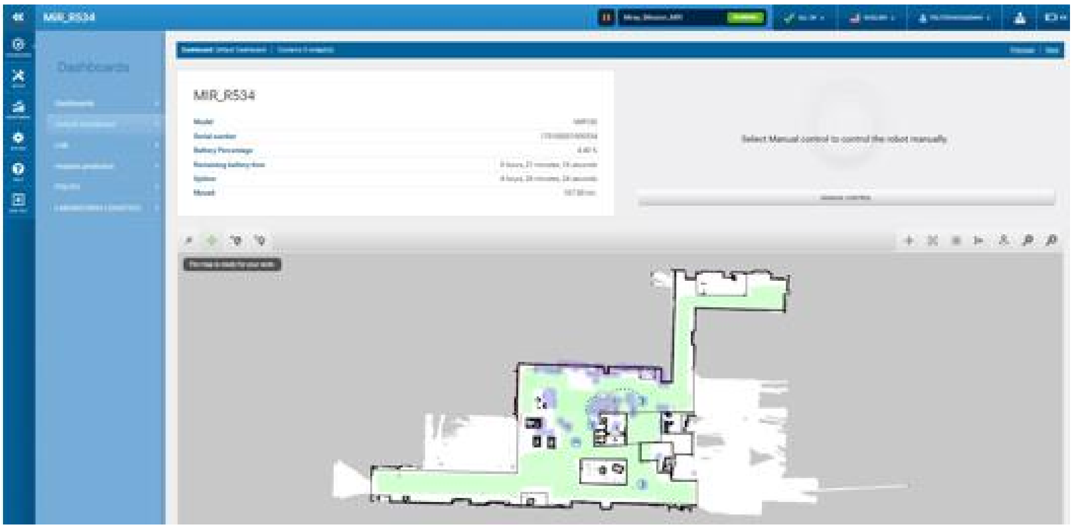
- Abuse of privilege: this type is done via insider workers who have some privilege due to their position, or job. They got unauthorized users to trespass physical and logical access and control the robot to perform unauthorized tasks or performance weaknesses.

- Physical damage: robots are also prone to physical damage, attack, and theft by insiders (unsatisfied employees), and intruders. This is mainly due to a mad employee from the company or paid by a competitor.

- 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 extended in some cases to become a sabotage operation resulting in destroying, hijacking, or severely paralyzing the ability of robotic systems to properly perform their intended task this type can be done by a competitor of the company or by the terrorist attack if the mobile manipulator is used in some military field.

- Tracking and monitoring robotic applications may incorporate undercover following frameworks that can screen and track the automated administrators without their knows all by furtively collecting data approximately them counting personal details, devices in utilizing, topographical areas, the outline checked by the laser scanner for the industry or a clear genuine see of the operation side from the camera. This principle is similar to "find my device" on Samsung or iPhone smartphones it is always tracking your topographical location on your path for a period of time but here it is used for security not for hacking.


MIR_R534

Model	[illegible]
Serial number	[illegible]
Battery Percentage	[illegible]
Remaining battery time	[illegible]
Uptime	[illegible]
Moved	[illegible]

Select Manual control to control the robot manually

Figure 11 shows the map drawn via software taken by the laser scanner for the operation site that map can be leaked by cyber-attack

- Active traffic analysis: which affects the integrity threats (man/meet-in-the-middle) by 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.[9]

- Availability threats: include service-robbery/disruption/interruption of network communications, exhaustion of resources, and buffer overflow (CPU).

- Verification dangers incorporate the noxiousness of third-party applications and services, social designing and phishing methods, mishandling of benefits, key-stroke enrollment, taking delicate archives, lack of justified (logical/physical) access controls, and arrangement of dummy/fake nodes, and spoofing.
- Secrecy dangers incorporate, in expansion to the utilize of malware, detached activity examination (i.e. spying), sensitive data burglary, noxious code infusion (i.e. XSS or SQLi), presentation of delicate data, side-channel attack, dumpster plunging, and the selection of social designing or phishing methods.

2.3: Negative effects of the hack.

Security dangers the rise of different mechanical security and cyber-security issues, dangers, and vulnerabilities, an expansion to the risk impacts are displayed as takes after:

• Security and system flaws: these risks can affect the processing and performance of the mobile manipulator, and it may cause disruption processes to perform the needed task, leading in some cases to financial losses, due to the effect caused by data interception, system blockage, extraction, and physical damage that may be caused by the malfunction of the robot.

• Back-doors ill-configured: all the robots in the world have robotic applications or applications with third-party access which can lead to various backdoor and rootkit attacks. This led to putting robot users/companies under constant control, monitoring and tracking, when the robot is functioning or switched on, registering keystrokes, and taking pictures/videos without their permission or knowledge. Which leads to data leakage and the destruction of its reputation.

• Fake applications or links [Trojan]: many robotic applications are developed by third-party developers, and some of them could be fake applications masqueraded as legitimate apps. Such applications include various malware types attached to them such as backdoor, spyware, Trojan, and ransomware, and can target the privacy, availability, and authentication of robotic users.

• Remote-access insecure wireless, and communication ports, as well as unused ones if not closed, could lead to interception where attackers use those vulnerabilities to have remote access to a given robotic system to start the attack, the most attacked robots are those who rely on vulnerable (LoRaWAN) communications. This leads to reputation destruction and in some cases to financial losses due to paying for not publishing the data/

• Device theft: robotic devices are also prone to physical theft, and control, a clear example is the hijacking of a drone when it is flying over a restricted/army area so the military can "hack" the drone by taking full access to land it off. So the same can be done with the mobile manipulator they can take full access to it which may be dangerous because they can monitor the mobile manipulator for example when the plant is closed and take a full clear view of new products or damage. This will not lead to mobile manipulator loss like the drone but it may cause leakage of critical information from inside the plant or damage the robot itself or the some products.

• Insecure backup and data storage: Unsecured cloud or hard disk storage can easily lead to data leakage or loss. Because any attack or damage to the hard disk can be critical and disable the ability for industrial safe operations which may also lead to affect the performance because as with any device the full storage leads to malfunctions. On the mobile manipulator, the risk from data leakage is low because he doesn't have big data to store because he is more live streaming except for the stored application for robot functioning which may be affected.

• System failure robotic systems: this risk is caused in case of cyber-attack or malfunction are subjected to various issues including major system failures, power drainage, and the stop of operation activity.

•Battery limitations: as any robot the mobile manipulator are resource-constrained and as such, they are inclined to battery power draining battery life expectancy over the battery and asset fatigue in case of a monitoring hack is done on it.

• Inaccurate activity: threshold the lack of available robotic activity thresholds increases the risk of robots performing abnormal and deviant activities without being detected. This may have an impact on both operational and functional safety and security procedures and cause economical loss due to task delay or unaccomplishment.

Chapter 3: Attacks Classification And Explanation.

Every robot in the world is formed using the combination of three elements which are firmware, hardware, and communication. Which collaborate with each other to form the robot and make it do the mission/Tasks supposed to.
The attacker benefits from the vulnerabilities in those elements to make his attack according to a variety of methods which will be covered in this chapter.

3.1- firmware attacks.

Many people get confused between firmware and software but actually, they do not refer to the same term. The firmware is software that's included in a piece of hardware. So to make it simpler the camera, hard disk, network card, and router all are hardware but in order to function those components, it is needed software which is the firmware. In this section, we will cover a list of possible scenario attacks on the firmware of the mobile manipulator.[10,11,12]

-Botnet attacks: are a major threat because they deploy in large numbers which leads to a large-scale cyber attack carried out by badware-infected devices controlled remotely. It can turn any robot device into a zombie bot, unlike other malware which can replicate itself like the "worm" because it let the attacker perform a large number of actions at the moment. Here the threat has the access to working within the network. The botnet can be scaled up or changed to inflict more damage. It also includes network communication features that allow the attacker to use the botnet to route communications. It is used to compromise systems, recruit new devices, and distribute malware. The most common type of botnet attacks: Brute force attack (it uses a rapid repetitive password guessing algorithm)-Distributed Denial of Service (DDoS) attacks (it floods a service with web traffic to crash it and interrupt service).Spam and phishing (attackers can send a spam email for phishing designed to trick employees to share sensitive information or login credentials)-Device bricking(it happens when a device is infected with malware that deletes its contents, often to remove evidence of a primary attack It cause device stop).

-Worm attacks: a worm is not a virus it is actually more serious than a virus because it can disrupt IT operations and cause data loss to the mobile manipulator, it also targets the robotic systems by exploiting the vulnerabilities of their network's connected devices the dangerous part that it is self-propagation and it replicates to spread automatically over other connected robotic devices and target industrial control systems . [13]

-Trojans and RAT attacks: as its namesake, he takes the concept of the famous Trojan horse which is a masqueraded virus that stays silent without any sign of activity usually in the form of a legitimate application and it can be carried out via link, email. It is done when unauthorized access is obtained by bypassing all the deployed security measures. It targets the authentication process, and the data of the mobile manipulator systems' privacy, and integrity confidentiality, and can be linked to Botnets to conduct "DDoS attacks". The danger here is that the Trojan can stay for years leaking data without any blockage or malfunction the only sign that can be detected by battery drainage. [fig 12]

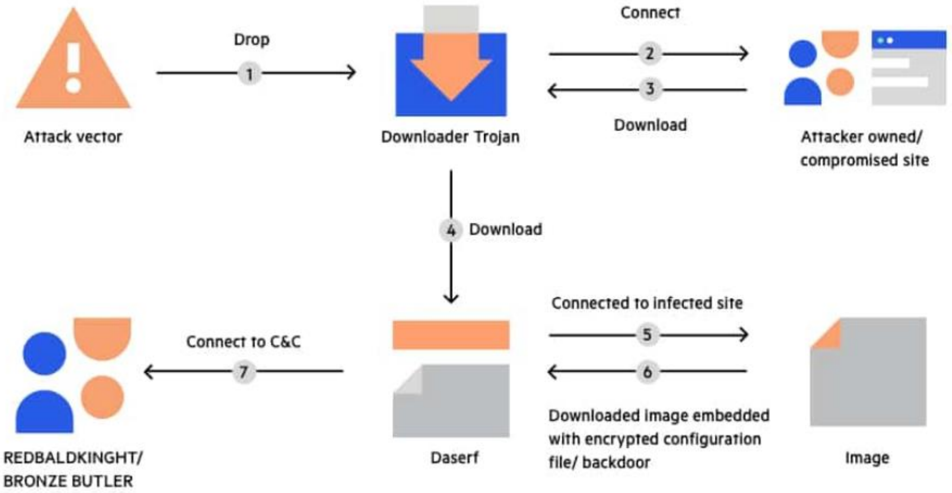

Attack vector
Drop
1
Downloader Trojan
Connect
2
3
Download
Attacker owned/ compromised site
4 Download
Connected to infected site
5
6
Downloaded image embedded with encrypted configuration file/ backdoor
Image
Daserf
Connect to C&C
7
REDBALDKINGHT/ BRONZE BUTLER

Figure 12 Shows how the Trojan Attack the device

-Spyware attacks: the purpose is to gather information and data from the mobile manipulator and the connected user's device and send it to a third party over the internet without any notice or acceptance of the user. That information is obtained usually from cookies, and web browser history. He can also download other software like display advertisements (not necessarily displaying them), or redirect the browser. Spyware does not self-replicate or self-distribute like other "worms".Thus, this results in being capable of monitoring the user's activity and consequently its robot's activity.

-Ransomware attacks: Usually it starts with a phishing email or notification that aims to encrypt all the data generated/linked to the mobile manipulator systems, devices, and applications, and lock the backed up data while preventing users from accessing this data without pay using a Bitcoin payment to the hacker wallet (usually Bitcoin because it is secured payment method).

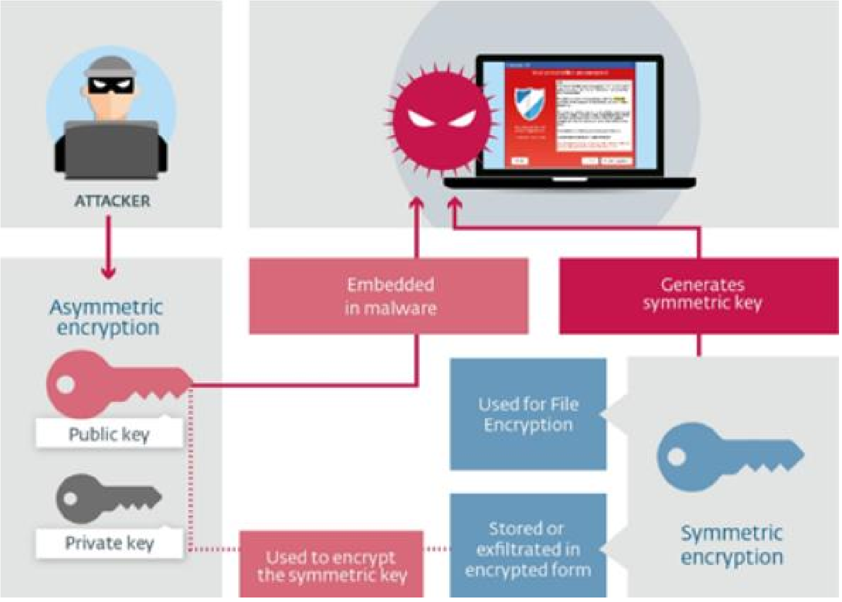


Figure 13 Shows the ransomware attack.

-Rootkit attacks: allow the hacker to have the privilege to control access on a high administrator level with the ability to have access to critical information and data of the mobile manipulator. The aim is to shift mobile manipulator data and systems' logs. Same as Trojan he can be leaving always a backdoor to attacks whenever needed in the future or by installing covert spyware, which affects the confidentiality, integrity, authentication, and privacy aspects.

-Buffer overflow attacks: its mode of operation is to fill device memory with more data than the buffer capacity to control the mobile manipulator and hijack it. The attacker can modify the execution path of the application and, amend the program's execution path to expose data or damage existing files. Buffer overflow is based on two main types: stack overflow attach (when the data kept on the stack is corrupted so the attacker sends a continuous space in memory used to organize data associated with robotic function calls. This vulnerability is found in (C or C++ language) and heap overflow based (occurs where the amount of memory is too large to fit the stack and the written data are not being checked. This attack type is used to affect different robotic security services such as robotic data and systems' authentication, availability, and confidentiality).

-Password cracking attacks: is considered an offline attack because the attacker target the authentication of the mobile manipulator 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: brute force attacks that guess and capture a user's password or personal identification number, or simply by knowing the standard password given by the manufactured company which is rarely changed by some company, 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 attacks (OPGA) [14,15]

-Reverse engineering attacks (person-to-person attacks): their success depends on the attackers' capability to convince their victims inside workers and lure them with money or a higher position in case of a competitor attack. The attacker aims to retrieve critical, and useful information needed to gain access to the mobile manipulator. This targets both data and mobile manipulator systems' privacy, and integrity.

-Surveillance attacks: In other words, there is a peeled eye that controls/looks at all the activities and surroundings of the hacked device especially as we mentioned before the mobile manipulator has a camera and laser scanner that sent live time data which can be controlled/hacked by the attacker. Usually, it is done via creating malicious robotic applications, third-party applications, and fake anti-virus programs masquerading as legitimate ones, and include also fake updates and pop-ups that urge robotic users from clicking on them to fulfill the update task. Malware can be activated even if the user clicks on the exit button. Once the malware is activated, all the user's private information and data are stored and covertly leaked to malicious parties, keeping robotics users and operators under constantly covert surveillance with the ability to control and hijack the operational robot. Thus, this type of attack targets robotic data and systems' confidentiality, integrity, authentication, and privacy.

-Malicious code injection (MCI) attacks or Remote Code Execution (RCE) attacks:
Occurs when the attackers execute malicious codes in order to perform an injection attack in the code of the application. The attacker exploits an input validation flaw in the software to recognize the vulnerabilities in the robotic software as a result of this exploitation flaw the attacker injects a malicious code script and runs it without the user's knowledge.

Phishing attacks: are when the attacker sends messages pretending to be a trusted person/entity (insider worker, or a formal email from a company) which target mobile manipulator users causing them to install malicious masqueraded files, divulging sensitive information such as mobile manipulator credentials, and clicking harmful links. It leads to exposure of the device insurance and leads to compromise and loss of control of the mobile manipulator. This can affect both robot data and systems' privacy, integrity, availability, and authentication processes.

3.2- Communication attacks.

In this section, we will try to cover all the possible scenarios of the attacks on mobile manipulator which is related to the network and communication between the mobile manipulator and the console which is usually a computer.[16,17]

-Jamming attacks: is a type of denial of service which prevents other nodes from using the channel to communicate with each other it interrupts and disrupts the robot-to-robot and robot-to-human communication with the aim to suspend further robotic activities and jam any sort of communication and control. Thus, targeting both systems and data availability which leads to complete blockage of the mobile manipulator.

-De-authentication attacks: is a disruptive technique that hit the wireless connections it is also a type of denial-of-service it rends to temporarily, periodically, or disable the mobile manipulator from being able to connect to his operator disturb the communication between operator and robot, and prevent it from re-connecting back and hijacking the mobile manipulator. This aims to target the availability, authentication, and integrity of both data and systems.

-Traffic analysis attacks: since some robotic systems rely on open wireless communications this attack occurs when the hacker takes access to the same network used by the mobile manipulator robot so he captures all the network traffic and analyzes them to learn about the company here the hack is not on the system or credentials but on the network 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 retrieving 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. Using encrypted traffic can secure the content but doesn’t prevent the attacker to obtain some important information.

-Eavesdropping attacks /sniffing or snooping attacks: this type of attack takes advantage of the unsecured network communication to monitor the transmitted mobile manipulator traffic data whether it is encrypted or un-encrypted open channels communications. This leads to collecting all the sensitive information about the mobile manipulator system and the current task done by it. It targets the robot’s confidential data and privacy. Some advanced eavesdropping attacks recover the data via an information-gathering process in the form of a “cloning and replay” for the attack.

-False data injection attacks (FDIA): it happens by compromising the reading of the sensor in such a tricky way that undetected any errors introduced in the calculations of values and state variables. It is one of the top priority issues to deal with in the ROS. It targets the privacy and integrity of the robotic data and the availability of robots, by intercepting and modifying their payload. It is usually done using the initial interception of the ongoing communication and changing it by injecting false data, which deviates the robots from performing their intended activity in an accurate manner or leaves them prone to response delays. This cause the inaccuracy of the mobile manipulator which leads to additional cost due to time-wasting and maintenance.

-Denial of service attacks (DOS): can be done from everywhere in the world which makes it hard to investigate or catch the attacker if he is in a different country of the victim. It aims to prevent mobile manipulator users from accessing the robotic systems and the operator device. DoS is done by sending multiple requests to the server, to overload servers or the operating systems with a bunch of data or access to the processor or main memory. It hit the weakness in the network infrastructure or the security system. These attacks can involve a bunch of different systems shelling a specific service with requests for access to this service. In this type of attack, a big number of computers are involved, and take part each device sends a small part of the whole data flood organized by the hacker, but to involve all these computers the hacker infects them first with a virus-like “Trojan or worm” .The IP address of compromised machines - dubbed zombies or bots - is sent back to the criminal, who will use it to launch a “DDoS”. The network of zombie machines is sometimes known as a “Botnet”.

-Replay attacks: these occur when the attacker eavesdrops on secure network communication, by storing and replaying old messages sent between the mobile manipulator and its operator device to disrupt the ongoing traffic. It is considered one of the most dangerous frequent attacks because the attacker does not need advanced skills to unpack an encrypted message after analyzing it from the network. The replay attack's mechanism is based on capturing the transmitted message sent by the mobile manipulator to its operator device which in this case can be the login credentials, live RGB-D image, and map drawn by the laser scanner it this affects the availability of both data and robotic systems.

-Masquerading attacks: are ranked as one of the main electronic crimes perpetrated by such malware attacks. This is done by using a fake identity such as a network identity to take unauthorized access to the operator's computer which in his turn sent to another robotic device connected to this device or by forming a black hole for sent data. The objectives of those attacks are either by affecting the performance, or speed of the mobile manipulator which leads to non-accurate task accomplishment and worker integrity.

-Man-in-the-Middle (MiMA) attacks: it is usually done via redirecting the legitimate user to a website that is totally similar to the one used by the user, once he put the credentials on the fake website it is sent to the hacker. It occurs when an attacker is capable of actively listening and intercepting the communication between two robotic entities or nodes, altering the information and injecting it without being detected. This allows the attacker to control the communication between these legitimate entities. 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 communication channel and either actively or passively eavesdrop. This type of attack targets the mobile manipulator data's confidentiality, integrity, and authentication.

-Identity attacks: 70% of these attacks start with phishing. This attack includes identity revealing attacks, which consist of retrieving the identity of the robot to put its operator's privacy at risk. Equally important, the attacker can track the location of the robot, which exposes all the needed information and the geographical location of robotics systems along with their users and devices.

-Network impersonation attacks: occur by obtaining the credentials of the mobile manipulator user in a given network by claiming its network ID. This allows an attacker to advertise fake data which confuses other network entities and floods the robotic networks via DoS attacks.[18]

-Message tampering–fabrication–alteration attacks: it changes or deletes the resource without any authorization. It is done by breaking the integrity of the send/received messages, which is done by creating fake messages or modifying them. In this attack, the authentication and data integrity is affected. This can lead to a change in the mobile manipulator events log.

-Illusion attacks or capabilities: In the case of a mobile manipulator which is not connected via the internet, this attack is done by putting a compromised robot in the network to generate false data. Which leads to the spread of this false data over the network. In the mobile manipulator case, fake messages are capable of changing the decision of the robot controller.

3.3- Hardware attacks.

These attacks can vary from:

-Hacking (pishing, Hardware Trojan) is done by implementing those viruses that left a back-door for the attacker to gain another attack later whenever needed on the mobile manipulator this is done usually by insider/workers or during the maintenance. They can have full access to the whole hardware, which could lead to data loss or mobile manipulator use depending on the purpose and the target of the hacker. In addition to stole data physically without the need for any virus, any insider worker can make it.

-Physical damage is done by a mad employee or paid by a competitor company.

Chapter 4: Risk Study For Implementing The Mobile Manipulator.

The risk management process starts with its main component, Risk Assessment. However, risk assessment is a continuous process that should be maintained during the system lifecycle. Vulnerabilities and threats usually indicate the likelihood of an attack. This thesis emphasizes the effects of cyber-attacks on the functionality of the Mobile Manipulator. Hence, an impact-oriented analysis is adopted and only vulnerabilities that lead to those kinds of impacts are investigated. This means that although the mobile manipulator and its different components may be subjected to a spectrum of vulnerabilities, we are not assessing them all. We are only analyzing known vulnerabilities that may lead to harmful impacts on the robot.
In order to have a wide view of all the risks and their likelihood to happen, we tailored a table that combines Threat Risk Assessment (TRA) which evaluates the potential losses through any act or condition exploiting the vulnerability to cause this loss it consists in the term of threat ability to exploit vulnerabilities with Failure Mode & effect analysis (FMEA) with the which is systematic process that requires thoughtful consideration of all the potential failure modes associated with a new design or process, failures are prioritized according to their seriousness level and consequences, how frequently they occur or have occurred, and how easily the threat can be mitigated. The purpose of the FMEA is to take action to avoid failures or decrease their consequences, starting with high-priority threats.

4.1 Risk Modeling

All of the security risk analyses are based on two factors: the likelihood of a successful attack against an asset, and the impact of the attack.
Usual information security overviews classify cyber threats into four fields: confidentiality, integrity, availability, and authentification of the mobile manipulator and its information.

For example, according to the results obtained from 20 expert responders (members of the automatic control and robotics community) to a survey performed by ["An experimental security analysis of an industrial robot controller, in security and privacy"], "30% had robots accessible from the Internet, 76% never performed a professional cyber security assessment on their infrastructure, and more than 50% of the respondents did not consider cyber-attacks a realistic threat".[14] This study left us fearfully worried about the security measure that is considered while manufacturing and performing robotic systems which surely include the mobile manipulator. For this reason, we will study all the potential risk and their impacts and the likelihood to try to reduce this attack in the future.

Qualitative risk analysis.

A mobile manipulator can be subjected as we mentioned before to a big variety of threats from insiders/external threats. Using a virus threat to stole the data, take control of it, or cause a malfunction.

In this section we will try to list the potential dangers of the mobile manipulator and the level of impact that can be caused due to those dangers:

Firstly, threats can alternate the required operation from the mobile manipulator in a physical way. Threats could occur by accidental situations by inexperienced workers that may not know how to operate it well, or due to their lack of attention since the mobile manipulator is a dynamic robot, also an attack from an insider that can include some virus or destroy the hardware, or natural conditions like earthquakes, floods, humidity which affect the electric circuit. Expiration of the life span of the components could cause five different impacts on the mobile manipulator which are the following:

1. Partial damage, which causes malfunction.
2. Destruction, therefore dysfunctionality of the robot.
3. Disruption, entails the interruption of total/partial robot components.
4. Degradation, causes the decrease of the range of capability of any robot component over time.
5. Unexpected behavior, which could be considered as a degradation of the whole mobile manipulator, not just a component, usually causes imprecision of mission performance or wrong command.

Secondly, cyber threats can affect the normal operation mode in a virtual way without the need to be physically in the operation site, that is, threads can modify the information gathered, stored, or transmitted by the robot. These threads have more impact on external entities than on the mobile manipulator itself. In this way, we have listed the impact caused by cyber threats into three groups, which are as follows:

1. Issues associated with robot manufacturers or open-source developers (drivers and core software).
2. Issues associated with third-party solutions (libraries) needed by robot manufacturer applications.
3. General vulnerabilities associated with the overall software components of the robot which in some cases does not consider high security.

In addition, we model the risk related to the attack in terms of the final user. Here we can identify three groups of final users for the mobile manipulator such as commercial users, and domestic and high-level organizations, in our work we are mainly focusing on a commercial one.

The risk to commercial and business can be classified as follow:
1. Intellectual property, which could be done by a competitor company.
2. Economic impact which includes the fixing cost of the damaged assets and the loss of profit caused by repairing the damage.
3. Destroy company reputation if the attack was published (Usually this type of attack is published on the dark web because it is the safer way)
4. Economic damages were caused by the stealing of sensitive information related to the company plant.

Risk assessed to domestic users can be classified as follow:
1. Economic risk which can be explained by the additional cost that requires fixing the mobile manipulator on the component side and/or environment side.
2. Psychological, this includes the leakage of some private information (Low Risk)
3. Physical damage if a human got injured. (Low risk)

Finally, cyber threats can affect also the component of the mobile manipulator which are the firmware in a physical or virtual way. As we mentioned before the mobile manipulator has sensors and a camera that can be beneficial for the hacker so we will list the component and the risk effect in the order of most dangerous and most likely to happen to the lowest:
1. Camera: it is present in the mobile manipulator and is the most likely to get hacked by the attacker to take a live RGB-D image which may be sensitive if the industry is developing a new product or even stealing some sensitive information.
2. Sensor: the mobile manipulator have a laser sensor to draw a map of the operation, IMU for the accuracy of movement. So the hacker can steal the map of the plant which can be the chain

of the production line or cause malfunction by confusion of the IMU. Both cause full disclosure of the scenario activity.

3. Range: track the path of the mobile manipulator which causes a record of some private activities.

4. Localization: The attacker can localize specifically the location of the mobile manipulator live which can help to stole it or make a physical attack.

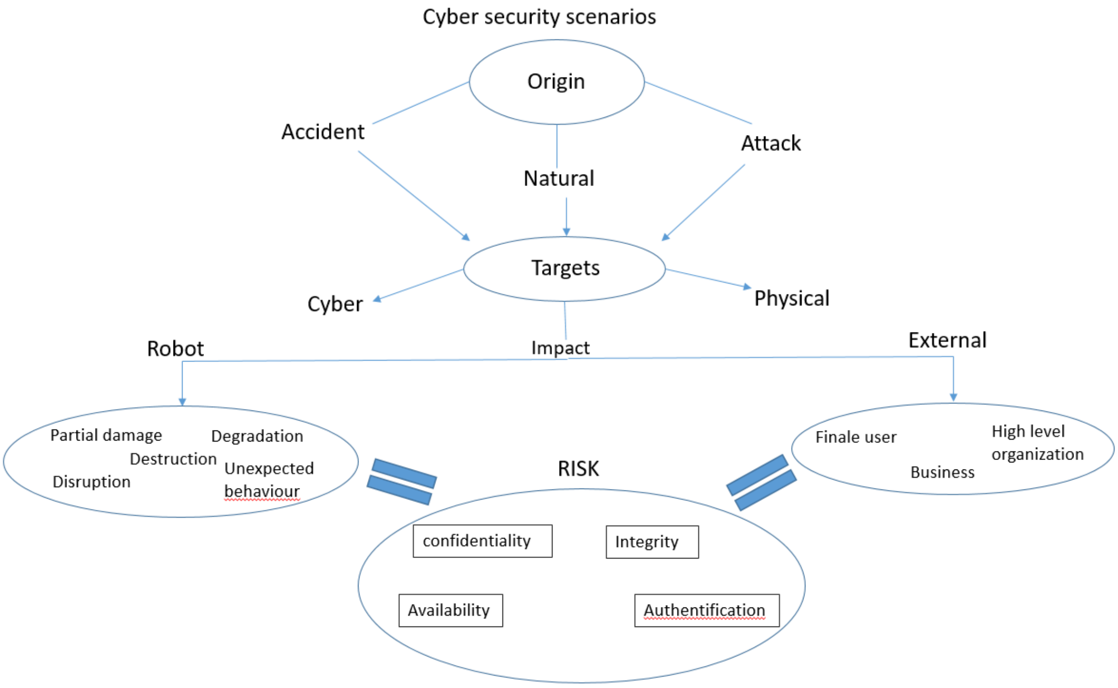


Figure 14 Shows the Cyber Security Scenarios source and it's targets .

4.2- Quantitative Risk Assessment Determination:

Quantitative risk assessment estimates the level of adverse effects of the release of specific waste from the site. This is a tool for calculating existing and future health risk figures associated with exposure using the complete identified pathway.

Definition of labels:

1) Threat Event: refers to the threat that is currently being analyzed.

2) Threat Sources: refer to the threat source, which can be Internal which refers to a worker that works currently in the company, External which is a hacker nonemployed or from a competitive company.

3) Capability: this is one of the characteristics of the threat source. An attacker with high capability is one with a high level of expertise and is well-resourced. Because of the increasing interest in cyber-security, there is an increasing number of highly capable threat sources. Especially, in a scientific and research environment. The reader should note that the attacks we are implementing can be implemented by a person with moderate or even low capabilities.

4) Intent: this is one of the characteristics of the threat source. The adversary seeks to undermine critical functions of the system and may result in physical damage by causing loss of availability.

5) Targeting: this is one of the characteristics of the threat source. The adversary targets a specific mission or function within an organization (i.e. the target of the attack is not random, however, the threats discussed here are not unique to the robots).

Capability, intent, targeting scale: (Very high=5, High=4, Medium=3, Low=2, Very Low=1).

6) Cause: refer to the factor glitch that the attacker exploits to hack the mobile manipulator.

7) Consequences: are the result/ effects that are caused if the attack was successful.

8) Impact on: give a quantitative assessment of how much the impact affects the following factors if the attack was successful the scale is graded on : [1=low, 2=medium, 3= high].

-Confidentiality.

-Integrity

-Availability

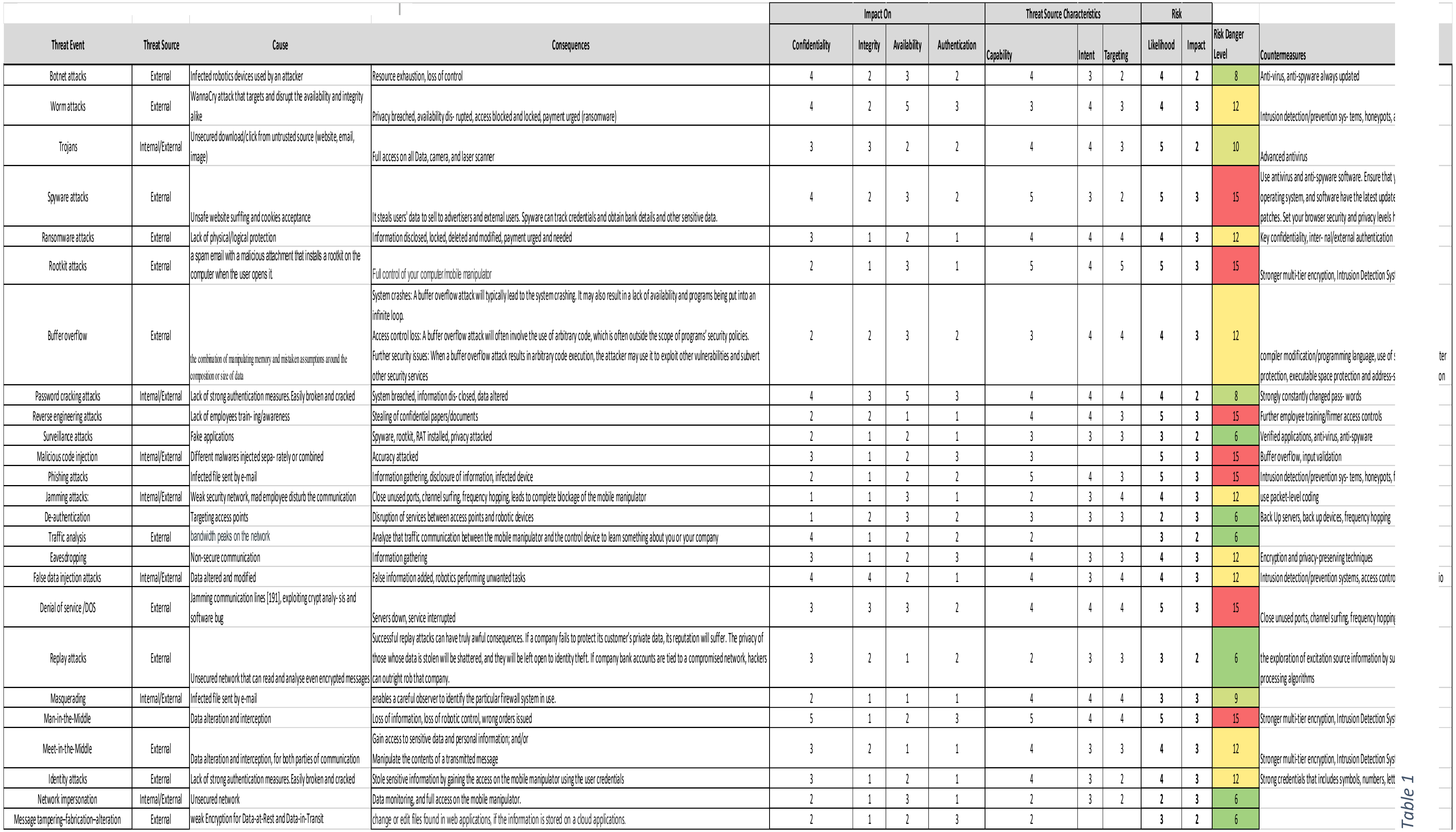
-Authentication.

9) Overall Likelihood: this is a combination of the likelihood of attack initiation and the likelihood initiated attack succeeds. If both items are high then the overall likelihood is high. If one of them is moderate and the other one is high then the overall likelihood is moderate.

10) Level of impact: severe or catastrophic effect on the system means high impact. For the first attack, while Windows operating systems are highly affected by the attack, Linux operating systems are moderately affected because they only take the first 15 route advertisements and ignore the remaining.

11) Risk: this is the final risk assessment measure, which is the product of the overall likelihood and the level of impact. The moderate likelihood and moderate impact result in moderate risk as in the case of the IPv6 RA floods threat. Similarly, high likelihood and high impact result in high risk as in the case of the deauthentication threat.

12) Countermeasures: Some suggestions to avoid/ mitigate the risk in case the attacker starts its attack on the mobile manipulator.



				Impact On				Threat Source Characteristics			Risk				
Threat Event	Threat Source	Cause	Consequences	Confidentiality	Integrity	Availability	Authentication	Capability	Intent	Targeting	Likelihood	Impact	Risk Danger Level	Countermeasures	
Botnet attacks	External	Infected robotics devices used by an attacker	Resource exhaustion, loss of control	4	2	3	2	4	3	2	4	2	8	Anti-virus, anti-spyware always updated	
Worm attacks	External	WannaCry attack that targets and disrupt the availability and integrity alike	Privacy breached, availability dis- rupted, access blocked and locked, payment urged (ransomware)	4	2	5	3	3	4	3	4	3	12	Intrusion detection/prevention sys- tems, honeypots, a	
Trojans	Internal/External	Unsecured download/click from untrusted source (website, email, image)	Full access on all Data, camera, and laser scanner	3	3	2	2	4	4	3	5	2	10	Advanced antivirus	
Spyware attacks	External	Unsafe website surffing and cookies acceptance	It steals users' data to sell to advertisers and external users. Spyware can track credentials and obtain bank details and other sensitive data.	4	2	3	2	5	3	2	5	3	15	Use antivirus and anti-spyware software. Ensure that y operating system, and software have the latest update patches. Set your browser security and privacy levels h	
Ransomware attacks	External	Lack of physical/logical protection	Information disclosed, locked, deleted and modified, payment urged and needed	3	1	2	1	4	4	4	4	3	12	Key confidentiality, inter- nal/external authentication	
Rootkit attacks	External	a spam email with a malicious attachment that installs a rootkit on the computer when the user opens it.	Full control of your computer/mobile manipulator	2	1	3	1	5	4	5	5	3	15	Stronger multi-tier encryption, Intrusion Detection Syst	
Buffer overflow	External	the combination of manipulating memory and mistaken assumptions around the composition or size of data	System crashes: A buffer overflow attack will typically lead to the system crashing. It may also result in a lack of availability and programs being put into an infinite loop. Access control loss: A buffer overflow attack will often involve the use of arbitrary code, which is often outside the scope of programs' security policies. Further security issues: When a buffer overflow attack results in arbitrary code execution, the attacker may use it to exploit other vulnerabilities and subvert other security services	2	2	3	2	3	4	4	4	3	12	compiler modification/programming language, use of s protection, executable space protection and address-s	ter on
Password cracking attacks	Internal/External	Lack of strong authentication measures.Easily broken and cracked	System breached, information dis- closed, data altered	4	3	5	3	4	4	4	4	2	8	Strongly constantly changed pass- words	
Reverse engineering attacks		Lack of employees train- ing/awareness	Stealing of confidential papers/documents	2	2	1	1	4	4	3	5	3	15	Further employee training/firmer access controls	
Surveillance attacks		Fake applications	Spyware, rootkit, RAT installed, privacy attacked	2	1	2	1	3	3	3	3	2	6	Verified applications, anti-virus, anti-spyware	
Malicious code injection	Internal/External	Different malwares injected sepa- rately or combined	Accuracy attacked	3	1	2	3	3			5	3	15	Buffer overflow, input validation	
Phishing attacks		Infected file sent by e-mail	Information gathering, disclosure of information, infected device	2	1	2	2	5	4	3	5	3	15	Intrusion detection/prevention sys- tems, honeypots, f	
Jamming attacks:	Internal/External	Weak security network, mad employee disturb the communication	Close unused ports, channel surfing, frequency hopping, leads to complete blockage of the mobile manipulator	1	1	3	1	2	3	4	4	3	12	use packet-level coding	
De-authentication		Targeting access points	Disruption of services between access points and robotic devices	1	2	3	2	3	3	3	2	3	6	Back Up servers, back up devices, frequency hopping	
Traffic analysis	External	bandwidth peaks on the network	Analyze that traffic communication between the mobile manipulator and the control device to learn something about you or your company	4	1	2	2	2			3	2	6		
Eavesdropping		Non-secure communication	Information gathering	3	1	2	3	4	3	3	4	3	12	Encryption and privacy-preserving techniques	
False data injection attacks	Internal/External	Data altered and modified	False information added, robotics performing unwanted tasks	4	4	2	1	4	3	4	4	3	12	Intrusion detection/prevention systems, access contro	io
Denial of service /DOS	External	Jamming communication lines [191], exploiting crypt analy- sis and software bug	Servers down, service interrupted	3	3	3	2	4	4	4	5	3	15	Close unused ports, channel surfing, frequency hoppin	
Replay attacks	External	Unsecured network that can read and analyse even encrypted messages	Successful replay attacks can have truly awful consequences. If a company fails to protect its customer's private data, its reputation will suffer. The privacy of those whose data is stolen will be shattered, and they will be left open to identity theft. If company bank accounts are tied to a compromised network, hackers can outright rob that company.	3	2	1	2	2	3	3	3	2	6	the exploration of excitation source information by su processing algorithms	
Masquerading	Internal/External	Infected file sent by e-mail	enables a careful observer to identify the particular firewall system in use.	2	1	1	1	4	4	4	3	3	9		
Man-in-the-Middle		Data alteration and interception	Loss of information, loss of robotic control, wrong orders issued	5	1	2	3	5	4	4	5	3	15	Stronger multi-tier encryption, Intrusion Detection Syst	
Meet-in-the-Middle	External	Data alteration and interception, for both parties of communication	Gain access to sensitive data and personal information; and/or Manipulate the contents of a transmitted message	3	2	1	1	4	3	3	4	3	12	Stronger multi-tier encryption, Intrusion Detection Syst	
Identity attacks	External	Lack of strong authentication measures.Easily broken and cracked	Stole sensitive information by gaining the access on the mobile manipulator using the user credentials	3	1	2	1	4	3	2	4	3	12	Strong credentials that includes symbols, numbers, lett	
Network impersonation	Internal/External	Unsecured network	Data monitoring, and full access on the mobile manipulator.	2	1	3	1	2	3	2	2	3	6		
Message tampering–fabrication–alteration	External	weak Encryption for Data-at-Rest and Data-in-Transit	change or edit files found in web applications, if the information is stored on a cloud applications.	2	1	2	3	2			3	2	6		

Table 1

Figure 15Shows a complete FMEA risk study

After studying the risk their cause, consequences, impact, and the likelihood we find that we have such threats that have a higher level of occurring which should be treated first because they are the most dangerous [Spyware, Rootkit, pishing, malicious code injection, DOS, Man In The Middle, Reverse engineering] lower level risk doesn't mean to not take any step to avoid them they should be also avoided. In the following section, we will list the solution and countermeasure that can be adopted by the company implementing a mobile manipulator to prevent or mitigate the hack or its effect. All the solutions are not guaranteed to stop or eliminate the hack such hacker are professional and they are improving to continue the hacking by finding some glitch to initiate their attack.

4.3 Solutions and countermeasures.

In the following section, we will try to cover all possible solutions and countermeasures to avoid and limit the likelihood of a cyber-attack on the mobile manipulator which can be implemented for robotics in general.

4.3.1 Cyber threats intelligence

The Cyber Threat Intelligence (CTI) is built on gathered information about robotic threats and threat actors that would help in preventing harmful cyber-events built on the Advanced Persistent Threat (APT) concept through early detection and prevention. In fact, CTI gathers information from human intelligence (HUMINT), Open Source intelligence (INT), technical intelligence (TECHINT), and intelligence gathered from the dark web (silk road) [19,20]. Hence the robotic domain can be an enhanced evidence-based malware analysis, security incident outcome utility, and data/information security controls.

CIT can be categorized into three types of intelligence as follows:

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

In fact, the usage of CTI, especially in supply chains and Industry 4.0 [21], allows for a faster predictive and reactive Incident Response Service (IRS) [22] through the detection of cyber-threat, risk assessment, and log inspection and monitoring. This allows the combination of the human-machine analytical capability to reach a higher level of information security (INFOSEC) and it depends 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 upholds the overall risk assessment and risk management policies and procedures.
- Development of predictive cyber-security to guarantee a higher level of threat detection in a precise and suitable manner with the least false-positive and false-negative rates.
- Enhanced incident response systems that combine human-machine assets, especially in detecting and responding to incidents using ML and AI (Machine Learning and Artificial Intelligence) security measures before, during, and after the event has happened, through early detection, ongoing prevention, and lessons learned, respectively.
- Enhanced decision making which is achieved in a much more precise and suitable manner based on the information about a cyber event including an attack, intrusion, defense…

4.3.2. Active security awareness

The Active Security Awareness (ASA) program demands being furthermore extended and adopted because it can highly reduce robotic threats that cannot be addressed by using robotic software and hardware devices. This demands an extensive focus on the security and safety of human elements business on the adoption of different security awareness programs, training, modules, and (online) lessons to help rising an effective and affordable security awareness culture targeting all the personnel working in the field and domain of robotics [24].

The advantage of applying ASA are:

- Professionally developing of Solid security policies to enforce security to show a resilient commitment to fulfilling the needed cyber-security and mobile manipulator security.
- Security requirement analysis formulate effective policies and management procedures and apply them in the robotic domain.
- Designating formal security processes which help in designing secure solutions in the noncryptography domain, containing the configuration and deployment of firewalls, honeypots, intrusion detection, and prevention systems that are used on the Robotic Operating Systems (ROSs) and the corresponding applications.
- Reduced operational threats which would result in restricting the drain of financial resources and losses, whereas increasing the terms of economy and investment.

- Real-time security awareness generates up-to-date security awareness against security risks, threats, and issues that surround the robotic domain.
- Advanced employee education elevates a higher real-time security awareness and knowledge linked to employees' expected behavior, activities, and responsibilities to effectively protect and prevent any leakage of robotic information.

4.3.3 Active response: detection and prevention

In active response, detective and preventive procedures are fundamental to provide additional security protection via an easier and less complex implementation of detective and preventive security procedures including the usage of centralized and decentralized hybrid, lightweight [25,26] and AI-based [27,28] intrusion detection and intrusion prevention systems, in addition to antivirus mechanisms to trigger an automated response through constant and continuous monitoring. Such usage can bring many benefits to the robotic domain, particularly in the IIoT field.

- AI-based detection through the adoption of ML-based "Machine Learning-Based" mechanisms to guarantee a higher precision in a timely manner.
- Hybrid detection involves the combination of signature-based, behavior-based, and anomaly-based IDS/IPS patterns to include a larger variety of robotic cyber-attacks and threats.
- Ensuring a higher level of detection and prevention via constant vulnerability monitoring through a constant vulnerability check, assessment, and management of the up-to-date systems, applications, and security patches.
- Advanced activity monitoring allows the consecutive monitoring of a robotic device's behavior over time and compares it to detect whether the behavior threshold is different than the normal pattern (rogue device).
- Easier deployment guarantees an easier integration around the robotic systems, including on networks, devices, software, firmware, or even robotic operating systems, to guarantee stable detection and protection.
- Easier management to guarantee a faster response for threat responders and (cyber) security professionals implicating IT security.
- Enhanced access management which specifies the right data categorization and protection through enhanced authentication mechanisms such as privileged account management, or securing robotic communications through endpoint network encryption.

4.3.4 Active management: precaution and correction

Active management contains the adoption of both precautions and corrective procedures. Precaution is fundamental in the early stages of any robotic design. In fact, other security precocious procedures should also be considered during the early phases of robotic testing and design. This is fundamentally required to guarantee that safety and security procedures are considered by both manufacturers and integrators to guarantee efficient use. Furthermore, robotic operators must also grow a certain degree of awareness and training, in addition to a screening process to forbid their use for criminal or terrorist purposes. In addition, corrective procedures are also vital as they can allow robotic systems to self-healing. Thus, being capable of restoring their operational capabilities independently without any serious interruption(s). Corrective procedures can be applied to isolate infected robotics systems, sensors, and devices from the other operational devices to inhibit further damage and attack escalation over a given system, especially if the attacks target the availability of robotic systems in case of a threat that duplicate itself like the case of worm attack.

4.3.5 Robotic security protection

In spite of the attacks that surround the embedded robotic systems' architecture, effective countermeasures can be adapted and used to hinder security attacks [29]. These countermeasures can help with overcoming any exploitable security gaps. Next, we list the main actions that should be taken to prevent robots' security attacks.

- Hardware protection Robots have been disposed to different types of hardware attacks, since their early stage of manufacturing and maintenance. These results, hardware testing, and monitoring are key to preventing any future exploitation [29]. Many solutions have been presented this includes isolating Internet Protocol (IP) core mechanisms [30], combined with implementing solutions for payload detection [31], and the implementation of the Integrated Circuit (IC) fingerprinting technique [32].
- Firmware protection securing software demands considering the firmware aspect of robots. Hence, it is fundamental to guarantee that the software patches are always updated, protected, and always monitored, and tested for any suspicious activity to protect the firmware, by the adoption of a general standardized operating system such as NuttX OS [29]. This prohibits the exploitation of the firmware and decreases the probability of an attack. Whilst, it is also advised to add an authentication process to secure robots. Furthermore, the utilization of message

authentication and encryption mechanisms helps ensure secure communications between robots and their control systems.

• Application protection it is fundamental to limit, reduce and overcome the probability of an application being threatened by any possible cyber-attack. Doing so would highly demand the need to develop a well-built, well-defined, and well-secured application code, that prohibits any potential code exploitation. Hence, this makes the robot's control system less tended to modification attempt(s) or malicious code injection. Therefore, before designing any application, each application must undergo a security testing phase to identify any potential weakness and/or security gap that can be detected. This helps by decreasing and prohibiting further exploitation and future cyber-attack(s). [29]

4.3.6 System hardening

Robotics' system issues started ongoing with the design phase. Although, lately, more concern has been given to overcoming this limitation with the focus on ensuring how to secure robotic system's software, hardware, and communication. Thus, lately, various solutions were presented. For this case, two solutions were presented: one was to incorporate a Control Flow Integrity (CFI) check into the Real-Time Operating System (RTOS) [33]. The other one was to invent a Control-Flow Attestation for Embedded Systems Software (C-FLAT) to check remotely the CFI on a given embedded device in [34]. An analyzed cyber-physical security threats targeting the communication link between "Adept MobileRobots" platforms and their clients [35,36] the authors analyzed the vulnerabilities found in the communication link used by robotic applications. Next, the authors targeted confidentiality integrity, availability, and authentication using an impact-oriented approach. This was done by following the discount risk assessment form issued by the National Institute of Standards and Technology (NIST) [37]. The authors designed an open-source Robot Attack Tool (RAT). Furthermore, the level of risk of the attacks carried out was qualitatively assessed with the identification of physical consequences. The goal is to improve the safety and security of the automated platform by increasing awareness and increasing understanding of new emerging threats. Furthermore, with regard to risk assessment, a comprehensive survey of existing designs and risk assessment studies have taken into account both the safety and security of industrial infrastructures[38]. a new method (was introduced) that identifies risks to mobile agent systems [39], another adapted a classic risk assessment approach to be applied during the initial phases of the development process for autonomous systems including service robots [40]. Those analyses were based on the collaborative method based on the HAZOP tags (HAZard OPerability), which was applied to Unified Modeling Language (UML) models. The presented risk assessment approach was applied to an assistive robot, which provided assistance for standing, sitting, walking, and health monitoring which is similar approach for the mobile manipulaor. Then physical indicators were investigated for cyber-attacks on a rescue robot [41] this study found how it could negatively impact robotics rescue and impair emergency response procedures. Furthermore, a flexible and portable large-scale robotic wooden construction platform [42]. Skillman as a framework for planning and execution using a module with empirical knowledge to integrate perception, planning, knowledge-based inference, and implementation of various skills such as robot paths [43]. However, further study is also needed from a cyber-security perspective, so it was introduced to recover robotic vehicles (RVs) from various (physical) sensor attacks, using a state-space predictive model adoption technology based on general system identification technology and using sensor measurement prediction [44]. When attacked, the sensors can isolate and recover the compromised sensors to prevent further damage. Experimental results, conducted on a quad rotor and a rover, revealed the ability to safely recover the mobile robot from various attacks and prevent a collision. Lately, it was provided an original software/hardware solution for a global low-level architecture for long-range, easily repeatable remote sensing agile robots in different environments and on different platforms (land, surface, submarine, and air) [45]. Also, we discussed the judicious choice of Ardupilot as autopilot which means a robot that drives itself after programming it like a mobile manipulator and presented the ESP32 as a new cost-effective and power-efficient hardware solution. Experimental results showed the ease of tracking and achieving levels of independence, except for flying devices (Drone).

Furthermore "ScatterID" is a lightweight system that connects light and battery backscatter tags to single-antenna bots to defeat Sybil attacks [46]. The Experimental results on the iRobot Create platform reveal an accuracy level of 96.4% for identity verification.

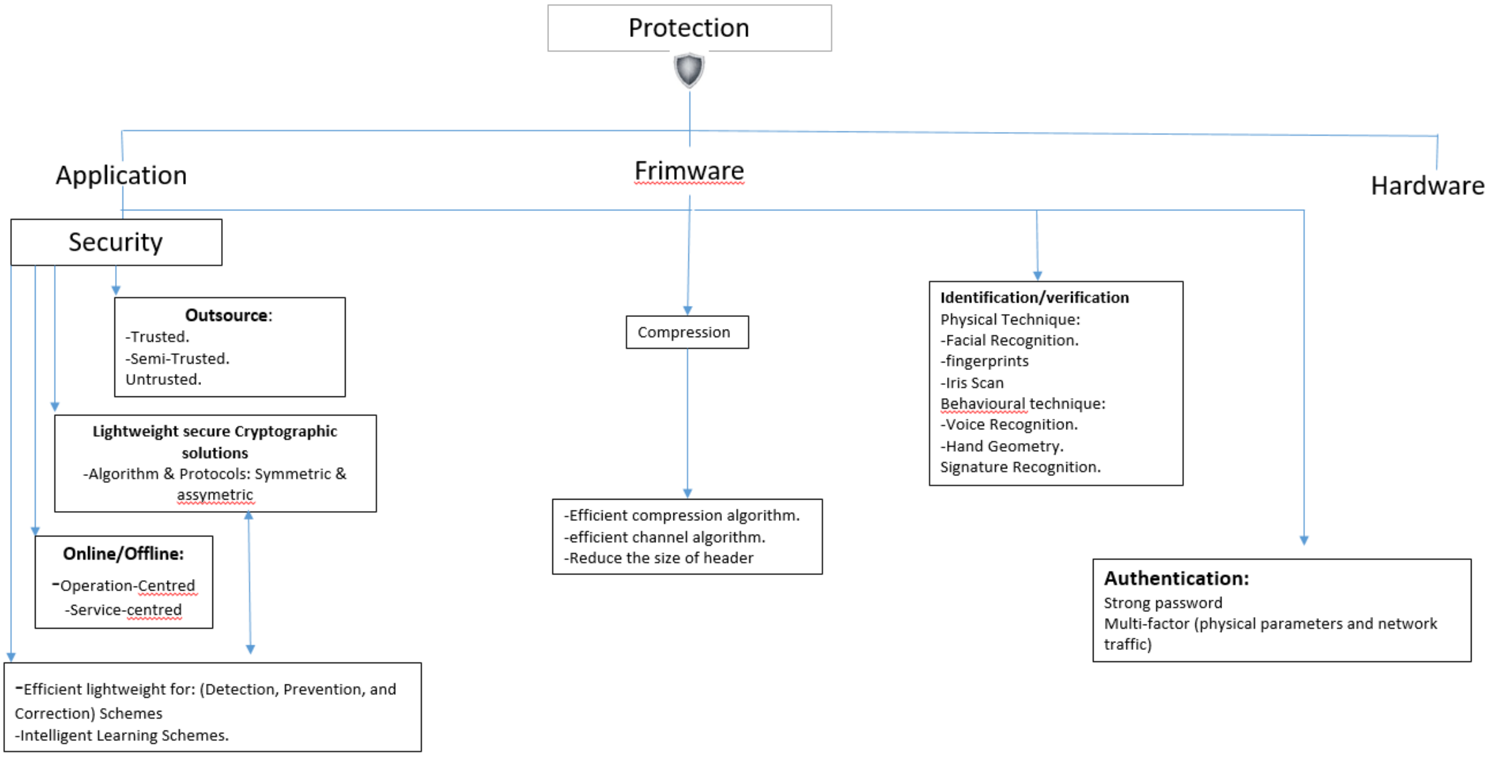

Protection
Application
Frimware
Hardware
Security
Outsource:
-Trusted.
-Semi-Trusted.
Untrusted.
Lightweight secure Cryptographic solutions
-Algorithm & Protocols: Symmetric & assymetric
Online/Offline:
-Operation-Centred
-Service-centred
-Efficient lightweight for: (Detection, Prevention, and Correction) Schemes
-Intelligent Learning Schemes.
Compression
-Efficient compression algorithm.
-efficient channel algorithm.
-Reduce the size of header
Identification/verification
Physical Technique:
-Facial Recognition.
-fingerprints
-Iris Scan
Behavioural technique:
-Voice Recognition.
-Hand Geometry.
Signature Recognition.
Authentication:
Strong password
Multi-factor (physical parameters and network traffic)

Figure 16 Protection Requirements for the Mobile Manipulaor

4.3.7 Robotic systems: identification, verification, and authentication

In an automated system, both identification and verification are necessary to prevent unauthorized access to mobile manipulator control machines. Hence, biometrics systems and technologies are dedicated to playing a major role in this context. However, before a biometric system can be set up, a database is also needed to securely store biometric templates. This allows the stored data to be used for future use this process is known as the registration process.

In order to achieve the process of identification and/or verification, several biometric technologies are needed, these biometric techniques can be divided into physical and behavioral biometric techniques. Physical biometric techniques include facial recognition, fingerprint, and iris scan. Behavioral biometric techniques are mainly based on voice recognition, hand geometry recognition, and signature recognition. In fact, authentication is primarily used as the first line of defense ensuring that both the source and the destination are authenticated [47]. Authentication can also be based on multi-factor authentication, where a second security mechanism is required to access a system in addition to a password or encrypted first-factor authentication that only requires the entry of a single password or secret key. This makes the attack probability of success low compared to just one factor. In the following, we list several bot authentication systems. In fact, an investigation of the relationship between password protocols and other cryptographic fundamentals realized that password-authenticated key exchange and public-key cryptography are incomparable under black-box reductions. Initially, a study was the first to introduce a remote user authentication scheme using a password. Another introduced a two-factor authentication system based on the use of smart cards (badges). Similar authentication methods for electronic payment systems. Lately improved two-factor user authentication scheme to protect wireless sensor networks (WSNs) that the mobile manipulator uses to communicate [48,49]. This system uses only the hash function with successful user authentication that uses three message exchanges. Both security and performance analysis indicates that it is more secure and efficient compared to other well-known authentication systems. “Das et al.” Introduced the first smart card-based password authentication scheme for WSNs [50]. However, the proposed solution lacks mutual authentication and user anonymity [51]. In addition, a cross-authentication scheme based on temporal credentials between the user, the gateway node (GWN), and the sensor node. Security and performance analysis indicates that this system provides more security features and a high level of security without any connection, computation, or storage burdens. Furthermore, a systematic evaluation framework for plans to be objectively evaluated. Evaluation results indicate that not all current schemes are perfect. Hence, more work is needed in this regard, for an advanced credential-based timeline security scheme with mutual authentication and key agreement for WSNs in [52] by using a lightweight one-way hash compute, this authentication system significantly reduces the execution cost against various attacks including internal attacks. Meanwhile, a realistic lightweight anonymous authentication protocol to secure access to real-time application data for WSN [53] this solution provides more security features with high levels of security at a low cost for connection and account. Lately, we find revealed that the initial authentication based on the temporal credentials cross-authentication scheme (GWN) was vulnerable to various types of attacks, and provided a scheme that leads to further reductions in computational cost [54] Thus, reducing security flaws and improving performance, making it more suitable for WSN applications. Hence, an efficient two-factor authentication scheme was introduced for a single gateway environment that achieves user anonymity, while preventing desynchronization attacks [55]. However, these models were not sufficiently scalable in multi-gated industrial WSNs, but they have been shown to provide more security characteristics compared to reducing security flaws and improving, especially for WSNs. As a result, comprehensive lightweight user authentication and key agreement scheme

Both security and performance analysis show that this system resists some security vulnerabilities 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 vulnerable to spoofing attacks and offline password guessing attacks. Hence, a plan to overcome these problems was proposed in [56]. This system supports dynamic node addition and easy-to-use password change mechanisms using BANlogic, providing mutual authentication. Security analysis shows that this scheme is secure against known attacks of authentication protocols including middleware and man-in-the-middle attacks. However, another study stated that symmetric key techniques were not sufficient to build message recognition protocols [57]. Moreover, the authors also provided very strong evidence that message recognition protocols (MRPs) cannot be built from 'cheap' primitives using only hash and XORing functions. Hence, a scientist attempted to develop a privacy-preserving two-factor authentication framework exclusively for WSNs to overcome different types of attacks. Although this scheme has its pros and cons, it can withstand popular attacks, and achieve better efficiency at a low computational cost.

4.3.8 Cryptographic solutions and protocols

In fact, cryptographic protocols are used to authenticate the user(s) or device(s) using cryptographic algorithms as a basic component. These components can either be a hashing function (with or without a key), or symmetric and asymmetric encryption algorithms. As a matter of fact, designing effective cryptographic algorithm results in the reduction of the required resources and latency. Furthermore, an effective authentication protocol should decrease the required communication overhead. This is achieved by decreasing the size of the communicated message during the authentication steps. Nonetheless, enhancing the key management techniques and securing the mobile manipulator operation system management layer can assist in reaching a better security level. In this context, symmetric cryptographic protocols are favored since they are known to be more lightweight than asymmetric ciphers, specifically with the Advanced Encryption Standard (AES) being faster than Elliptic-Curve Cryptography (ECC) in [58]. Furthermore, symmetric protocols are more energy-efficient, especially with the use of optimized AES block cipher. On the contrary, stream ciphers can be composed of block ciphers using the Counter (CTR) and Output Feedback (OFB) operation mode [294]. For that, a solution was presented to secure robot operating systems communication channels by adopting cryptographic methods [59]. In fact, this cryptographic method aids in reducing DoS attacks. In addition [60], a Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) in the robot operating system core to secure the robot communication. This solution produces a fine-grained control over permissions to publish, subscribe or consume data. Though, the authors did not secure the ROS master, which can be accomplished via a secure channel or digital certificate [61]. Later, an improvement to the cyber-security level of cloud data. This included the presentation of a new security model with ideal key selection, by clustering secret information with a K-Medoid clustering algorithm formulated on a data distance measure and encrypting the clustered data using Blowfish Encryption (BE) and stored in the cloud [62]. The results of the testing revealed the improved level of accuracy and maximum level of cyber-security that the confidentiality-based cloud storage framework provides. Furthermore, a Cloud-Edge hybrid robotic system to enable dynamic, and flexible feedback control for physical human-robot interactions (pHRIs) [63]. This solution was tested on numerous robots and revealed its robustness in mitigating network latency within the Cloud-Edge perception feedback loop. A new study presents a model that produces mutual authentication and encryption mechanism to access the hosted robotic services, using the Kerberos module and the Elliptic Curve Integrated Encryption Scheme (ECIES) for data encryption [64]. The authors also performed a cryptanalysis examination on their solution using the Proverif tool and revealed the ability of their system to overcome different security threats and attacks. A study compared consensus protocols used in swarm robotics and revealed how they were defeated in the presence of Byzantine (malicious) robots [65]. Therefore, Argos–blockchain interface was introduced to give a secure robot swarm coordination through blockchain-based smart contracts as “meta-controllers”, that as well overcome Sybil attacks. Nonetheless, additional work is needed to ensure its effectiveness against other robotics-related threats ultimately, a three-layer-based study of interconnection architecture with blockchain technology for Industry 4.0, to attain a secure and reliable connection in the midst of entities [66]. Despite its benefits, it does not meet trade-off between operational performance and security, along with the intricacy in data storing.

4.3.9 Intrusion detection systems and firewalls

It is extremely vital to apply various methods of intrusion detection systems (hybrid solution). This helps increasing the level of protection and reaction opposed to known (signature method) and unknown (specification and anomaly detection methods) threats which surround the mobile manipulator. In fact, different propositions were provided for this purpose. This involves a synthesis technique used to construct a distributed IDS to secure a class of multi-agent robots in [67] their IDS includes a decentralized monitoring mechanism and an agreement mechanism. The acquired testing results demonstrate that the method is functional and can detect intrusive behavior with a good error rate (15% error). The success of this sort is reinforced by similar systems, such as the determination of behavior in the use of credit cards using neural networks.

This is accomplished while authorizing the administrators' knowledge to be effortlessly introduced into the system in a method that new important information can be embedded to keep the data updated [68]. Another nonparametric density estimation approach was introduced by utilizing Parzen-window estimators with Gaussian kernels to create an intrusion detection system employing normal data at most. The authors revealed that regardless of its high computational demands throughout the testing phase, it does not demand any training at any rate. Another technique named WebSTAT is an unconventional intrusion detection system that analyses web requests and searches for evidence of malicious behaviors, guaranteeing both flexibility and extensibility, alongside a much more effective web-based attack detection at a minor false positive rate. Experimental results demonstrate that this stateful intrusion detection can be performed on high-performance servers in a real-time manner.

Another is the mIDS, as a general methodology of an anomaly-based IDS that employs the Binary Logistic Regression (BLR) statistical tool to classify local sensor activities and detect the malicious behavior of the sensor node [69]. Assessment results show a detection rate that ranges between 88 and 100% using routing layer attacks. This does not appear to be an optimal solution. Another method is a new network intrusion detection model employing boosted decision trees. The generalized accuracy of the boosted decision tree was compared with various algorithms including Naïve Bayes, and k-nearest neighbor (kNN), and the testing results show that this algorithm surpasses existing algorithms when applied for real-world intrusion.

Another hybrid IDS method was introduced to integrate the merits of anomaly and misuse detection to overcome the overly high false alarm rate of anomaly detection. This hybrid IDS combines k-Means, K-nearest neighbor, and Naïve Bayes for anomaly detection. The main disadvantage of their introduced method is that real-life datasets have a somewhat small variance between normal and anomalous data. In fact, the recently introduced work by different authors reveals an improved protection version for robotic domains.

For instance, an active MANETbased automated convention titled PD-ROBO with an IDS structure to overcome replay assault in mechanical-based Mobile Adhoc Networks (MANETs) [70]. Results showed its efficacy in overcoming directing control overhead and accomplishing the right Quality of Service gratification in robotic communication.

ROS Immunity is introduced as a solution that permits ROS users to harden their systems against attackers with low overhead, with the use of robustness assessment, automatic rule generation, and distributed defense with a firewall [71]. This solution was also examined on a self-driving car, a swarm robotic system, and the outcomes revealed a low nominal overhead with 7–18% extra system power, a low false-positive rate of 8%, and the capability to react and stop attackers from exploiting unknown vulnerabilities in less than 2.4 s this solution has high protection for the mobile manipulator. In addition, a new ensemble system based on the modified adaptive boosting with an area under the curve (MAdaBoost-A) algorithm to more efficiently detect network intrusions [72]. Their mode was compared to already existing conventional techniques, and it demonstrates that it can accomplish a better performance for imbalanced multi-class data both 802.11 wireless intrusion detection and customary enterprise intrusion detection. After discussing the problem of intrusion detection for zero-day deceptive attacks then introduced an intrusion detection system based on an anomalous behavioral pattern detection technique for closed-loop robotic systems to detect zero-day deceptive attacks [73]. Preliminary results show that it surpasses other solutions in detecting zero-day strictly deceptive attacks with high effectiveness.

In closing, the Global Anomaly Threshold to Unsupervised Detection (GATUD) is introduced as an add-on anomaly threshold technique that identifies any abnormal deviation and enhances the performance of the Supervisory Control And Data Acquisition (SCADA) unsupervised anomaly detection approaches [74]. Preliminary results show that it can accomplish a significant enhancement in the unsupervised anomaly detection algorithms.

4.3.10 Honeypots security solutions

Honeypots are very practical tools that complement other security technologies with the aim of forming a firm, and cultivating defensive network security systems . Honeypots can be used as a stand-alone system. In fact, they can also be similarly used in cooperation and collaboration with IDSs and firewalls, exceptionally with their ability to detect, prevent and react. This allows them to be a vastly useful deceptive tool that captures the attacker by sacrificing a given dispensable or unnecessary system to lure the server as a decoy [74]. In fact, if honeypots are used with IDSes, they are able to reduce both false positive and false negative rates. however, they also establish a high level of affectivity and pliability to respond to different types of attacks. Thus, different honeypot systems were introduced in the literature. To solve robotic issues and problems, Irvene et al. presented a “HoneyBot” [75]. This HoneyBot is based on a hybrid interaction honeypot which is designed explicitly for robot systems. Far from other honeypots, HoneyBot can exactly be deceiving intelligent attackers through the dependence on HoneyPhy and techniques from traditional honeypots in the company with device models being employed. This allows the authors to trick the attackers into believing that their exploits were triumphant, while communication was logged to be employed for attribution and risk model creation. Another type of honeypot was introduced by R. Marcus, identified as the Backofficer Friendly (BOF) [76]. This honeypot is a lightweight honeypot that is free for distribution. This method guarantees a precise extraction of the fundamental meaning and most essential aspects of the honeypot's idea and insights. This grants BOF to have a clear perspective of the attack process, with the ability to collect logs and send alerts, in addition to responding with fake replies whenever a user connects to HTTP, FTP, and telnet ports. Another honeypot method was introduced and is called "Specter" was created and sold by a Swiss company called Netsec[77]. This type of honeypots is employed for commercial productions with the objective of detection. Specter is capable of simulating roughly thirteen different OSes (including Windows and Linux), with the ability to offer around fourteen different network services and traps. This provides 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. In developed a game-theoretic model that analyses deceptive attacks and defense 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. This allows the defender to use a mixed defensive strategy that keeps the attacker's successful attack rate low. Furthermore, another honeypot method named "Honeyd"[78] is classified as an open-source thus far powerful honeypot production is employed for detection and reaction against a given attacker. Additionally, it is capable of hiding the guest's OS before the attacker detects it, with the ability to accomplish or overcome 400 OS kinds at a given IP stack level. This reaches hundreds of computers and devices at a single machine use. Hence, this permits the simulated reply to an attacker's request with the capability to alter the reply script to guarantee much more flexibility against the attacker. Ultimately, another approach, called Honeynet, was introduced it can be modified to guarantee better detection and reaction against a given attack, especially with new methods and techniques being employed and used to capture and control data. Thus, it can guarantee a higher flexibility and access control ability.

4.3.11 Artificial intelligence-based solutions

The choice of AI-based solutions was not limited to just performing highly accurate robotic tasks in a timely manner. In fact, current work is now focused on deploying AI in ensuring a highly secure robotic environment, with high accuracy and lower burdens. A presentation of the implementation of the fuzzy logic system, and reinforcement learning to build risk mitigation modules for human-robot collaboration scenarios [79]. Test results showed that the presented risk mitigation strategies improved safety and efficiency by 26% from the default setting. Furthermore, presentation of the main security threats to autonomous mobile bots and how to overcome them. Thus, RoboFuzz has been introduced to automatically perform vector noise sensor values on appropriate occasions, putting the robots at risk. Test results indicate that concrete threats can be imposed on bots with a success rate of 93.3%, with a 4.1% work efficiency loss in mitigation mode. "Bykovsky" introduced Multivalued Logic Minimization (MVL) for the analysis of aggregated objects .To ensure the full use of MVLs, a heterogeneous network architecture was also introduced using three custom levels of AI such as logical modeling of discrete multi-valued logic, boolean logic, and fuzzy logic. This solution is intended to provide additional secret coding, data aggregation, data protection, and communications for network addresses and target control of botnets. Also, the Fog-assisted Secure Anonymous Tracking (SAT) method supports robotic Internet of Things (IoRT) tracking through the Fog Computing Network (FC) system [80]. The SAT test is based on the method of Counting Bloom Filter and (ECC). The results of the analysis and evaluation reveal the effectiveness of the SAT, especially in terms of false-positive rate, memory cost, and query runtime consumption in a safe manner.

After explaining all the possible solution and countermeasures to mitigate, or try to eliminate the risk we will do a table that summarize all the possible solution in addition to the advantages and disadvantages of implementing those solutions:

Approaches		Advantages	Disadvantages
Intrusion Detection Systems IDS	Synthesis technique for distributed IDS	Can detect new attacks, without harming the performance of the mobile manipulator. Categories all new attacks due to its high sensibility in detecting the policy violation.	Malicious monitors by sharing false information that affects the monitor system of the mobile manipulator.
	WebSTAT	Ensures a more effective web-based attack detection at a lower false positive rate, by operating on multiple events streams correlated network and operating system with the entire contained in server logs. It ensure a High performance in real time.	Have a high rate of false negative rates
	Network IDS	The generalized accuracy of the boosted decision tree outperformed the compared algorithms	Unsuitable for malware attacks
	Parzen-window	Adaptive to changes, and does not require training at all. It can easily integrate new training examples into models without the need for any retraining	High computational demands
	Hybrid IDS	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

	Novel anomaly detection	Low-complexity cooperative algorithms can possibly improve both detection and containment processes, nodes can effectively identify an intruder trying to impersonate a legitimate neighbor.	Unable to detect different vulnerability types.
Honeypot	HoneyBot	Accurately deceives intelligent attackers.	Users are limited without physical or visual access to the robotic system.
	Backofficer friendly	Clarify the attack process, collect logs, and send alerts and fake replies to the attacker.	The detection of the attack is limited to seven ports only.
	Specter	Offers 40 different network services traps and simulate 30 different OSs. It actively gathers information about the attackers and fakes a given reply to their request	Limit the detection activity on only 14 TCP ports to IP/Port Snorting
	Honeyd	Creates virtual hosts on a network where it can be configured to run arbitrary services and reports bugs and source code	Never gain access to a complete system despite compromising simulated service.
	Honeynet	Adaptive so it can be modified to ensure a higher detection and reaction against attack with new method to capture and control data	The honeynet can be fingerprinted by the hacker and launch attacks in the outbound limit

Table 2 Summarise The Counter measures that should be taken by a Company adopting a mobile manipulator ar a robot device in general

4.4 Security requirements:

Based on the reviewed work, we found that various security requirements still need to be studied, performed, and analyzed to enhance the discussed security countermeasures and recommendations for future research directions. A very limited number of submitted work involved managing the security aspect of the bots during the design phase of the mobile manipulator, and much focused on how to maintain privacy and confidentiality through encryption without taking into account the source authentication part and data integrity through the use of a strong-key hash. Mechanism (such as HMAC) or using an authentication process mode such as Cryptography-based Message Authentication Code (CMAC) and Galois Message Authentication Code (GMAC) [81]. On the other hand, only a few studies discussed forensic use [82]. Thus, more advanced attention is required to detect the event before a particular automated system can be exploited through a specialized robotic digital forensics investigation. No research has relied on the adoption of an automated self-healing system to overcome any potential power/system failures with systems acting as backup. Hence, many aspects require further studies and a deeper understanding to secure robotic systems in all shapes, aspects, and fields. Thence, in this section, we include the main requirements to ensure the security of the botnet domain. In addition, we provide our recommendations for potential security requirements to improve security.

It is essential to ensure the security of the mobile manipulator's wireless communications by implementing various security mechanisms. This maintains secure communication and ensures confidentiality, integrity, availability, and authentication.

-Adaptive security:

It is essential to implement an active and adaptive security solution to ensure the security of the mobile manipulator. This adaptive solution is divided into two types to know which data to be secured, and from who:

Threat-centred: It mainly evaluates threats to implement the corresponding security measures against them. If we don't have any risk this security shouldn't be considered to avoid additional costs.

Data Centred: It focuses mainly on the data sensitivity that must be evaluated first to secure it, instead of evaluating the threat level.

-Trusted assistants outsource security:

It relies on trusted assistants, it assigns to a specific assistant a specific heavy operation to preserve security and privacy in order to maintain the availability of the systems. This includes relying on Rivest– Shamir–Adleman and Extended Tiny Encryption Algorithm (XTEA) protocols [83], along with the use of Trusted Platform Module forWSNs [84,85]. However, this operation is expensive in terms of cost and maintenance.

-Semi-trusted assistance outsources security:

Based on an entity that performs its assigned task in order to maintain confidentiality by preventing the disclosure of sensitive information. It's subjected to learning more about the essential information that should be secured, whereas nodes rely on unconstrained accessible devices due to the unavailability of hardware equipment. This will allow the storing of the encrypted data in a remote server using Key Ciphertext-Policy Based Encryption (CPABE) [86] and Key Police-Attribute Based Encryption (KP-ABE) [87].

-Online/Offline security:

It transforms the cryptographic schemes into two phases:

i) Offline base: The messages are encrypted before initiating the security service and identifying the destination. It reduces the online cryptographic overhead by producing ciphertexts and storing them.

ii) Online base: It uses the stored data in the offline phase

This approach can be implemented in the mobile manipulator because it doesn't have such a heavy operation related to unknown data.

-Physical layer security (PLS):

It is an emerged paradigm employed to promote wireless network security without relying on encryption techniques. It allows the user to exchange confidential messages over a secured wireless, it is done by utilizing the main properties of the network channel. The PLS method is suitable for the mobile manipulator because it mainly uses the network.

-Low power security:

It provides the necessary basis to build up energy-efficient security services, it reduces energy consumption by accreditation on low power. Various optimized low-power security asymmetric cryptosystems were presented in [88–89] including "Elliptic-Curve Cryptography (ECC)", and the open-source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data (NTRU) operations.

Chapter 5: Conclusion

At the present time, robotic systems are used in the majority of the domains that are based on critical infrastructure. Nevertheless, robotic systems are prone to a variety of vulnerabilities that are mainly due to the lack of security by design of mobile manipulators and the reliance on open wireless communication channels which can be used by an attacker to launch dangerous attacks, which may have critical consequences on the infrastructures which in turn can vary from economical losses to loss of competition if the hack was done by a competitor, to maybe the loss of human lives caused by the malfunction of the robot. In this thesis, we have described a security architecture for mobile manipulators for industrial use in order to understand the effect of the industry adopting a mobile manipulator. We showed that threats can result in total loss of the Confidentiality, Intent, availability, and authentication of the mobile manipulator. Many studies show that a number of research robots are accessible and controllable from the Internet, demonstrating a risk to users' safety and privacy. Therefore, it is very important to protect robots from any possible attack and by all means necessary by developing a mechanism for using the mobile manipulator while securing it from malicious actors by detecting and preventing attackers from breaking these systems to inject malicious malware or/and data to cause either chaos and havoc in the mobile manipulators' operation, or to leak sensitive information from the industry, especially it has a camera and a laser scanner. For that purpose, we start by defining what is a mobile manipulator, sectors where it can be used, and possible threat sources and types of attack, in addition to an impact-oriented analysis approach to assess the risk of these attacks as was shown qualitatively in the physical impacts for losing the availability of the robot while performing critical applications, and quantitatively to mitigate the higher risks or avoid them with the help of Failure Mode & effect analysis and threat risk assessment. As well we widely explain the solution and countermeasures that can be adopted by the company to avoid/mitigate the risks, which make the use of mobile manipulators have more advantages than disadvantages that occur if the hack was done.
So it is mandatory for the companies that implement a mobile manipulator to ensure secure wireless communication with minimal overhead in terms of delay and required resources by , lightweight cryptographic algorithms and protocols at the network and/or at the physical layer. In addition, it should use a privacy-preserving technique to ensure the privacy of legal entities. Finally, non-cryptographic solutions should be designed to protect the application of the mobile manipulator such as lightweight intrusion detection or prevention systems.

REF:

1. E. W. Dijkstra, “A note on two problems in connexion with graphs,”

Numerische mathematik, vol. 1, no. 1, pp. 269–271, 1959.

2. D. Fox, W. Burgard, and S. Thrun, “The dynamic window approach to

collision avoidance,” IEEE Robotics & Automation Magazine, vol. 4,

no. 1, pp. 23–33, 1997.

3. W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu,

and A. C. Berg, “SSD: single shot multibox detector,” in European

Conference on Computer Vision. Springer, 2016, pp. 21–37.

4. Design and Implementation of Mobile Manipulator System

Yugen You, Zhun Fan_, Wenzhao Chen, Guijie Zhu, Benzhang Qiu, Jiaming Xin,

Jingming Chen, Furong Deng, Youzhao Hou, Weixiang Liang and Runzhan Fu

5. G. Salton and M. J. McGill, “Introduction to modern information

retrieval,” 1986.

6. 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)

7. 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)

8. 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)

9. Rubio, J.E., Alcaraz, C., Roman, R., Lopez, J.: Current cyberdefense trends in industrial control systems. Comput. Secur. 87, 101561 (2019)

10. Falliere, N., Murchu, L.O., Chien, E.: W32. stuxnet dossier. White paper, Symantec Corp., Security Response 5(6), 29 (2011)

11 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)

12 Goyal, R., Sharma, S., Bevinakoppa, S., Watters, P.: Obfuscation of stuxnet and flame malware. Latest Trends Appl. Inform. Comput. 150, 154 (2012)

13. 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)

14. Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson, Upper Saddle River (2017).

15 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)

16. 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)

17. Rubio, J.E., Alcaraz, C., Roman, R., Lopez, J.: Current cyberdefense trends in industrial control systems. Comput. Secur. 87, 101561 (2019).

18. Senie, D., Ferguson, P.: Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. Network (1998)

19.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)

20. 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 IEEEWorld Congress on Services (SERVICES), vol. 2642, pp. 3–8. IEEE (2019)

21. 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)

22. 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)

23. 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)

24. 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)

25. 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)

26. Pham, V., Seo, E., Chung, T.-M.: Lightweight convolutional neural network based intrusion detection system. J. Commun. 15(11) (2020)

27. He, H., Gray, J., Cangelosi, A., Meng, Q., McGinnity, T.M., Mehnen, J.: The challenges and opportunities of artificial intel

28. 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)

29. Falliere, N., Murchu, L.O., Chien, E.: W32. stuxnet dossier. White paper, Symantec Corp., Security Response 5(6), 29 (2011)

30. 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)

31. Waksman, A., Sethumadhavan, S.: Tamper evident microprocessors. In: 2010 IEEE Symposium on Security and Privacy (SP), pp.

173–188. IEEE (2010)

32. Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P., Sunar, B.:Trojan detection using icfingerprinting. In: IEEE Symposium on Security and Privacy, 2007. SP'07, pp. 296–310. IEEE (2007)

33. 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)

34. 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)

35. 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)

36. 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)

37. Joint Task Force Transformation Initiative et al.: Guide for conducting risk assessments. Special Publication (NIST SP)-800-30 Rev 1 (2012)

38. 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)

39. 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)

40. 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)

41. 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)

42. 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)

43. 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)

44. 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)

45. 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. P

46. 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)

47. 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)

48. He, D., Gao, Y., Chan, S., Chen, C., Jiajun, B.: An enhanced twofactor user authentication scheme in wireless sensor networks. Ad Hoc Sens. Wirel. Netw. 10(4), 361–371 (2010)

49. 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)

50. Chen, T.-H., Shih, W.-K.: A robust mutual authentication protocol for wireless sensor networks. ETRI J. 32(5), 704–712 (2010)

51. 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)

52. Li, C.-T., Weng, C.-Y., Lee, C.-C.: An advanced temporal credential-based security scheme with mutual authentication and key agreement

53. 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)

54. 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)

55. 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)

56. 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)

57. 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)

58. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.: A

survey of lightweight-cryptography implementations. IEEE Des.

Test Comput. 6, 522–533 (2007)

59. 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)

60. Hussein, A., Elhajj, I.H., Chehab, A., Kayssi, A.: Securing

diameter: comparing tls, dtls, and ipsec. In: 2016 IEEE International Multidisciplinary Conferenc

61. 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)

62. Hussaini, S.: Cyber security in cloud using blowfish encryption. Int. J. Inf. Technol. (IJIT), 6(5) (2020)

63. Tian, N.: Cloud-edge hybrid robotic systems for physical human robot interactions. Ph.D. thesis, UC Berkeley (2020)

64. 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)

65. 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)

66. Alcaraz, C., Rubio, J.E., Lopez, J.: Blockchain-assisted access for federated smart grid domains: coupling and features. J. Parallel Distrib. Comput. (2020)

67. 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)

68. 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)

69. 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)

70. 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)

71. Rivera, S., Iannillo, A.K., et al.: Ros-immunity: integrated approach for the security of ros-enabled robotic systems (2020)

72. Zhou, Y., Mazzuchi, T.A., Sarkani, S.: M-adaboost-a based ensemble system for network intrusion detection. Expert Syst. Appl. 162 (2020)

73. 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)

74. 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)

75. Irvene, C., Formby, D., Litchfield, S., Beyah, R.: Honeybot: a honeypot for robotic systems. Proc. IEEE 106(1), 61–70 (2018)

76. Ranum, M.: Backofficer friendly (bof)

77. Spitzner, L.: Specter: a commercial honeypot solution for windows. Acesso em 26(08) (2003)

78. Provos, N.: Honeyd-a virtual honeypot daemon. In: 10th DFNCERT Workshop, Hamburg, Germany, vol. 2, p. 4 (2003)

79. 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)

80. Alamer, A.: A secure anonymous tracing fog-assisted method for the internet of robotic things. Library Hi Tech (2020)

81. 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)

82. 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)

83. Needham, R.M., Wheeler, D.J.: Tea extensions. Report (Cambridge University, Cambridge, UK, 1997) Google Scholar (1997)

84. 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)

85. 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)

86. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attributebased encryption. In: IEEE Symposium on Security and Privacy, 2007. SP'07, pp. 321–334. IEEE (2007)

87. 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)

88. 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)

89. Koblitz, N.: Elliptic curve cryptosystems.Math. Comput. 48(177), 203–209 (1987)