Ashutosh Kumar, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Attacks & Preventing Measure On Cloud Robotics System, A Review with Cloud Heritage Techniques

Ashutosh Kumar, Gaurav Singh Panwar, Gori Sharma,
Jivesh Tiwari, Assistant Professor Dr. Rajkumar
Department of Computer Science and Engineering (AIML)
Quantum University, Roorkee, India

Abstract- This study investigates the vulnerability landscape of cloud robotics systems, identifying potential attack vectors that threaten the integrity, availability, and confidentially of robotic operations in a cloud environment. we delve into threats such as data branches, unauthorized access, intruders, and service disruptions within the cloud robotics paradigm. The research proposes a set of preventive measures to fortify this security technique, including the implementation of secure communication protocols, robust access controls, and an intrusion detection system. In this paper, we conduct a comprehensive study of security issues in the real-time cloud robotics environment. By analyzing different attack vectors in cloud robotics networks, we find attacks that manipulate the network resources, microarchitecture resources, and function parameters respectively.

Keywords— Cloud Robotics, Security & Attack, Threats

I. INTRODUCTION

The advance cloud robotics system has promoted the rapid development of traditional robotics system. A variety of robots and autonomous systems are introduced to alter our lifestyle in a revolutionary manner. In some complex scenarios, one single robot is not enough to complete the tasks within the demanded deadline. Thus, a couple of robots can be connected as a MRS to work on the tasks together. These robots can be the same type or different types with different functionalities. This collaboration can effectively reduce the task completion time. A MRS usually requires a centralized service to coordinate the involved robots. This service collects information from all the robots to make decisions, and sends to each robot the instructions for the next round. Although cloud computing brings great convenience to the robot systems, it can also open new attack cyber space for advere saries to affect the entire MRS. In this paper, we present a systematic study towards the above security threats and security functionality of robotic network. First, we build an analytic model to disclose the performance characteristics of multi-robot systems and remote location workloads. Based on this work, we identify a critical execution path and a series of function robotics device that can determine the performance of the entire cloud robotics system. Then we identify a couple of attack strategies that can affect the execution of the target workloads.[9,10,11]

Cloud Heritage Techniques- The cloud heritage technique is that technique where we inherent with base cloud and child cloud. When attackers attack any cloud network, they can't find the exact location of the cloud network.

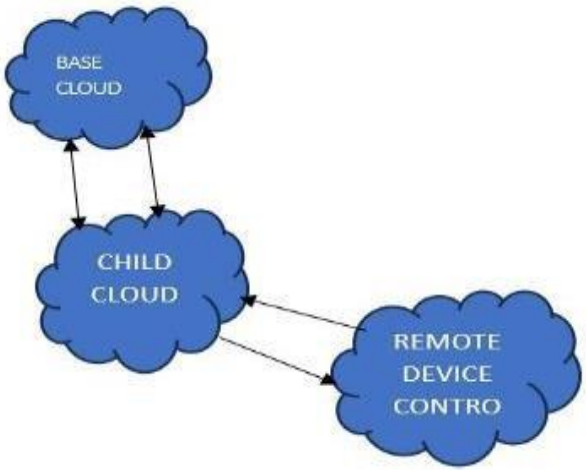

Fig 1. Cloud Heritage System

II. SYSTEM ARCHITECTURE OF CLOUD ROBOTICS

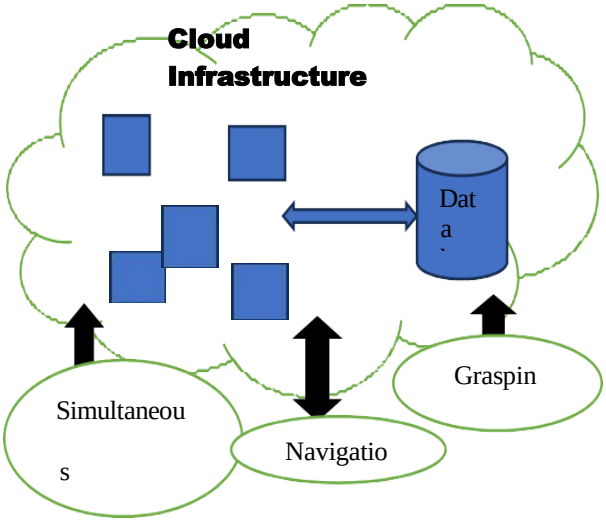

Fig 2. Architecture of Cloud Robotics

The architecture of cloud robotics is mainly composed of two parts: the cloud platform and its related equipment and the bottom facility. The bottom facilities usually include all types of mobile robots, unmanned aerial vehicles, machinery and other equipment.[1,11]

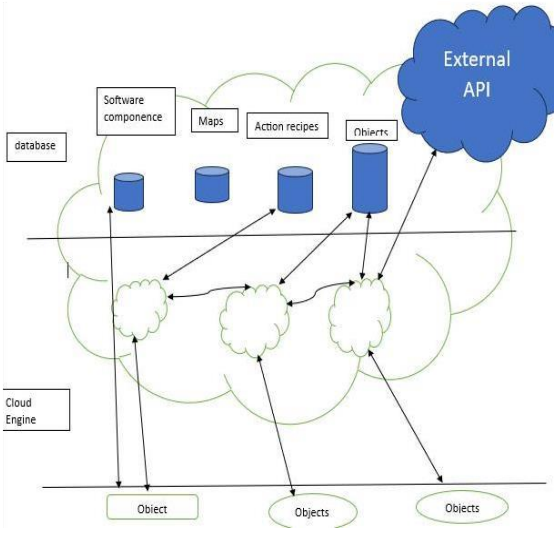

Fig 3. Implementation of cloud robotics in industrial environment

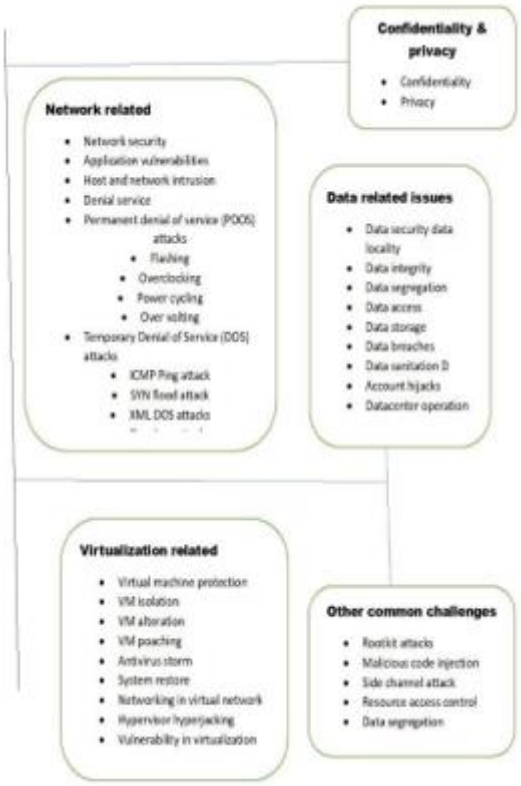

Fig4. Key issues& security problem

Background & threat model Robot platform

In this section, we describe the structure of robot apps and development cycles. We use the Robot Operating System (ROS). ROS platform, it is an open-source middleware framework designed for robotics. They are responsible for hardware abstraction, message passing and also provide device drivers for various sensors and motors. to support different types of functions, e.g., localization, path planning, path tracking, etc. the lifecycle of robot app development and operation. First, the developer decomposes the design of the target app into some functions.. Then the developer start installing the ROS core libraries to integrate these functions as an app workflow and deploys the app to the robot. . They exchange messages through the ROS Topics, which are many-to-many named buses that store the robot or environment states. The communication follows the publish-subscribe messaging protocol: nodes can subscribe to a topic to obtain relevant data, or publish data to a topic.[2,3]

Robot Workloads

A robot workload can be abstracted as navigating the robot to a given destination based on the cloud environmental information captured from sensors. So different workloads always follow a standard type of pipeline. The computation pipeline is composed of three major processing stages: perception, planning, and control. Each node represents a type of functional computation. The solid arrows denote that the connected two networks communicate in the publisher mode, and the arrows represent a client/server paradigm.

Perception: This stage perceives data from the sensors, and processes them to extract estimated states of the environment and the robot. It consists of two computation cloud robotics devices. the workload associated with perception includes processing sensor data, performing compute vision tasks, and extracting meaningful information that the robot can use for decision-making.

Planning: This stage is responsible for describe the long-range actions of the robot based on high-level goals by users. Planning refers to the process of generating a sequence of actions.in cloud robotics system planning may involve offloading computationally intensive planning tasks to cloud servers.

Control: Control: Control involves the execution of the planned actions to manipulate the robot's actuators and achieve the desired movements or behavior. The workload for control includes real-time processing to adjust the robot's actuators.[7,8]

III. THREAT MODEL AND ASSUMPTIONS

We consider a cloud-based MRS system, which involves multiple robots, and each robot runs many function nodes. They collaborate to complete a given workload (e.g., exploration, navigation). We assume the underlying OS and ROS core libraries in each robot are trusted: the communication and isolation mechanisms are correctly enforced. How to protect the network security of the ROS core libraries attack wireless networks, steal private data, and defeat the threats. Some functions cloud network are executed on the remote cloud server and the executed results are transmitted back to the cloud robotics device. We assume that all offloaded cloud networks execute in the same VM. This is reasonable since the communication latency among these cloud networks can be minimized. We assume the cloud computation and its communication with the cloud robots are also well protected by cryptography. However, we assume that only one cloud network in one robot is untrusted. It aims to perform attacks against the cloud resources, which can further affect the whole MRS workload.

Threat Model: ‘‘Third-party components releasing process create additional security threats (third-party component may be compromised during their distribution)”. Second, a lot of public functions in the cloud robotic system contain software bugs. According to the Robot Vulnerability Database, up to the date of writing,

17 robot vulnerabilities and 834 bugs (e.g., no authentication, uninitialized variables, buffer overflow) have been discovered in the repos of 51 robot components, 37 robots, and 34 vendors in the ROS platform. Most of them are still not addressed yet. An adversary can easily exploit those bugs to compromise the function node. Our goal is to identify the possible consequences a malicious node can bring to the entire MRS.[4]

Possible attack strategies

From the above analysis, to compromise the performance of a cloud network-based MRS workload, the system can try to delay the execution time of VDP. We identify several possible attack strategies to achieve this goal.

Cloud Robotics Network Contention

To ensure the performance of the MRS under the cloud roboticsnetworkenvironment,
communication between the cloud server and local robots. Using UDP protocol. As a result, the adversarial cloud network can flood the network bandwidth and resources with useless UDP messages. This can also affect the latency, causing safety issues when the robot works at a fast speed. [9]Micro-architecture Contention: If the adversarial

cloud network is co-located with the critical cloud networks on the same cloud server, it can generate malicious contention on the micro-architectural units to deprive the resource usage of the critical cloud network and increase their computation time. This is feasible if they share the hardware resources, even they are in different VMs. [9,10]Direct Delay: If the adversary is able to directly affect the execution of the computation cloud network along VDP via the user interface, we can potentially increase the processing time of the cloud robotics system. Then this strategy can decrease the maximum velocity, and increase the local task and global workload completion time.[9,11]

Types of attack: the table shows the types of attack, it is clear that this type of attack is the most common in robotics because of their server impact of robots and their resources. Another reason for this is theat DoS attacks are easy to execute. They can even be performed through the use of publicly available tools, which allow attackers to create malicious code, such as bots.[5,6]

Table-1 Types of attack

Robot	Types	Reference	Attack								Level		
Cone-O-Bot	Medical	[5]	DOS	MitM	Tampering	Theft	Total	Taxes			HW	Network	FW
PeopleBot	Mobile	[6]	1				1	1					1
ARB IRB 140	Industrial	[7]	1	1									1
PeopleBot	Mobile	[8]	1	1	1						1	1	1
											1		
Erector Spykee	Toys	[17]	1										1
Raven II	Surgical	[18]	1	1							1	1	1
											1	1	
Kuka Box	Collaborative	[23]	1									1	1
ARB IRB 140	Industrial	[24]				1						1	1
Amigo-Bot	Mobile	[28]	1				1				1	1	1
AscTec Hummingbird,iRobot create	Drone/Autonomous,Mobile	[29]						1				1	1
Raven II	Surgical	[57]	1	1								1	
			1										
Jacobos Robot	Mobile	[58]	1									1	
Parrot AR Drone 2.0	Drone/Autonomous	[62]										1	
Raven II	Surgical	[65]	1					1				1	1
CHIMERA	Mobile	[65]										1	1
NPS ARSENL	Drone/Autonomous	[80]		1								1	1

IV. CONCLUSION

This paper described the origin and development of cloud robotics, from the allocation of resources and communication mode perspectives and analyzed cloud robotics communication architecture. We identify estimated and prioritized the risks associated with attacks targeting the availability of the robotics system. We perform comprehensive evaluation and case studies to show the attacks and cause server safety and performance issues. This paper aims to bring together the most relevant studies and to identify the most common risks , threats and vulnerabilities[1,2,3,4,5,6,7,8,9,10,11]

REFERENCES

1. Robotics technology market, https://www.alliedmarketresearch.com/robotics-technology-market (2020).
2. Ros pr2 package, http://wiki.ros.org/Robots/PR2/ (2020).
3. Open source robot operating system, http://www.ros.org/ (2019).
4. Robot vulnerability database (rvd), https://github.com/aliasrobotics/RVD/ (2020).
5. "Cloud Computing Security with Identity-Based Authentication Using Heritage-Based
6. Technique", IJAERS, International, 2017.
7. Siciliano, Bruno, O. Khatib, Springer handbook of robotics, Springer, Secaucus, NJ, USA: Sprinter-Verlag New York Inc, 2016.
8. C. Goldfeder and P. K. Allen, ``Data-driven grasping,'' Auto. Robots, vol. 31, no. 1, pp. 1_20, Apr. 2011.
9. M. Chen, Y. Zhang, Y. Li, M. M.Hassan, and A. Alamri, ``AIWAC: Affective interaction through wearable computing and cloud technology,'' IEEE Wireless Commun., vol. 22, no. 1, pp. 20_27, Feb. 2015.
10. Robotics technology market, https://www.alliedmarketresearch.com/robotics-technology-market (2020).
11. Ros pr2 package, http://wiki.ros.org/Robots/PR2/ (2020).
12. Open source robot http://www.ros.org/ (2019).
13. Robot vulnerability operating database system, (rvd), https://github.com/aliasrobotics/RVD/(2020).
14. "Cloud Computing Security with Identity-Based Authentication Using Heritage-Based Technique", IJAERS, International, 2017.
15. Siciliano, Bruno, O. Khatib, Springer handbook of robotics. Springer, Secaucus, NJ, USA: Sprinter-Verlag New York Inc. 2016.
16. C. Goldfeder and P. K. Allen, Data-driven grasping," Auto. Robots, vol. 31, no. 1, pp. 1_20, Apr. 2011.

17. M. Chen, Y. Zhang, Y. Li, M. M.Hassan, and A. Alamri, AIWAC: Affective interaction through wearable computing and cloud technology," IEEE Wireless Commun., vol. 22, no. 1, pp. 20_27, Feb. 2015.
18. G. Hu, W. P. Tay, and Y. Wen, "Cloud robotics: architecture, challenges and applications," IEEE Network, vol. 26, no. 3, pp. 21-28, 2012.
19. B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, "A survey of research on cloud robotics and automation," IEEE Transactions on Automation Science and Engineering, vol. 12, no. 2, pp. 398-409, 2015.
20. L. Turnbull and B. Samanta, "Cloud robotics: A review of technologies, developments and applications," Robotics and Computer-Integrated Manufacturing, vol. 64, p. 101938, 2020.