# Cloud Robotics Security Threats: Attacks on Cloud Network

**[1]Umesh Kumar, [2]Dr. Ramesh Vishwakarma, [3]Dr. Rishi Kumar Sharma**

*[1]PhD Scholar of Computer Science Rabindranath Tagore University, Bhopal, India*
*email umeshkumar.tech@gmail.com*
*[2]Dept. Computer science Rabindranath Tagore University, Bhopal, India*
*email rameshaisect@gmail.com*
*[3]Dept. FCE Poornima University, Jaipur,India*
*email rishi.rishi1526@gmail.com*

## Abstract

*This research paper presents the security risk of cloud robotics analysis, methods and ways of their protection, prospects of using duel authentication system to decentralization of decision-making systems and information protection. A detailed analysis and research of attacks on cloud robotics system components was carried out and protection recommendations were developed.*

***Index Terms—Cloud robotics, Edge of computing, Attack, Protection.***

## I INTRODUCTION

In the last few years, the cloud robotics systems have been widely developed and implemented. The cloud robotics market research notes a steady and rapid increase in the number of such devices every year. Analysts currently estimate the number of active robotics devices at 21 billion and in a few years their number will exceed to 50 billion. Due to the development and widespread introduction of cloud robotics technologies, information security experts are concerned about their level of protection. According to them, the huge number of poorly protected cloud devices gives new opportunities to cyber criminals. Yes, there are already known cases of breakage of several cloud robotics systems. This task is especially relevant when using these tools at critical infrastructure.

New technologies and new tools are creating new types of cyber threats. Many companies today have introduced their protection models, which are constantly trying to standardize, correlate and implement it.

The development of cloud technology makes its adjustments in the field of information security. Therefore, the advent and edge of computing technologies allow solving several cybersecurity problems. The main trend of edge computing is remote monitoring and data processing directly on cloud robotics devices. The main advantage of this approach is the minimization of processing time and decision-making due to the absence of the need to transfer all data to a data center (data center) or cloud. The combination of cloud robotics and edge computing is a promising area and can be used in industry, hospitals, climate control systems, and “smart” buildings, in the management of the infrastructure of the city or region, in trade and logistics networks. Of particular interest is the use of edge computing for network security monitoring and access control systems. This technology is quite effective in preventing certain types of at- tacks and the spread of malicious software. Also, performing calculations immediately after receiving a signal allows you to decide whether to generate an alarm, move the “object” to quarantine, isolate, if necessary, several cloud robotics devices to prevent network compromise or system failure. The widespread introduction of cloud robotics devices creates large amounts of information that are increasingly difficult to transfer to a data center or cloud, process and store them, so the use of edge computing is a necessity for many areas of the digital society. The study of traffic minimization technologies, data storage, resources, and security in cloud robotics using edge computing is a crucial task today for the development of digital society and the entry of humanity into the fourth industrial revolution.

## II EDGE COMPUTING

As the number of devices increased exponentially, the load on both the data channels and the storage cloud (trillions of gigabytes) increased, so the use of edge computing became a necessity, not a whim. We note that the use of edge computing and cloud technologies together is possible, and in some cases necessary, especially in industry. Edge computing is the most important component for cloud robotics, which helps reduce latency and increase the reliability of deployed systems. In the models of cloud architecture are presented, the need for cloud robotics protection is determined, the results of research on the construction of information protection systems for cloud robotics devices, including shared and centralized, conducted simulation load depending on the number of devices.

Security issues are quite relevant and aimed at the comprehensive protection of information and robotics device protection. Thus, focuses on the complexity of cloud robotics protection and presents eight key security technologies: network security, authentication, encryption, security attack, security analytics, and threat forecasting, interface protection, delivery protection.

mechanisms. Prospects for implementation and threats facing cloud robotics systems are presented. The analysis of these works confirm the relevance of security issues, areas of protection, and the main conceptual approaches to device security. Large cyber-attacks have occurred more than once and the number of hacker attacks is growing. The urgency of the problem is underscored by incidents, the loss of capital which is measured in billions of dollars.

## III VULNERABILITIES

In total, Cloud experts have identified about 25 different vulnerabilities in each of the studied devices and their mobile and cloud components. The conclusion by Cloud experts is disappointing: a secure cloud robotics system does not exist today. The particular danger to the Cloud robotics system is hidden in the context of the spread of targeted attacks. It is only necessary for intruders to show interest in anyone, and our helpers from the world of robotics turn into traitors, openly open access to the world of their owners.

Because the issue is extremely acute, companies that develop equipment, communications, network devices, software, and cybersecurity companies are looking for means to protect robotics devices. One of the leading companies in the development of security in the network is Cisco Systems, which played a leading role in the development of the cloud robotics model at the World cloud robotics Forum, developed the cloud robotics security framework, which became a useful addition to the reference model.

Portable devices account for the largest number of attacks, and the use of wireless communication technologies between system elements creates the preconditions for a cyber-attack on the system. Unauthorized access is most often carried out by hackers through entry points (access) to the cloud network or used to launch a DDoS attack. Given the large number of sensors connected to the system, the use of wireless net- works, cloud services, etc. does not provide a reliable perimeter of cybersecurity of the object. Another area is the theft of confidential user data (companies). The powerful potential of cyber threats has the technology of machine learning and the use of artificial intelligence systems through dual purpose (the algorithms used can both counteract cyber- attacks and create them). New technologies (Cloud Robotics) create new cyber threats, which can be resisted only with the use of new information technologies.

Leading companies and specialists implement multi-level comprehensive protection systems based on the use of the latest technical tools, qualified personnel, control procedures, administrative regulations with strict compliance with them. In such systems, the emphasis is on setting up early warning systems that monitor the operation of IT equipment in real- time, notify administrators in the event of any abnormal activity, allow timely detection of attacks, as well as analyze potential threats. The criteria for the stability of such a defense system are the ability to respond to attacks in a timely and adequate manner and to restore the operation of the object with minimal losses.

Results of our research system is a cloud robotics system, the hardware of which can be divided into the following elements

:communication subsystem (wireless communication in the sensor network, includes a radio receiver with cloud network),

1. computing subsystem (data processing, node functionality),
2. sensor subsystem (network connection with the "outside world"),
3. power subsystem.

Tasks facing the system to the hardware:

- low electricity consumption,
- the ability to work with a large number of nodes at relatively short distances,
- relatively low cost

## IV CLOUD ROBOTICS ARCHITECTURE

- work autonomously and without maintenance,
- have a camouflage effect,
- be resistant to the environment.

Given the fact that sensor networks are vulnerable to many attacks, the issue of cybersecurity is especially relevant in the implementation of cloud robotics systems to protect the perimeter of the regime object. We assume that it is necessary to carry out temporary protection of the perimeter during the transportation of cargo/person/reconnaissance operation. This scheme contains a set of devices used to create a zone of the temporary perimeter security system. Also performed modeling of a typical fire alarm system of a separate room on the example of a garage. The set of devices is typical.

Modeling of systems allowed to determine that the main areas that need attention from cybersecurity are:

communication security, protection of the devices themselves, control over the operation of devices, control of network interaction.

## V ATTACKS

DoS attack on the physical level. A DoS attack is characterized by an attempt by an enemy to stop a network or destroy a network security service. In a Cloud Robotics system, a DoS attack can occur at different levels of the protocol stack, can affect several levels simultaneously, and use the interaction between them. DoS attack at the physical level can be carried out by interfering with the radio frequencies on which the system operates. In such an attack, one attacking robotics device may disconnect all or part of the network (for example, blocking data transmission). An attack on the Cloud Robotics system's detection of a sensor (in our case, a sensor/camera around the perimeter of a security object) and an attempt to physically access it is critical to our system.

In this case, an attacker can destroy the device, try to replace the data, access sensitive information (including cryptographic keys), use the device to log on to the network. DoS channel level attack. DoS collision attack at the channel level is usually aimed at depleting the resources of Cloud robotics device. This attack affects the packet transmission process, causing exponential delay and packet retransmission procedures in some MAC protocols. Thus, when a large number of bits are damaged in a packet, the robotics-device will try to use error correction robotics-device to recover the damaged bits, thus wasting limited energy resources. Another example of such an attack is a "collision" at the end of the frame, which leads to the retransmission of the entire packet.

Another embodiment of the attacks inherent in the IEEE

802.11 protocols may be the generation of an RTS message to a base station or neighboring node, which will lead to the processing of this message and generate a CTS message, followed by waiting for signal reception, and all other robotics device stop transmitting data to receiving robotics device for the time specified in the RTS message. Handshake methods can also be implemented. Let us analyze attacks on routing protocols. The known Black Hole attack aims to use a routing protocol to redirect packets from or to the target node through a specific node. This attack can be used to drop packets or a "middle man" (a method of compromising a communication channel in which an attacker, by joining a channel between counterparties, interferes with the transmission protocol by deleting or modifying information).

Another type of attack is a selective forwarding attack, which is similar to a Black Hole attack, but in this attack will be rejected packets that meet certain criteria, not all. When implementing the "Rapid Pressure" attack, the procedure of opening the route at the request of routing protocols is used. The malicious node generates and transmits a route request to its neighbors, and as a result, the node is more likely to be part of the selected route between the source and destination. The "Funnel" attack is characterized by the fact that the attacker tries to either compromise the node, or place its own in the path of as many networks flows as possible, and the latter then begins to act on the type of funnel – collecting all the traffic of the sensor network. In protocols that use broadcast, the attacker, listening to the channel, informs neighbors that he "knows" the shortest route to the base station. Once it has managed to stand between the transmitting sensor node and the base station, it can perform any action with the data packets coming to it. Sybil attack is characterized by the fact that the attacker tries to compromise the existing node, or connect your own with several pseudo-identifiers and thus pretending to be several nodes at once. Thus, neighboring nodes may perceive it as "their own". Such attacks are used to disrupt the mechanism of distributed storage, routing mechanisms, data aggregation mechanisms, voting mechanisms in the network.

A wormhole attack poses a serious threat to the security of sensor networks because it does not require compromising the sensor node. For example, an attacker listens to a channel, receives a broadcast to request a route from the base station, and forwards it to the nearest neighbor. The robotic device that received this message will consider it the parent, that is, the one closest to it, although this is not the case. The attack is based on creating a special path between two or more network nodes to transmit intercepted packets, and the nodes will think that they transmit packets by the shortest path.

One type of attack is a flood attack (HELLO flood attack). The peculiarity of this attack is the attempt to transmit to the network many optional messages that will deprive the network of various resources (computing power, channel capacity, energy resources). Having a high frequency radio transmitter with sufficient computing power, the attacker sends Hello packets of many cloud robotics devices of the sensor network. Upon receipt of this message, the robotics devices perceive the compromised robotics device as a neighbor and include the received address of the sender in the mailing list. In this way, the attacker gains access to data sent from the mobile devices (Cloud robotics devices).

Transport layer functions include the delivery of packets (TCP) and datagrams (UDP) from sender to recipient. Attacks at the transport level are aimed at analyzing the regularity of traffic and sending parallel duplicates of messages in other ways used at this level. Given the fact that most transport protocols support sensitive information and are therefore vulnerable to memory depletion, an avalanche attack attacker makes new connection requests each time increasing the amount of confidential information in the attacking node, gradually leading to the robotics devices becomes faulty (failure of the node from further connections) due to resource depletion) and uses this shortcoming.

Another typical attack of this level is the desynchronization attack, because of which an attacker tries to break the connection between two working robotics device in the network, repeatedly forging messages to them. In particular, transport layer protocols can use sequence numbers to track successfully received packets, identify packet loss, and detect copies. Attacker-generated packets can use these sequence numbers to reassure the node that packets have been lost and to provoke retransmission, which can have the effect of depleting the resource and filling the data channel when valid information does not arrive at the database or arrives with a delay.

Attacks on data aggregation are aimed at changing the behavior of the network. Data aggregation and merging procedures are used in networks where the location of typical sensors is close to each other. Such procedures are used to combine multiple data to eliminate redundant information. To save resources, this is positive, but it is dangerous from the point of view of cybersecurity. Thus, the calculation of simple mathematical functions (minimum, maximum, average, sum) used in aggregation in the presence of a single malicious node or the replacement of real data from sensors can change the behavior of the network in part or completely. Privacy attacks are aimed at capturing information collected by sensors and can be implemented by listening to the network, analyzing traffic, and/or capturing the robotics device. This is especially true for those networks that do not use data encryption.

Recommendations for counteracting attacks on components of the cloud robotics system Resist DoS attacks at the physical level. IEEE 802.11 (Broadband) standards use frequency hopping. In this case, the interference transmitter must “know” the sequence of hopping or create interference with a larger frequency band. It is proposed to use spectrum expansion technology to protect against such attacks. The transmission of such a signal will be similar to noise, which will reduce the risk of intentional interference with the information signal. Besides, when the signal disappears from any part of the network or cloud robotics device, network element, DSS should generate an alarm on the unit. Robotics devices that have detected an interference attack must send a short message to their “neighbors” and the base station about the attack on the network. In this case, if the message “does not reach” the base station from the attacked robotics device, it is likely to receive an alarm message from the robotics device that was not attacked.

To counteract cloud robotics intrusion attacks, each sensor used in the system must be equipped with a tamper (a miniature button on the board of the device that is squeezed when opening the case or disconnecting it from the mounting location). When the tamper is triggered, the hub sends push- messages and SMS to all users of the security system (if there are such messages in the devices to be used), as well as the transmission of the message to the base station. Besides, it is desirable to provide software that when the tamper is triggered during “arming”, all data stored on the device was destroyed automatically. To avoid detecting sensors, they should be placed in hidden places, but suitable for their installation, use materials that are resistant to external influences. Sensors and cameras have their range, so when placing such devices should take into account this figure and install them with an overlap to avoid insensitivity. If installed correctly, the sensor will detect the danger and send an alarm to the base station until the attacker approaches it.

The proposed system uses an RFID tag to identify a person. The decision support system provides a situation where the RFID tag and motion sensor is activated, but we do not receive a signal from the camcorder. This situation may indicate that the tag was “removed” or “replaced “and the motion sensor detected movement, but attackers could disable the camera to avoid being identified as violators. This set of parameters will generate an alarm on the unit. To counter a DoS attack at the channel layer, there is authentication to verify that the robotics device generating the message is authorized on the network in combination with encryption. In our case, we use the WPA2-PSK authentication standard with an AES encryption type. Given the energy limit, the use of asymmetric encryption becomes impossible in such systems. The main disadvantage of using symmetric encryption is the problem of key distribution. When using a symmetric cryptographic scheme, it is necessary to ensure the reliable and secure installation of shared cryptographic keys between two robotics devices before they can exchange data. Key installation and management techniques should be suitable for use with hundreds and thousands of robotics device. Another way to improve security is to install an RFID tag on all devices on the network and conduct a combined (two-factor) cloud robotics device authentication procedure. It is proposed to use block chain technology to protect against interference with the program code and substitution of sensors. This technology is a distributed database that is potentially available to everyone. Thanks to the use of block chain technology, it is possible to counteract fraud, manage identification, transactions, verify the status of elements of various systems, and ensure data integrity. Combining block chain and Internet of Things technologies can solve several security issues, namely: tracking sensor data measurements and preventing duplication of any other malicious data; authentication and secure data transmission. Cryptography is proposed to protect against eavesdropping, injection, and packet modification.

To counter aggregation attacks, it is proposed to use aggregation delay and authentication methods. To prevent routing attacks, we use channel-level encryption and authentication using a global public key. Sybil attacks can be prevented by verifying the identity of the sensor nodes (using a shared symmetric key from a trusted base station) and limiting the number of neighbors that the node may have. In this way, the compromised node will only be able to contact trusted neighbors. You can counter a funnel attack using a geo-routing protocol, in which traffic “naturally” directed to the physical location of the base station is difficult to redirect to create a funnel.

The proposed system uses static sensors that require duel time authentication in the network. Edge computing in information security systems can be used to counter several considered attacks and is the subject of further research. The use of clusters of security systems, cloud robotics clusters in combination with edge computing creates new approaches to technologies for building secure cloud robotics with decentralized data processing. The list of attacks is an open classification group that can be supplemented and expanded. The implementation of cloud robotics device clusters in combination with edge computing requires further research. They need to develop a cluster model and mathematical software for cloud robotics systems in combination with edge computing to minimize information processing and decision making time.

## CONCLUSIONS

The analysis allowed us to generalize cyber threats to the components of Cloud Robotics systems. As a result, it is determined that the largest number of attacks occur on cloud network devices, and the use of wireless communication technologies between the elements of the system creates the preconditions for a cyberattack on the system. It is determined that today multi-stage complex protection systems are being implemented, based on the use of the latest technical means, qualified personnel, control procedures, administrative regulations with their strict observance. The analysis of attacks allowed determining their list and exploring the features of implementation. As a result of the analysis and generalization, recommendations for counteracting attacks on the components of the Cloud Robotics Devices system have been developed.

## REFERENCES

[1]G. Immerman, The importance of edge computing for the iot, 2020.
URL: https://www. machinemetrics.com/blog/edge-computing-iot. [2]Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet
of things: perspectives and challenges, Wireless Networks 20 (2014) 2481–2501. doi: 10.1007/ s11276-014-0761-7 .
[3]S. Shokaliuk, Y. Bohunenko, I. Lovianova, M. Shyshkina, Technologies of distance learn- ing for programming basics on the principles of inte- grated development of key compe- tences, CEUR Workshop Proceedings 2643 (2020) 548–562.
[4]A. Vovk, Methods of information security IoT, Master’s thesis, NTU of Ukraine ”KPI named after Igor Sikorsky”, 2018.
[5]M. Young, The Technical Writer’s Handbook. Mill Valley, CA: Univer- sity Science, 1989.