International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 26th Nov 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-12

DOI: 10.48047/IJIEMR/V09/I12/79

Title: CLOUD ROBOTICS: CURRENT SECURITY STATUS AND SECURITY ISSUES WITH CLOUD ROBOTICS DEVICES ON THE REMOTE LOCATION
Volume 09, Issue 12, Pages: 409-420
Paper Authors

DR. RISHI KUMAR SHARMA,MRS. ARADHANA SAXENA,DR. R.K. KAPOOR

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CLOUD ROBOTICS: CURRENT SECURITY STATUS AND SECURITY ISSUES WITH CLOUD ROBOTICS DEVICES ON THE REMOTE LOCATION

DR. RISHI KUMAR SHARMA[1],MRS. ARADHANA SAXENA[2],DR. R.K. KAPOOR[3]
[1]Assistant Professor (CSE), Scope College of Engineering ,Bhopal 462010,India
[2]Assistant Professor (CSE) ,Scope College of Engineering ,Bhopal 462010,India
[3]Associate Professor (CS), NITTTR ,Bhopal 462010,India

ABSTRACT: With the development of data science, cloud network and other robotics technologies, Cloud robotics involves several robotics working together to execute any task. Working with more than one robot can be done inside the cloud robotics. Cloud robotics combine, cloud robotics and multi robot system to design a new system called multi robot system (MRS).MRS improve the real time working performance with low cost. This research work describes the current security status, and security issues and architecture of Cloud Data Security System (CDSS).

Keywords: Cloud Network, Big Data, Cloud Robotics.

I. INTRODUCTION: The starting of robots in industrial organization production in the past some decades has incurred many improvements in the industrial and robotics sector. Robot friends are becoming much familiar in our lives. These days, the nature of warfare has fully changed drastically, and technology plays a key role in shaping warfare tactics. Intelligence, Observation and Reconnaissance (ISR) is one of the important applications where army satellites are used. UAVs, UGVs, USVs, ROVs, AUVs, and others are broadly used in the ISR application. So Cloud robotics network security is most important for the remote device. With the evolution of robotics, pre - programmed robots have reached advanced levels of working performance in the real-time robot applications, accuracy, compatibility and robustness. As network technology evolved during later part of the 1990s, researchers evolved and improved the control of robotic network system and their robustness, and the field of ``networked robotics" [4] appeared.

A robotic communication network refers to set of robots connected by the communication network system [5]. A robot in the networked robotics is regarded as node. With the help of sensing data shared among nodes, the node task can transmit command information remotely and receive feedback measurement, thus ensuring that unique operation is carried out. With the evolution of big data ,cloud computing [7] and other latest technologies , the unification of cloud technology and (MRS) multi-robot systems allows for design of MRS with high complexity and high performance . At the 2010 Humanoids conference, James J. Kuffner proposed concept of ``cloud robotics'' [10] and detailed the potential benefits of robot clouds for the first time.

However, many technical issue cannot be ignored. With the starting of cloud computing, the selection of types of computation communication modes and distributions that should be applied in apart scenarios is critical for overall execution performance. Another most important aspect is cloud security, especially the storage of important data in the cloud; increases the requirements on various aspects of the systems. Finally, to ensure real-time performance, choosing the service quality guarantee methods and corresponding effect analyses is challenging.

In this research work, there are two important contributions as follows:

1.The main enabling techniques of cloud robotics are analysed, inclusive of big data, cloud computing, cooperative robot learning, open source resources , and secure network communication.

2.The main problems and challenges of these days, cloud robotics system are stated: secure data interaction between robots and the cloud platform, cloud security, and service quality guarantee technique and effect analysis.

II. THE ARCHITECTURE OF CLOUD ROBOTICS:

Cloud robotics main aim at transferring the high complexity of the computing process to the cloud platform by communication technology. This greatly lower the computational load on the robots.

The architecture of cloud robotics is mainly developed 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. Accordingly, the cloud platform is composed of a large number of high-performance servers, proxy servers, massive spatial databases and other components.

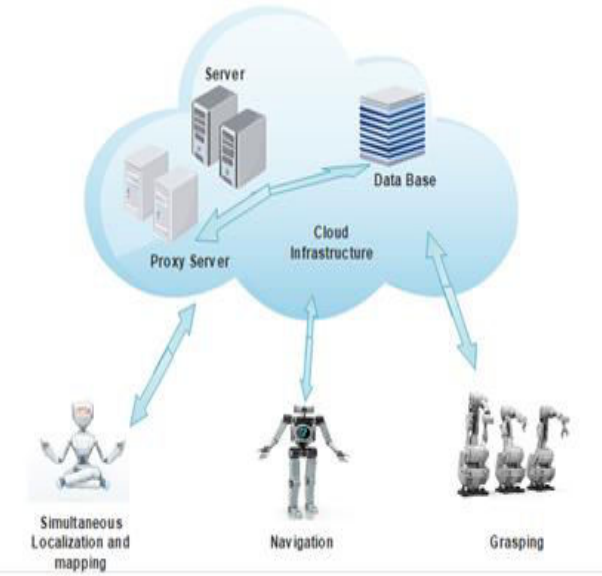

Fig.1 Architecture of Cloud Robotics

III. NETWORK CONNECTIVITY:

Connectivity develops with cloud robotics system as well. Traditional inter communication system within cloud robotics is a typical Machine-to-Machine (M2M) communication mechanism. Collaborative learning requires that the global task priority is greater than the priority of the node task, and this applies to dynamic packet interaction and control as well. These constraints result in higher quality requirements on the control system algorithm.

It is worth noting that inside-machine communications system usually use active and ad hoc routing protocols . In unfamiliar environments, networked robots may choose a proactive routing protocol to determine a path. Proactive routing protocols include periodic packet switching and routing table updates, which makes the consumption of computing resources and memory resources particularly large.

With the starting of cloud infrastructure, robotics under clouds have another choice to deal with computing or storage task. However, latency is a challenging problem in traditional network robotics.

In the cloud scenario, expense of time is divided into four types:

1) pre-processing time for sending and receiving specific data;

2) time used in sending and receiving data which has a lot to do with data size and network bandwidth;

3) time consumed in cloud for data processing; and

4) network delay which is inevitable. To make the introduction of cloud practical, the sum of above elements should be less

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

than time consuming without cloud.

S.No.	Approach	Model	Resource	Caused by	Energy cause by	AI Level	Robotic Application
1	Stand Alone	On Board Computing	Weak	Computing Load	Computing Load	Weak	Static & structured
2	Network Robotics	Ad-hoc cloud computing	Medium	Computing & Communication Load	Computing & Communication Load	Medium	Real-time processing
3	Cloud Robotics	Hybrid System(cloud computing +Ad-hoc cloud computing)	Strong	Only Communication Load	Only Communication Load	High Level	Combine System (real-time processing + resource-intensive)

Table1.Comparisons of Approaches

IV. KEY ISSUES AND CHALLENGE

This section focuses on key issues & challenges in cloud robotics. In computer networks, there are a variety of insecurity factors. Cloud robotics platforms require to interact using data or information, which means that data to be analyzed must be uploaded in a few format. In addition, the processed data information also require to be returned from the cloud robotics platform to the robot in a certain form. Finally, the introduction of service quality assurance systems and effects' analysis, in order to maintain the network flow for a given bandwidth enhances real-time performance and computational efficiency. New insecurity factors are constantly emerging. In this work, the author finds out that insecurity factors mostly lie in the following six aspects.

1.Cloud Robotics Environment

Robot network is connected to application of robots in different regions through radio waves or cable links. Robots are connected with networks to receive information passed via the networks. In the of transmission of information, the lines are inevitably subject to the influence of natural environment and social environment, thus imposing huge adverse impact on the network. In nature, there are several factors that affect network security.[1]For example, extreme humidity, temperature, earthquake, anti-dust conditions, fire, wind and some prominent incidents will all cause serious damage to and influence on the network in terms of transmission lines on the one hand and the stability of the network on other hand.

2.Cloud Robotics Resource Sharing

Existing robotics network has increasingly high requirements for resource sharing, including hardware, software and data sharing. Both robot-robot and robot-server resource sharing is required, so robot-base-center (RBC) can quickly access network and robot information even if they are in a different place, very convenient. However, at same time, this convenient process also presents some “opportunities” for some

attacker people and many illegal attackers may take advantage of certain loopholes to steal or destroy information. In addition, robots' own software or hardware failure can also cause robot-network security problems, resulting in undesired disclosure. Moreover, since most of the robot network transmission has to pass through a certain distance, there will be certain time difference between resources available for sharing on the robot network and the actual use by RBC, such as network robot task. In such distance, robot-network security issues may also arise, providing convenient temporal and spatial conditions for illegal theft of information.

3.Cloud Robotics Data Communication

In robot- networks, information transfer and exchange is completed through data communications. The transmission of data needs physical lines, radio waves and some electronic equipment for support. Insecurity factors also exist in such basic equipment. Information in the transmission process is quite vulnerable to damage, such as network line radiation, wiretapping and so on.

4.Computer Virus

In robot-networks, sharing of resources is expected to be achieved as much as possible, so there are generally a number of robots receiving information. Since there is no path to guarantee the security, each robot is much vulnerable to infection of viruses. Once the virus intrudes a robot, the results would be disastrous. The virus will have rapid regeneration and infection in the robot-network, soon spreading to the entire network and making all robot-network stages infected. If there is no good emergency measure, the virus can paralyze the entire robot-network in very short time.

5.Hacks

The hacker to find and attack the robot-network operating system's flaws and defects for the purpose, the use of robot-network security vulnerability for illegal activities, also known as cloud robot security an attacker. These attackers they employed to modify the robot-software, illegal invasion of the host to destroy others procedure, steal online or other information. The above heavy means although its purpose is not the same, but all of the robot-network information security system constitutes a threat, even some network attacker (hacker) can destroy the robot-network the release of hardware virus, resulting in the whole network system.

V. CHECK AND PROMPTLY REPAIR NETWORK SECURITY VULNERABILITIES:

Cloud robotics Network security vulnerability detection should be carried out frequently by the base-center, because it can help them to detect all kinds of insecurity factors and a variety of robot-network security vulnerabilities for timely detection and timely treatment, so that any vulnerabilities can be repaired and the results of such repair can be verified promptly. Vulnerability detection mainly includes three aspects—network vulnerability scanning, system security scanning and database system security scanning. The first is network vulnerability scanning, which conducts "black box" evaluation of internal network systems from the boundary points of network security. Scanning and analysis of the entire network from the perspective of cloud robotics network intruders can detect hidden safety issues or defects, which also needs to use the means of attacks contained in the knowledge data of the software itself. When such analysis detects any defect and loophole, corresponding repair recommendations will be proposed. The second is system security scanning. Each robot system is equipped with a system security scanner which is configured to the key service host as an agent. The scanner checks common system configuration errors and security vulnerabilities from the inside of the system, such as permission settings for key documents, user settings, path settings, ID settings, network service configuration, credibility of applications, etc. The system also has another function which is to find signs of hackers' attacks of the system and thus propose appropriate repair recommendations. The third is database system security scanning. A knowledge base of software itself exists in the database security scanner, which also contains all security weaknesses. So such scanning can, by using the existing settings, check the database services of the target host item by item through the network or the inside of the system, and then conduct a comprehensive assessment of the database after the thorough inspection. All security vulnerabilities, authentication, authorization, integrity and other issues are used as criteria for evaluation, such as account permissions, user settings, configuration status, intensity & duration of code password, patches and fixes, etc.

1. MAKE CLOUD ROBOTICS RATIONAL USE OF FIREWALL

All applications of the robot network

usually would set a firewall to defend the internal network from attacks. The so-called firewall refers to the establishment of a security control point in internal or external network or between any two networks. Any flow of data passing through the firewall needs to go through testing to decide whether to allow, reject or redirect, so that all incoming and outgoing network services and visits will be audited and controlled. Information security can be guaranteed, and the internal network can be protected from malicious attacks as much as possible.

2. IMPLEMENT INTRUSION DETECTION TO PREVENT HACKER ATTACKS

Intrusion detection is implemented to detect malicious and suspicious activities in cloud robotics network, and intercept and prevent them in a timely manner once discovered to ensure the normal operation of cloud robotics network. The damage caused by network intrusion sometimes is unimaginable. Therefore, once network intrusion is detected, effective measures must be taken immediately to stop it to minimize its consequences.

3. BACKUP AND TECHNOLOGY

In the cloud robotics network, data may often be interpolated destroyed due to malicious intrusion. To tackle with this, base center should pay attention to robotic-application backup and recovery technology. Data backup and recovery should become a habit, because system failure is inevitable in database system operation and loss of data often occurs. If database backup is well performed in advance, you do not require to worry even if a sudden system failure leads to the destruction of important data, because there is an intact backup of the data for restoration. Data backup is a wise act of precautions. After unpredictable failures, administrators can use the data backup to restore database to the state before the failures. In this path, the integrity and consistency of the data can be guaranteed.

4. RESOURCE ALLOCATION AND SCHEDULING

Uploading computational tasks with high complexity to the cloud is one of major notable characteristics of cloud robotics. Considering many working equipment, application, interface settings, and cloud robotics network environments, for a given computational task, choice of uploading, self-processing or assigning task to the nearest robot has an important impact on overall execution performance.

It is worth noting that, as with inter-machine communications, the amount of computations on the cloud makes the emergence of delays more likely. New algorithms and techniques are needed to

counter changes in robot- network delays in real time. Although wireless technology has made most important progress, once connection problems between the robots and cloud services appear, serious delays are almost inevitable. Therefore, when designing a new algorithm, we need to design a load distribution algorithm with an ``any time'' characteristic. Once it is apparent that a task that cannot be properly uploaded to the cloud, a mechanism for dynamic allocation of computing tasks should be activated, thereby reducing delay time.

Considering the big size of a information stream in the SLAM, navigation and another robotic applications, the major critical aspect is computation-communication trade off. As described above, major time consumption should be less than the on-board time consumption.

VI. CLOUD SECURITY AND SAFETY ISSUES

The introduction of cloud robotics technology (CRT) has greatly expanded the complexity of multi-robot operations. At same time, it also introduced new technical challenges: the privacy and security issues brought by the CRT . These hidden problems also affect information & data generated by robotics devices and sensors used in cloud robotics. Commercial science and technology solutions have suffered from serious data leakage incidents, especially during the upload of photos and video to the cloud . In scientific research and industrial practice, key data stored in cloud may be far from hacker to steal, leading to the loss of key data.

On the technical front, identity management and access control systems are two of the most important aspects of cloud robotics security. Current proposed solutions comprise a combination of multi identity and personal M2M authentication system with layered encryption. Additionally, data security is at the core of cloud security, which is composed of isolation protection of dynamic and static data storage. More effective integrated verification algorithms are key for data integrity. Also, another aspect of cloud security which deals with providing software-as-a-service (SaaS), has virtualization technology as its basis. Therefore, network, storage and server virtualization, are essential subsystems, which means that security mechanisms such as VM security isolation, access control, VM resource constraints, etc. need continuous improvement.

Safety is essential for robots, given the mission-critical deployment of many

cloud-robotic applications such as air and ground transportation systems, disaster monitoring and warning systems, and medical and healthcare systems. It is therefore important to ensure the overall stability of physical systems to avoid potential dangers such as imminent collision. ISO 60601 defines safety as avoidance of hazards to physical environment during operation of medical application under normal or single-fault conditions . We believe that this definition of safety can also be applied to nonmedical domains such as cloud robotics by broadening the scope of the hazards considered, including radiation leaks, faulty operation of the computation unit, thermal effects, software failures, biocompatibility issues, electrical hazards, and mechanical hazards. However, because there are various fault sources in the physical, networking, sensing, computing, and actuation domains that can make systems behave anomalously, it is challenging to get this goal in cloud robotics. Many uncertainties exist in their environment and physical systems. Any one of a variety of types of failure can occur at any place and at any time in cloud-robotic systems .

More work is needed on interaction safety [9]. There are two major cases. The first is when the cyber-physical interaction between the computation units in two different individual robots may affect either one's operation in hazardous ways. Second, the cyber-physical interaction between the computation units and physical environment may have harmful effects on the physical environment. The nature of physical environment may hinder operation of the computation unit in the second case. For example, tissue growth around implanted sensors could reduce communication and sensing capabilities.

Finally, from the social perspective of the robotic community, work is required to enhance the safety of cloud robotics. First, laws, regulations, and social structures such as insurance should be in place. Second, high-quality simulators are needed and robotic test fields should be constructed. Third, robotic systems should be continuously tested, and exercised at real scenarios (such as disaster sites) and in simulated mock-ups. Fourth, there should be active user communities to enable information exchange and user collaboration. In other words, sufficiently robust technology must be adopted for robotic systems developed for use at real scenarios (such

as disaster sites). Otherwise, it would be unclear if the cloud robotic systems could work well in real scenarios, for example. If a robot becomes inoperable on an access path, the robot itself would become an obstacle to other robots [6].

S.No.	Model	Real time Communication	Trust	Cost	Coverage	Self-Organization	Challenges & issue
1	Mobile ad-hoc NW	Good	Fair & Clear	Good	Fair	Best	P2P Communication
2	Delay tolerance NW	Bad	Fair & Clear	Good	Good	Fair	Long delay
3	Movable base Station	Good	Good	Bad	Good	Fair	Distribution and adjustment is difficult

Table2.Comparisons of Different Models

VII. PRIVACY AND SECURITY ISSUES

Because individual robots upload their personal private data for storage and processing by a remote cloud, there is a major concern about privacy and the leakage of private information [3]. A particular privacy issue for mobile robots is the leakage of their private location information in location based services. To solve the problem, a method called ``location cloaking'' makes users' location data slightly imprecise before being uploaded to the remote cloud [8]. Sometimes, however, imprecise data could not provide satisfactory or relevant results for some certain applications. Therefore, location cloaking needs to be adaptively tuned to balance trade-off between result accuracy and privacy for cloud robotics.

Security issues arise from every aspect of cloud robotics. This includes security for individual robots (e.g., eliminating the threat of worms and viruses), security in the cloud data-center nodes (e.g., preventing unauthorized access to personal data stored in the remote cloud), and security for data transmission over networks (e.g., encrypting communication protocols). First, security system should be lightweight, without involving much computation power and energy consumption by the robots. Second, cloud clones (copy robot) should be trusted. The robot should be able to check the identity of the cloud clone based on trust measurements or to identify a trusted cloud clone by itself . Third, storage and computation services provided (SP) by the cloud computing platform must be trusted. Finally, there is an urgent demand for technologies that endeavour to enforce security and privacy in data transmission when moving crowd sourced data to cloud data centers [1]. Blockchains [2] which has been considered as a potential solution to

address concerns of vulnerabilities, potential threats, and attacks, needs further research for cloud robotics.

VIII. CONCLUSION

Cloud robotics network security involves square respect area ,is a complex system. It is needed for the upkeep of the multi-robot participation, but also to engage the front prevention, monitoring, and afterwards make up for 3 understaffed, continue to strong safety consciousness, improve safety mechanism, establishing security technique & policy, thus enhancing security of cloud robotics network .Computer technology and network technology are widely used in real world, bringing convenience to robotics technology. But it also has its personal shortcomings, of which the most criticized is security issues, requiring key breakthroughs in the efforts to ensure computer network security. In this article, the author analyzes the reasons for security issues and technical countermeasures. It is believed that with growing maturity, cloud robotics network technology will bring more and more convenience and security to people's life and work.

References

1. C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, " Trust-based communication for the industrial Internet of Things," IEEE Commun. Mag., vol. 56, no. 2, pp. 16 22, Feb. 2018.
2. K. Christidis and M. Devetsikiotis, ``Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292 2303, 2016.
3. J. Mahler, B. Hou, S. Niyaz, F. T. Pokorny, R. Chandra, and K. Goldberg, " Privacy-preserving grasp planning in the cloud," in Proc. IEEE Int. Conf. Automat. Sci. Eng., Aug. 2016, pp. 468 475.
4. IT Technical Report, accessed on Oct. 2015. [Online]. Available:http://www.nytimes.com/2014/08/18/technology/for-big-data-scientists
5. F. Li, J. Wan, P. Zhang, D. Li, D. Zhang, and K. Zhou, ``Usage-speci c semantic integration for cyber-physical robot systems," ACM Trans.Embedded Comput. Syst., vol. 15, 3, 2015, Art. no. 50.

6. H. Osumi, " Application of robot technologies to the disaster sites," in Report of JSME Research Committee on the Great East Japan Earthquake Disaster. Tokyo, Japan: Jpn. Soc. Mech. Eng., Feb. 2014, pp. 58 73.
7. Y. Zhang, M. Chen, S. Mao, L. Hu, andV. C. M. Leung, " CAP: Community activity prediction based on big data analysis," IEEE Netw., vol. 28, no. 4, pp. 52 57, Jul./Aug. 2014.
8. F. Liu et al., " Gearing resource-poor mobile devices with powerful clouds: Architectures, challenges, and applications," IEEE Wireless Commun., vol. 20, no. 3, pp. 14 22, Jun. 2013.
9. A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, " Ensuring safety, security, and sustainability of mission-critical cyber physical systems," Proc. IEEE, vol. 100, no. 1, pp. 283 299, Jan. 2012.
10. J. J. Kuffner, " Cloud-enabled robots," in Proc. IEEE-RAS Int. Conf. Humanoid Robot., Nashville, TN, USA, Nov. 2010, pp. 176 181.