International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Probabilistic Security Interface for IOT Devices in the Cloud Network

Rishi Kumar Sharma, R. K. Kapoor, Pavan Kumar Sharma

***Abstract:** In the real world cloud robotics network are highly structured. The network security and IOT devices ability to cope with complex problem in such cloud environment crucially depend on exploiting this network security structured.C2M (Cloud to Machine) is the core network technology to implement cloud robotics. This paper firstly introduce the concept of C2M with Cloud Heritage Technique and the cloud network architecture of C2MHT (Cloud to Machine Heritage Technique) .Then it analyses the cloud security threats of C2M , moving the C2M robotics devices to unauthorized location and note.*

***Keywords :** C2M , C2MHT, Security Threats , Cloud Robotics.*

I. INTRODUCTION

With the development of the cloud environment, as a core mechanism of the cloud network, C2M has become a rich cloud (satellite network to be hotspot etc).Planning in high-level network robotics system is a fundamental and critical security problem.

Cloud Robotics is a specific field of robotics in which cloud network techniques like cloud computing ,cloud data base and the participant internet technologies are invoked for empowering the inter structure and shored cloud services for different robotics application.

Connectivity while the cloud network enable robotics system to be benefited through the powerful computation resources, data storage facilities and the communication of the data centre available in the cloud due to which sharing and processing of data from multiple robot units can be made possible. Inclusion of cloud computing techniques with robotic systems also enable humans to delegate tasks to robots remotely.

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author
Dr. Rishi Kumar Sharma*, Department of Computer Science Engineering, College Scope College of Engineering Bhopal (M.P.) India.
Dr. R. K. Kapoor, Department of Computer Science Engineering, National Institute of Technical Teachers' Training and Research, Bhopal (M.P.) India.
Mr. Pavan Kumar Sharma, Department of Computer Science , College Scope Jawaharlal Nehru P.G College Bhopal (M.P.) India.

Therefore, deployment of cloud computing technologies improves the operational performance and capacity of robotic systems by making them cost-effective and light weight by rendering them an intelligent brain in the form of cloud network.

As to the C2M security, C2M will face many threats in its Hardware application. How to secure the network of device privacy (Like ID, MAC Address, etc) and prevent the current cloud network security threats, we will face.

The rest of this paper is organized:-

1. C2M (Cloud to Machine)
2. Architecture and difficult of C2M network communication
3. Security threats

II. CLOUD 2 MACHINE

C2M architecture is divided into 4 part (fig 1). They are M2M and M2U, cloud network and C2M device layer, as shown in fig 1. C2M and M2U part is composed of base M2C server, C2M network and across point. The cloud network part include the satellite ,wireless and wire network ,it is responsible for communication sensory data (instruction) from the C2M and M2C.C2M AI based server is used to real time storage and transmit the data to the remote location (C2M part).

In the IOT devices (C2M Devices) process M2M, how we can ensure the device reliability and cloud network security of perception data in the M2C devices .

How to ensure the confidentiality and integrity of information in the signal transport process.

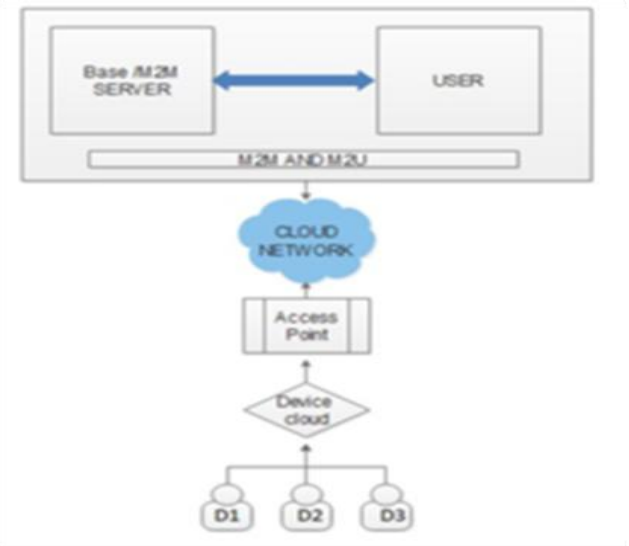

Fig 1. C2M Architecture

How to ensure the security of the Base server (M2C) and all kinds of remote devices. How to provide the secure and reliable data for Base.
How to achieve C2M remote monitoring and to understand the propose of all kind of C2M devices data timely and accurately these all type data security challenges of M2C and C2M

C2M consist of 3 main subsystems:-

1. M2M (machine to machine)and M2U (machine to user)
   a. Learning Approach
   b. Optimized network technique
2. Cloud Automated modeler network
3. M2C (Machine to cloud)
   a. Leaving approach for network
   b. Ai module for base and front

The core of the IOT or cloud robotics is interflow and inter connection between IOT device, namely D1,D2,D3 is the major from of C2N (Cloud to network) at this condition . In this narrow senses, C2M refers to the cloud machine communication .C2M is an extended to the cloud to machine operator to machine.
C2M is a machine and human based expert system employing AI for configuring devices, and evaluating cloud network most suited to the robotics environment and devices .C2M passes a feasible cloud network solution . According to the C2M function of its implementation, C2M can be divided in to:- Control location ,monitoring, online maintenance and device terminate , tracking.

Fig 2. M2M & M2C Architecture

III. AIMING OF THE REMOTE LOCATION APPLICATION (RLA) REQUIRMENT

When remote location application receives instructions. It should be able to verify the identity of the RLA of the instructions and be able to use the security parameters being stored in the RLA and the cloud N/W protected trigger instructions. So as to protect the RLA from the fake trigger control.

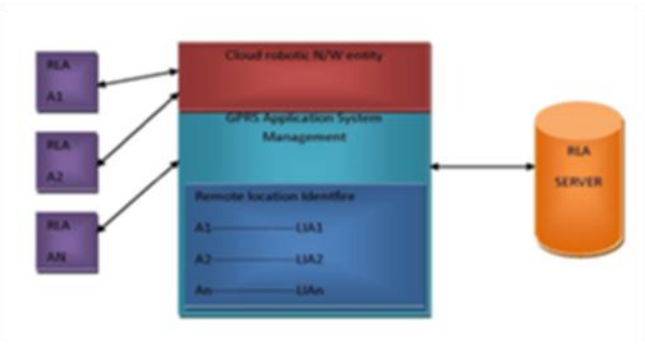

Fig 3.RLA Location ID

IV. RESEARCH ON CLOUD TO MACHINE HERITAGE TECHNIQUE (C2MHT)

Based on the M2M security technique, M2M security threats and the security system of C2M is proposed to solve the M2M network robotics security system problems. Which is shown in fig:-

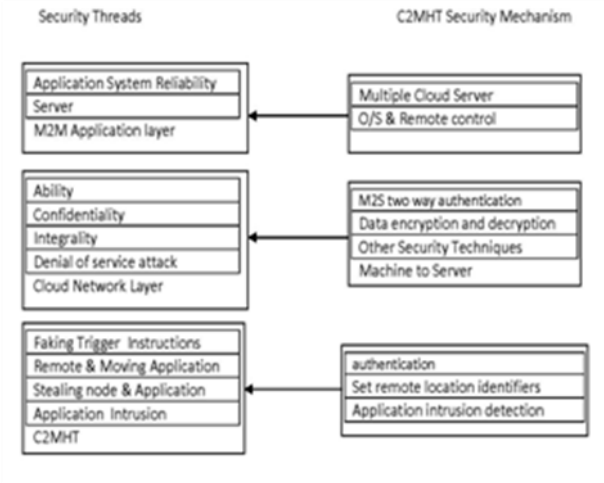

Fig 4. C2MHT

The C2MHT, which can be static or modulate network are used for gathering remote application information. The static network can obtain their remote application localization through C2MHT. The IOT & Cloud robotics application can move across different domain area within the cloud communication network, where the application authentication is required when they come into a new domain area.

V. ANALYSIS OF M2M AND C2MHT

Table- I : M2M & C2MHT

S.No.	M2M	C2MHT
01	M2M devices can be attached to the local network via both wired as well as wireless systems.	C2MHT is based on cloud network, which will be provided by CSP.

02	M2M network easy to maintain and create.	C2MHT is also easy to maintain and safe.
03	It uses minimum latency, consume less energy, has higher range and higher throughput.	C2MHT usage consumes less energy, higher range of service and normal throughput. C2MHT has higher rang of service and normal throughput.
04	It enables communication of machine without any third party intervention.	C2MHT enables communication of machine with or without any third party intervention.
05	The security issues, in IoT network are solve by using M2M technique facility.	The security issues, in IoT or cloud robotics network can solve by using C2MHT technique facility.
06	With the help of M2M technique high level of protection can be provided to large data .	Using C2MHT technique ,protection large group of divices and collected data is possible.
07	Utilization of cc with M2M makes the system dependent on cloud due to which flexibility and innovation become defaults.	Use of the cloud robotics with C2MHT also leads to cloud dependence but without limiting innovation and flexibility. .
08	In M2M technique security and ownership of data is the central problem.	In C2MHT technique ownership and data security not a problem.
09	Interoperability between cloud and M2M, IoT machines is a major issue in such network.	Interoperability between C2MHT and IoT machines is not a big problem.
10	M2M technique requires internet connection with reasonably high speed.	C2MHT technique does not demand internet connection with high speed.
11	Response time is M2M technique is high.	Response time is M2M technique is low.
12	Installation and operation cost for M2M is high.	C2MHT technique incurs less cost for Installation and operation

M2M and C2MHT devices will require data integrity validation which shall assure the integrity, consistency and accuracy of the data during its storage processing and retrieval .Therefore a trusted environment will be provided which can protect the sensitive data and assets in context of confidentiality and integrity by ignoring threats from the external entities .

In the M2M , there is ever a possibility of insider attack and outsider attack. Keys can be accessed or stolen by hacker without the permission and knowledge of end users. Our purpose is to provide secrecy to the network and smart devices as well as keys that are stored in C2MHT. The proposed C2MHT mechanism provides better network security and devices management system in the cloud robotics. This technique also offers superior security against server clouding, Byzantine failure and data modification attacks.

VI. CONCLUSION

Now this time in IOT and cloud robotics industry, M2M will have large range of hardware application. So, solving the problem of network robotics security for application and population has most important significance. This research work introduces the concept of C2M . One of the main feature of the C2M communication network is the fast continuously advancing and charming technique. This C2M technique enhancing interactive network security design analysis and increase the secure C2M expert security system scope through updating and terminating ability.

This work is not intended to make a comparison of M2M vs. C2M approaches. Our research work will show that both approaches have advantages. There are many factors that determine which planning approach is better-suited to the domain and problem. The focus of this systems paper was to describe the integration of probabilistic planning into C2MHT, and to demonstrate the execution of probabilistic security plans in real-time cloud robotics application scenarios.

The focus of this technique was to describe the integration of probabilistic robotics application security planning into C2MHT, and to demonstrate the execution of probabilistic plans in real-time robotics . This technique has involved the implementation of online dispatcher that uses the CHT architecture. Moreover, as the online configuration conforms to the Client/Server protocol used in the cloud robotics application.

REFERENCES

1. Atrash, A., Koenig, S.: Probabilistic planning for behavior-based robots. In: FLAIRS. pp.531–535 (2001).
2. A. Garg, P. Maheshwari, »A Hybrid Intrusion Detection System: A Review,« Intelligent Systems and Control (ISCO), 2016 10th International Conference, Coimbatore, India.
3. Atrash, A., Koenig, S.: Probabilistic planning for behavior-based robots. In: FLAIRS. pp. 531–535 (2001)
4. Buksz, R.D., Cashmore, M., Krarup, B., Magazzeni, D., Ridder, B.C.: Strategic-tactical planning for autonomous underwater vehicles over long horizons. In: IROS (2018).
5. Boutilier, C., Dean, T., Hanks, S.: Decision-theoretic planning: Structural assumptions and computational leverage. Journal of Artificial Intelligence Research 11, 1–94 (1999).
6. C.-Y. Chiu, C.-T. Yeh, Y.-J. Lee, »Frequent Pattern based User Behavior Anomaly Detection for Cloud System,« 2013 Conference on Technologies and Applications of Artificial Intelligence.
7. Celorrio, S.J., Fern´andez, F., Borrajo, D.: The PELA architecture: Integrating planning and learning to improve execution. In: AAAI (2008).
8. Dean, T., Kanazawa, K.: A model for reasoning about persistence and causation. Computational intelligence 5(2), 142–150 (1989).
9. D. B. T. S. M. S. A. E., R. J. , »Feasibility of Supervised Machine Learning for Cloud Security,« Information Science and Security (ICISS), Pattaya, Thailand, 2016.

10. Grisetti, G., Stachniss, C., Burgard, W.: Improved techniques for grid mapping with raoblackwellized particle filters. IEEE Transactions on Robotics 23(1), 34–46 (2007).
11. Littman, M.L.: Markov games as a framework for multi-agent reinforcement learning. In: ICML. pp. 157–163 (1994).
12. Songjie, J. Yao, C. Wu, »Cloud computing and its key techniques,«, Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference , Harbin, China, 2011.
13. Yoon, S.W., Fern, A., Givan, R.: FF-Replan: A baseline for probabilistic planning. In: ICAPS. pp. 352–359 (2007).
14. Microsoft 2017. Compute Linear Correlation, Available: https://msdn.microsoft.com/en-us/library/azure/dn905819.aspx.

AUTHORS PROFILE

Dr. Rishi Kumar Sharma is Assistant Professor in Scope College of Engineering Bhopal. He has done Ph.D. from Rabindra Nath Tagore University, Bhopal and MCA (Master of Computer Applications) from University of PTU. His research area includes Cloud Robotics, Cloud Security, Deep Space Network, IOT, Computer Vision and Computational Intelligence, Email – rishi.rishi1526@gmail.com.

Dr. R. K. Kapoor is Associate Professor in National Institute of Technical Teachers' Training and Research, Bhopal. He has done Ph.D. in the area of Adhoc Network Routing Protocols. His research area includes Adhoc network routing protocols, Cloud computing, Cloud security, Image processing, data security.

Mr. Pavan Kumar Sharma is Lecturer in Scope Jawaharlal Nehru P.G College , Bhopal. He has done MSc in Computer Science from Makhanlal Chaturvedi University. His research area Network Security ,DBA,AI.