International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

xx

COPY RIGHT

IJIEMR Transactions, online available on 03th May 2024. Link

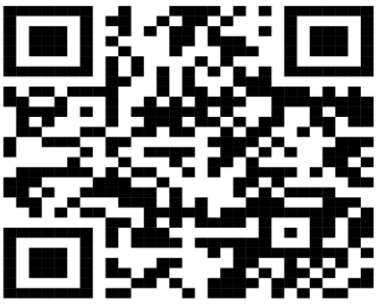
http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue5

10.48047/IJIEMR/V13/ISSUE 05/06

TITLE: Evolution of Remote Device Security System: From Remote IoT Device to Cloud

Volume 13, ISSUE 05, Pages: 48-51

Paper Authors **Nitu Sharma, Dr. Ramesh Vishwakarma**



International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Evolution of Remote Device Security System: From Remote IoT Device to Cloud

Nitu Sharma, Dr. Ramesh Vishwakarma

Research scholar (PhD) Rabindranath Tagore University Bhopal(MP), India nitutct@gmail.com

Dept. Computer science Rabindranath Tagore, University Bhopal, India rameshaisect@gmail.com

***Abstract*—**IoT devices have impacted nearly every part of life, whether they are used for essential or recreational purposes. The majority of conventional IoT devices use on-board processing units that are already configured and work in well-defined con- texts. By adding remote load-balancing techniques the robotics devices the device can communicate with each other to perform the desired job which reduces network intervention. In this work, we propose a remote device load-balancing technique in IoT. Load balancing is done by device computing multipath routing, and multipath routing is computed based on the remote base device of data such as the quality of the link. However, the sophisticated processing needs of contemporary and anticipated Internet of Things applications surpass the capabilities of on- board computing capacity. IoT cloud and associated technologies can increase performance efficiency and have a great potential to get over onboard hardware limitations. This study emphasizes IoT as an emerging trend while showcasing developments in IoT application security. A significant amount of work has been done to address emerging issues and maximize the potential of IoT ap- plications. Furthermore, there are encouraging developments for the next generation of adaptable, intelligent, and self-governing robotic systems in the Internet of Things age.

***Index Terms*—Remot Device Load balancing, Remote device load balancing , Cross-Data Evaluation**

I. INTRODUCTION

IoT is known to be the communication of the internet with real robotics devices expanding the thought from device-to-device communication to device-to-IoT cloud communication. By adding intelligence to the IoT devices, devices can communicate with others to perform the assigned job which in turn reduces the attacker's presence. In modern years, Cloud IoT has grown to be an important topic for researchers across the world. It has made its method into different scopes like transportation, cultivation, commerce, and healthcare due to its quality like running in an IP-based network and capable of holding millions of robotics devices and the IoT devices are capable of communicating and cooperating to achieve a target. In IoT devices, the communication among the devices can be carried out by using IoT cloud networks. The remote server is used to stock up and progress the data. Because of the limitation of range, power utilization and computational potential of robotics devices, the caching and dealing out will be constrained to some accessible resources. In IoT device routing plays an important role. Routing is the most demanding element that is considered in cloud IoT because of its in-built properties. Sometimes routing protocol explains how routing procedure takes place among the devices communicates with one another in the network and transfers the control data to select the best routes among multiple routes .

In the routing technique, the data has to be shared from a source robotics device to the destination robotics device using the nearest neighbor cloud robotics network. The best network path from the source and the destination robotics is calculated using the routing algorithms. The load balancing can be used to distribute the cloud robotics devices (CRD) among all the CRDs so that energy should be consumed among all CRDs equally and the network efficiency is also improved .

This paper presents context-aware load balancing in cloud IoT, load balancing is the spreading of the traffic along multiple routes that reduce the packet loss in the network. Load balancing is done by computing multipath routing among the source CRD and the destination CRD. Multiple routes help in increasing the reliability of CRDs for data transmission and throughput using energy consumption and bandwidth aggregation.

II. CROSS-DATA EVALUATION TECHNIQUE

It entails supplying data in two new steps so that the algorithm can be trained and evaluated: Divide the data into folds, which are smaller subsets that are utilized for training and evaluation, respectively for security.

III. REMOTE DEVICE LOAD BALANCING TECHNIQUE IN THE IOT

This section describes the remote device load balancing, security, quality of the link, proposed block diagram, and multipath computation.

The cloud IoT network environment is shown in below figure 1. It consists of IoT devices that are randomly deployed. It also consists of a gateway, cloud, and remote network. Cloud IoT devices gather the data and it sends data to the cloud through the gateway. The cloud stores the data of each device in the network and stored data helps in computing the path from the source to the destination device. In the remote device network, actual data is not stored, just the information of the

data is stored. The remote network gives the stored information to the source device to initiate the path discovery.

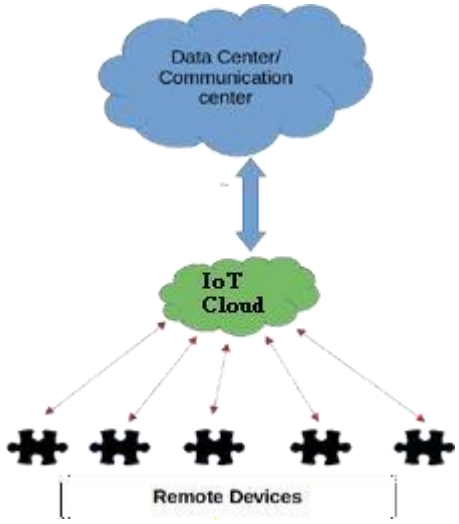


Fig. 1. Cloud IoT Environment

Example Scenario Let us consider D1, D2, D3, D4 Dn is the IoT device assigned to each device in the path.The highest data factor is given the first priority to send the data through it. The data factor of each robotics device i.e D1, D2, D3, D4, D5, D6 is calculated using the equation (Nearest Base = Initial robotics device - Current robotics device).

The total weight factor of path one (Dp1) is

Dp1=Sum (D1, D2, D3, D6) ——————- [1]

The total data factor of path two (Wp2) is

Dp2=Sum (D1, D4, D6) ———————- [2]

The total data factor of path three (Wp3) is

Wp3=Sum(D1,D4,D3,D6)———————- [3]

The highest priority of data factor is given by

Nbf = max (Dp1, Dp2, Dp3———Dpn) ———— [4]

Nbf= priority of data factor

IV. REMOTE ROBOTICS NETWORK QUALITY LINK

The link superiority is evaluated among the source and destination IoT devices. The quality of the link depends on the remote IoT device's capacity and the different technologies used by the remote IoT devices.

Case 1: As shown in Figure 3 source IoT device uses the cloud IoT network to communicate with the next IoT device, and the IoT device uses Bluetooth or wifi to communicate the data. As the cloud IoT network has high speed compared to Bluetooth or wifi and cloud IoT network can communicate for long distances and Bluetooth can communicate only for around 30 meters, so when the source IoT device sends data to the next device there will be packet loss due to the congestion in the link. Since the source node has a high speed compared to the IoT device, the source IoT device sends data packets continuously but due to the lower speed of the remote IoT

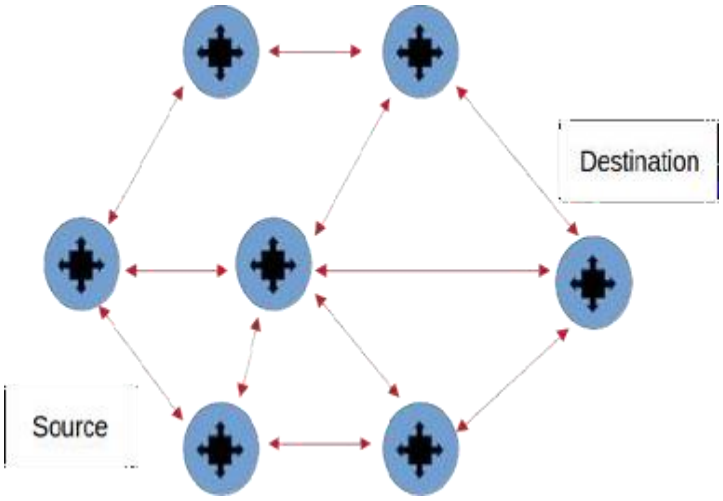


Fig. 2. Cloud IoT device communication

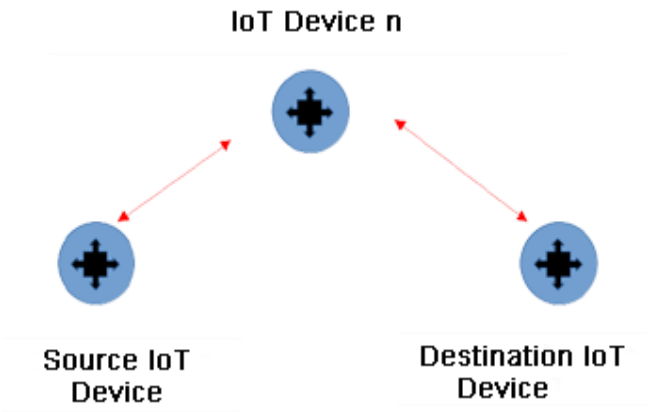


Fig. 3. Cloud IoT device communication Link -Case 1

device it cannot control the traffic and there will be a loss of data in the network.

Case 2: As shown in Figure 4 heterogeneous links connected to the Wi-Fi, and cloud IoT networks. The source IoT device uses Wi-Fi technology to send data and the IoT device uses Bluetooth network to send the data so there will be compatibility in the speed between the Bluetooth and there is no loss of packet in case 2. So the quality of the link is good for remote communication.

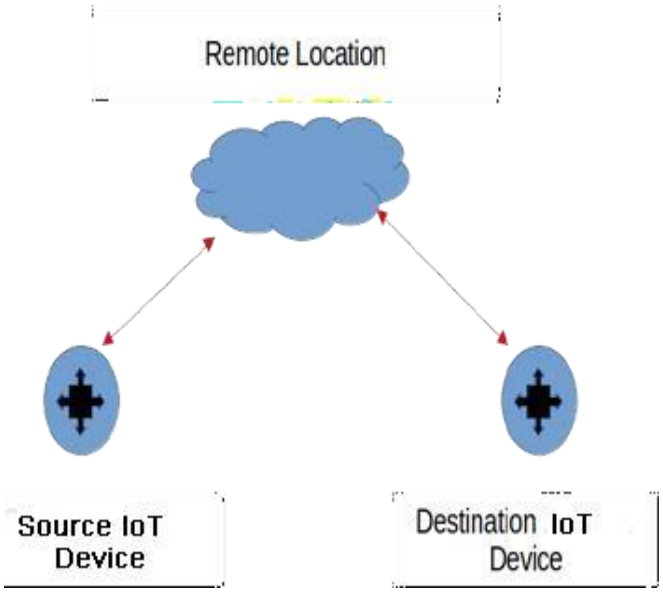


Fig. 4. Cloud IoT device communication Link -Case 2

V. PROPOSED WORK REMOTE DEVICE LOAD BALANCING TECHNIQUE

As shown in figure 5 different cloud IoT devices are deployed randomly over the entire network environment.

In our proposed work the devices we deployed are PCs, IoT mobile device sensor nodes, etc–. Each device in the network has its respective gateways. Cloud robotics networks have the gateway as a base station, a remote location side unit as the gateway for robotics device networks, a sink robotics device for sensor robotics devices, and routers for servers. The devices can also communicate with the gateway of other devices to know the information of the particular device. Each devices in the network are connected and each gateway is connected to the cloud and the cloud in turn connected to the robotics network. The first step is to find the location of the destination robotics device, in this source node finds the location of the destination node. If the destination device exists within the communication range of the source device then it directly finds the location of the destination device. If the destination cloud IoT device is not within the communication range of the source IoT device, then the source IoT device uses the intermediate IoT devices to find the location of the destination device. Source cloud IoT devices communicate with the gateway of that particular destination cloud IoT device, if the destination cloud IoT device is not located in that particular gateway then the gateway of the destination cloud IoT device communicates with the cloud to find the location of the destination cloud IoT device. Cloud has the information on all cloud IoT devices, such as the cloud IoT device ID of every intermediate cloud IoT device Location, cloud IoT device Energy, cloud IoT device Bandwidth, mobility of cloud IoT device, and neighbor cloud IoT device Count.

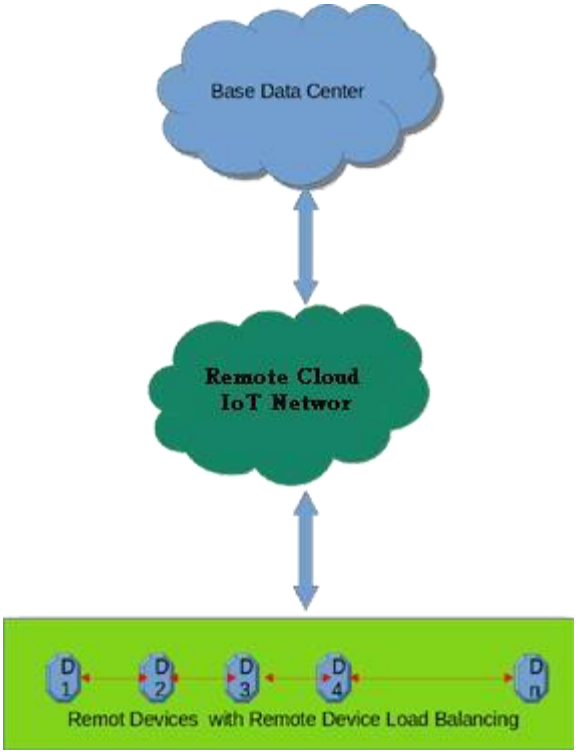


Fig. 5. Proposed block diagram

The cloud IoT base station checks for a particular location of the destination cloud IoT device and it sends it to the source cloud IoT device. Once the location of the destination cloud IoT device is found then the multipath routing is computed between the source and destination cloud IoT device.

VI. CONCLUSION

In this paper, we presented context-aware load balance in cloud IoT. We have proposed remote device load balancing for balancing the load. The path from source to destination is considered based on the type of data and its priority. Based on the time and date the next device is selected and data is passed through it. The technique shows that the proposed work improves packet delivery ratio, response time, load balancing capacity, and less delay compared to existing techniques. The efficiency of the overall network security is also better in all scenarios.

REFERENCES

[1] Dr. Rishi Kumar Sharma,"Identity-Based Remote Device Authentication Low-Cost Model and Performance Evaluation: A P2P Approach",Neuro Quantology, 2022.
[2] Rishi kumar Sharma,"An Approach towards Security in Heritage Cloud Using OTP System", IJARMATE, International, 2016.

[3] Chirag N. Modi, Dhiren R. Patel, Avi Patel, Muttukrishnan RajarajaN, " Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing" Procedia Technology 6 (2012, 2nd International Conference on Communication, Computing Security (ICCCS), 905-912.
[4] Gens. F, "IT Cloud Services User Survey, pt.2: Top Benefits Challenges", 2008, http://BLOGS.IDC.COM/IE/?=210.
[5] D. J. Brown, B. Suckow T. Wang, "A Survey of Intrusion Detection Systems", Technical report Department of Computer Science, University of California, San Diego, 2002.
[6] D. Stiawan, A. H. Abdullah M. Y. Idris, "The Trends of Intrusion Prevention System Network", 2nd International Conference on Education Technology and Computer (ICETC), 2010, Vol. 4 pp. 217–221.
[7] H. Zhengbing, L. Zhitang W. Jumgi, "A Novel Intrusion Detection System (NIDS) Based on Signature Search of Data Mining", in WKDD First International Workshop on Knowledge discovery and Data Mining, 2008, pp. 10–16.
[8] Arshad J, Townend P, Xu J, "A novel intrusion severity analysis approach for Clouds", Future Generation Computer Systems Journal, 2013, vol. 29(1), pp. 416-428.
[9] Grobauer B, Walloschek T, Stocker E, "Understanding cloud computing vulnerabilities", Security Privacy, IEEE 2011, vol. 9(2), pp. 50-57.
[10] Wang C, Q Wang, K Ren, and W Lou, Ensuring data storage security in cloud computing, in 17th International Workshop on Quality of Service, 2009, pp. 1–9.