AWS IOT Platform based Remote Monitoring by using Raspberry Pi

Deepak B. Andore
Balaji Institute of Telecom & Management, Pune, 411033, India

***Abstract* –To cater the needs of industry as well as society, it's the proper time to deploy the IOT based technology to monitor different operations. Automation concept is coming in each and every sector to automate every operation. The leading technology partners such as Amazon, Microsoft & IBM have invented different IOT based platforms to automate the processes as well as operations.Now a day, every industry is trying their best to deploy IOT based services to connect each and every thing. By using AWS IOT platform, it's very easy to interface different gateways such as Raspberry Pi and Arduino board.**

In this paper the Raspberry Pi is connected with AWS IOT platform for remote monitoring of any industrial as well as commercial application. Connections with remote locations can easily achieved by using messaging protocol such as MQTT (Message Queue Telemetry Transport). The publish-subscribe pattern requires a message broker. The broker is responsible for distributing messages to interested clients based on the topic of a message.

Keywords: **AWS, IOT, Raspberry Pi, MQTT**

I. INTRODUCTION

Different devices and instruments can be integrated using IOT and its integrated platform.IOT plays very important role while controlling and monitoring traditional as well as general household objects [1].In recent years, IOT has been attracting the attention of industrialists, researchers as well as government for deploying different services.By using internet, now a day it is possible to control and monitor all the things easily. Different things can communicate with each other, and can even make decisions by themselves with the help of internet [2]. Industry partners such as Amazon, Microsoft and IBM have introduced IOT based platforms such as AWS (Amazon Web Services) IOT, Microsoft Azure, and IBMBluemix Watson for effectively monitoring the remote applications.

As per the ABI Research [3], in 2014 wireless connected devices will increase to 16 billion, about 20% more than in 2013. According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020[4].The IoT allows objects to be sensed or controlled remotely across existing network infrastructure,creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. With the help of sensors, environmental monitoringapplications can be achieved such as environmentalprotection [5] by monitoring air or water quality [6], soil conditions [7], movements of wildlife and habitats can be monitored. Urban and rural infrastructures related operations like bridges, railway tracks; on- and offshore-wind-farms can easily monitored as well as controlled using IOT [8]. IOT plays a key role in industrial applications and smart manufacturing like network control and management of manufacturing equipment, asset and situation management, or manufacturing process control.

In this paper, Raspberry Pi is used as gateway for remote monitoring purpose. Depending on the requirement any sensor can be interfaced with Raspberry pi for controlling the application. Gateway is synchronized with AWS (Amazon Web Services) IOT platform.MQTT acts as a messaging protocol for remote connections to distribute messages towards interested clients.

The organization of the paper is as follows. In section 2 the relevant work on remote monitoring is reviewed to study the role of AWS IOT platform. The section 3 defines proposed model of remote monitoring. The section 4 defines design and implementation approach for proposed model. In final section 5, the work is concluded with future scope.

II. BACKGROUND ANDRELATED WORK

The study of the relevant article available in literature reveals that most of the remote monitoring systems are designed using Arduino board and different electronics sensors for home automation and health monitoring. Very few were tried to develop remote monitoring systems using AWS IOT platform and Raspberry Pi. The IOT based available remote monitoring systems are briefly discussed in following section.

A. IOT architecture

Many IOT- based healthcare applications [9], [10], [11] were introduced in the last decade. Most of the researchers worked

on IOT implementations by taking the help of reference model. According to the different articles, there are three different key aspects that play very important role in IOT implementation: network, cloud and data. Each aspect can be designed by using different blocks, and each building block having correlation with one or more blocks. All the three aspects having very strong relation with each other and able to influence different IOT applications.

B. Prerequisites for IOT Communication

The future is coming fast, connectivity is a commodity, and IOT is steadily taking shape, growing in popularity, and becoming a reality. So for IOT to truly become the next thing with all devices and users connected in and out of the home, we must take a look at the cost of connection, device type, and privacy. There are many network communication protocols which get operated at application layer for IOT devices such as MQTT [12] or CoAP [14], HTTP [13].

Depending on the application each and every protocol having its own advantage. After doing comparative analysis [15] researchers found that, MQTT is basically used in applications which demands QoS at different levels and multicasting of messages towards interested clients. CoAP is the best option to satisfy bandwidth requirement and round trip time (RTT). The future is changing drastically, and connectivity is acting like a commodity, and IOT is becoming a reality. The cost of connection, device type, and privacy plays very important role while deploying IOT concept for industry and commercial applications. To a large degree manufacturing organizations hereby become service organizations and end-to-end transparency is crucial. The insights gained with an integrated IoT approach from the customer side are also crucial and enable to offer better products, quality and services. And this brings us to the key role of data, in the end the major component needed to derive any form of value from sensors, IoT-enabled devices and other 'things', also in manufacturing.

III. DESIGN AND IMPLEMENTATION

In order to realize a remote monitoring system, the paper proposed an architecture which consists of AWS IOT platform and hardware components as shown in figure 1.

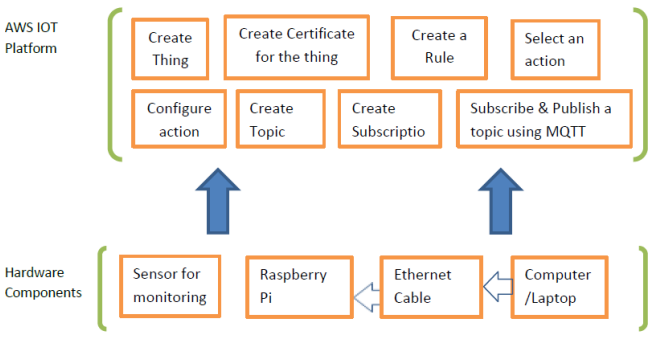

Fig. 1 Proposed System Architecture

The **AWS IOT platform** act like a cloud server for exchanging the information in between end user and system. AWS cloud server provides the facility of interfacing any gateway device such as Raspberry Pi, and Arduino board for controlling any application.

A thing is created on AWS cloud server for establishing communication in between Raspberry Pi and server. For authentication purpose a certificate has to be created for that thing. Depending on the requirement a rule is created to evaluate messages sent by the thing and specify what to do when a message is received. An action is selected and configured for sending notifications towards a client related to messages. For publishing messages a topic has to be created. Subscription is created for a topic in which communication protocol as well as end point of the respective client is defined. After creating the subscription, messages can be easily sent towards a particular client. By using MQTT broker a topic can be subscribed as well as published for sending different messages.

The **hardware components** includes gateway device as Raspberry Pi, Ethernet cable, computer/laptop, and different types of sensors for monitoring. Raspberry pi is connected with computer/laptop using Ethernet cable. A USB cable is used to power on the Raspberry Pi device. As per the application requirement, a sensor is interfaced with Raspberry Pi device for remote monitoring purpose.

Raspberry Pi device is programmed for pushing the data over the AWS cloud server.

Proposed system is implemented successfully by integrating AWS cloud server and Raspberry Pi device which is as shown in figure 2 and figure 3. As a prototype for remote monitoring, a IR sensor is connected to Raspberry Pi device.

For interfacing Raspberry Pi with AWS cloud server a thing is created on server which is as shown in figure 3.

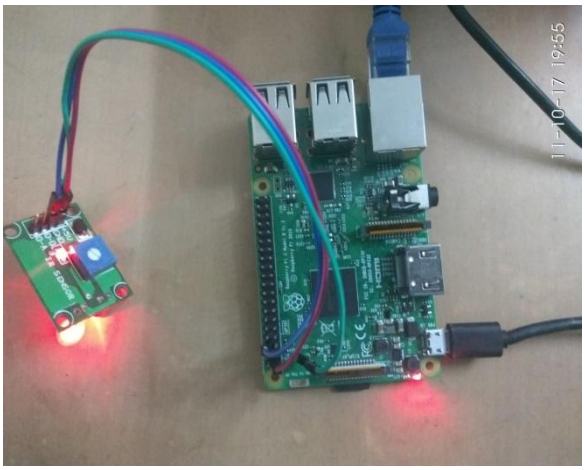

Fig. 2 Prototype for implementation

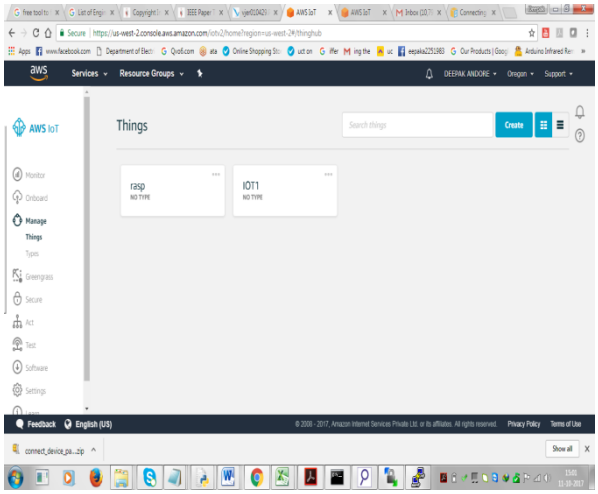

Fig. 3 Creating a thing on AWS cloud server

Stepwise procedure for creating certificate, rule, topic and subscription is as shown in following figures

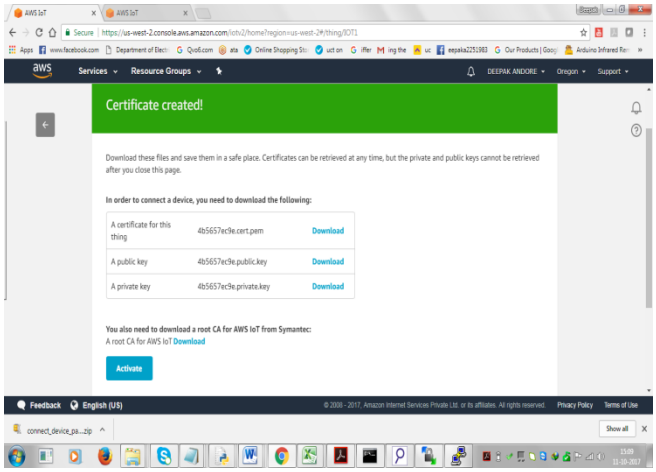

Fig. 4 Create certificate to connect a device

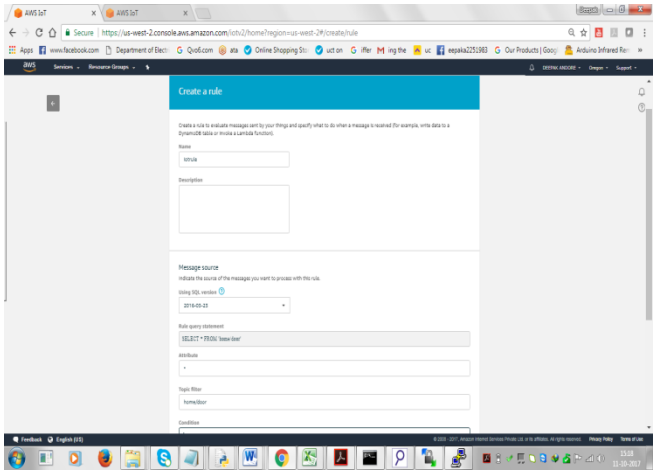

Fig. 5 Create a Rule

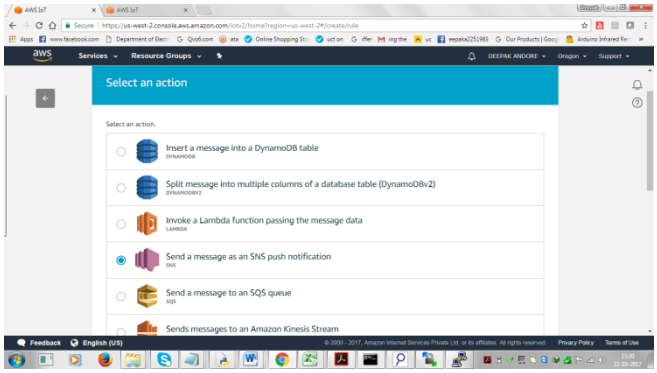

Fig. 6 Select an Action

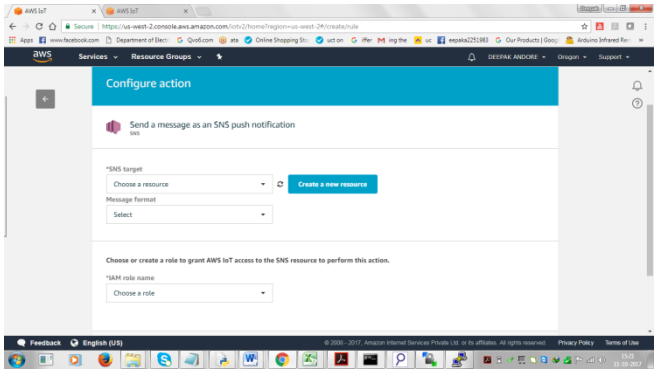

Fig. 7 Configure an Action

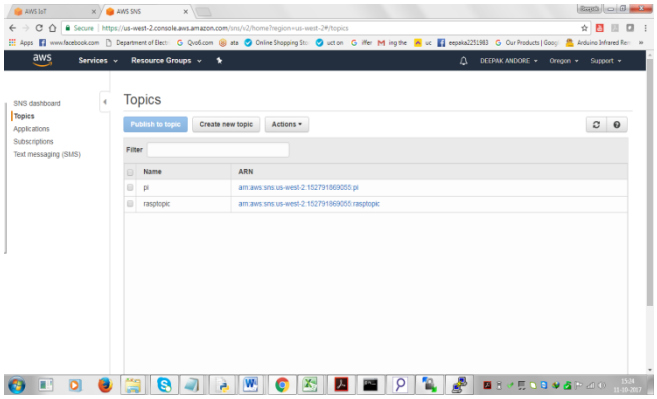

Fig. 8 Topics window

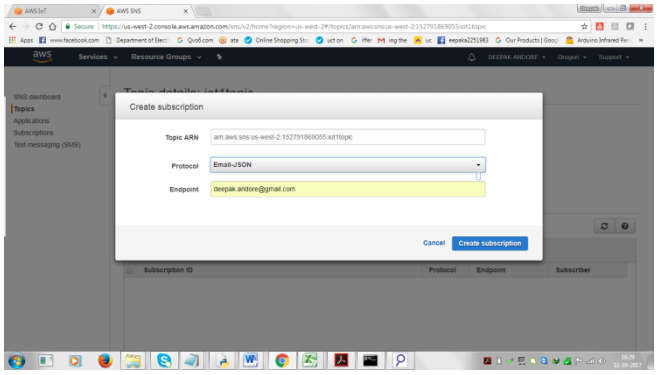

Fig. 10 Create Subscription

3.1 Programming Raspberry Pi

After interfacing IR sensor with Raspberry Pi device next step is to programme Raspberry Pi device with Putty as a software terminal. Following is the sample program loaded to Raspberry Pi device for fetching the sensor data and transferring it to computer/laptop.

```
import time
import paho.mqtt.client as mqtt
import ssl
importjson
import thread
importRPi.GPIO as GPIO
GPIO.setmode(GPIO.BCM)
GPIO.setup(21, GPIO.OUT)
defon_connect(client, userdata, flags, rc):
print("Connected with result code "+str(rc))
client = mqtt.Client()
client.on_connect = on_connect
client.tls_set(ca_certs='./certs/rootCA.pem',
certfile='./certs/rasp.cert.pem',
keyfile='./certs/rasp.private.key',
tls_version=ssl.PROTOCOL_SSLv23)
client.tls_insecure_set(True)
client.connect("a39vxay4763yi7.iot.us-west-
2.amazonaws.com", 8883, 60) #Taken from REST API
endpoint - Use your own.
defintrusionDetector(Dummy):
   while (1):
         x=GPIO.input(21)
if (x==0):
print "Just Awesome"
client.publish("home/door",
payload="Intruder Detected" , qos=0, retain=False)
time.sleep(1)
thread.start_new_thread(intrusionDetector,("Create intrusion
Thread",))
client.loop_forever()
```

IV. RESULTS

The implemented prototype is designed to achieve a security application which can be implemented for any house or office. If any unauthorized person try to enter into the house or office premises, then it can be easily detected by the designed system and a message get forwarded to the respective client using AWS cloud server. For remotely monitoring the designed application we can effectively use AWS IOT platform as shown infigure11.

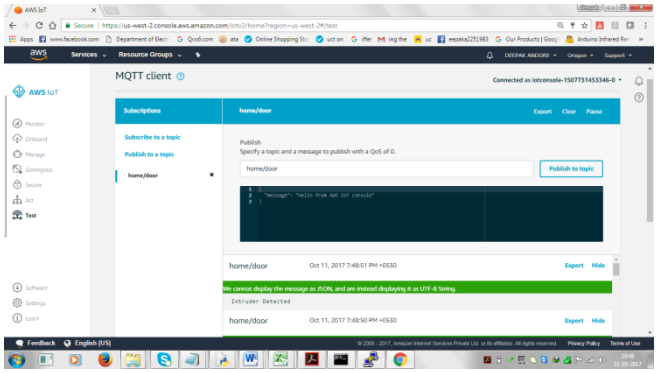

Fig. 11 Subscribing and Publishing a topic using MQTT client

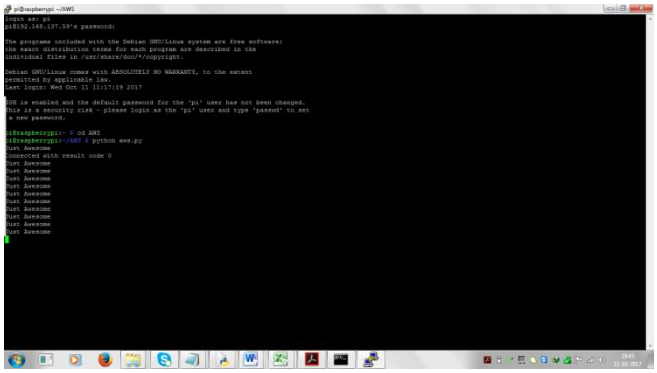

Fig. 12 Output on Raspberry Pi terminal

V. CONCLUSION

AWS IOT platform plays very important role in designing remote monitoring applications which can be used in various aspects such as security, identification authorization.

The designed system is very economic and effective for monitoring any commercial as well as industrial application. By subscribing and publishing the topics, any notification related to remote monitoring can be sent automatically towards respective client. So, the designed smart sensing module is reliable and robust to work under any condition.

REFERENCES

[1]. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges,” WirelessNetworks, vol. 20, no. 8, pp. 2481–2501, 2014.
[2]. C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, “Future internet of things: open issues and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2201–2217, 2014.
[3]. ABI Research. 9 May 2013
[4]. Gartner. 10 November 2015. Retrieved 21 April 2016
[5]. Davies, Nicola. "How the Internet of Things will enable 'smart buildings'". Extreme Tech.
[6]. "Molluscan eye". Retrieved 26 June 2015
[7]. Li, Shixing; Wang, Hong; Xu, Tao; Zhou, Guiping (2011. “Application study on Internet of Things in Enviornment Protection Field”. Lecture Notes in Electrical Engineering Volume. Lecture Notes in Electrical Engineering. **133**: 99–

106. ISBN 978-3-642-25991-3. doi:10.1007/978-3-642-25992-0_13

[8]. Gubbi, Jayavardhana; Buyya, Rajkumar; Marusic, Slaven; Palaniswami, Marimuthu (24 February 2013). "Internet of Things (IoT): A vision, architectural elements, and future directions". Future Generation Computer Systems.

[9]. V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative internet of things (IoT) for rural healthcare monitoring and control," in Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE), Second International Conference on. IEEE, 2011, pp. 1–6.

[10]. C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Sixth International Conference on. IEEE, 2012, pp. 922–926.

[11]. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID technology for IoT-based personal healthcare in smart spaces," IEEE Internet of Things Journal, vol. 1, no. 2, pp. 144–152, 2014.

[12]. A. N. Andy Stanford-Clark, "MQTT Version 3.1.1", OASIS Std., October 2014. [Online]. Available: http://docs.oasisopen.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

[13]. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext transfer protocol–http/1.1," 1999.

[14]. Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.

[15]. N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, and G. Reali, "Comparison of two lightweight protocols for smartphone-based sensing," in Communications and Vehicular Technology in the Benelux (SCVT), Twentieth Symposium on. IEEE, 2013, pp. 1–6.