Importance of Sensor Readings and Its Secured Delivery in Internet of Things

Kratika Gupta[1*], Ashwani Kumar[2], Suraj Rasal[3], Varsha S. Rasal[4]

[1]Department of Computer Engineering, Bharati Vidyapeeth Deemed University College of Engineering Pune, India
[2]Tata Consultancy Services, Pune, India
[3*] Department of Computer Engineering, Bharati Vidyapeeth Deemed University College of Engineering Pune, India
[4]Department of Computer Science & Engineering, Nehru College of Engineering &Research Centre, Thrissur, India

[*]Corresponding Author: surasal@bvucoep.edu.in , Tel.: +91-8793000079

Abstract— Internet of things plays a vital role in the human life. Raspberry Pi is one of the widely used IoT based module. IoT includes information delivery as important property aspect. In this paper importance of sensor reading is highlighted. Sensor readings are important values on which further values may depend. Like IoT appliances used in chemical , pharmaceutical or agricultural industries. In such industries, sensor reading values are important. This paper proposed the importance of sensor value delivery and its impact. IoT based water plantation is considered to explain how sensor values are used to perform certain tasks using raspberry pi module.

*Keywords:*IoT,sensor,Raspberrypi,security

I. INTRODUCTION

The popularity of cloud computing and social networking sites has increased at an astounding level. Usefulness of cloud and sites such as Twitter, Facebook et cetera cannot be disputed. A majority of enterprises have moved to cloud and they no longer need to invest in big servers, large infrastructure and IT staff where as social networking is being used for professional networking, job searches, current affairs, connection with friends etc. Security [1][2] has become the key to securing success in today's digital world. The Raspberry Pi is a credit-card-sized computer inspired by 1981 BBC micro. It is a capable little computer with ARM processor and works with many operating system, thus can be used in electronics projects, and for many of the things that your desktop PC does, like spreadsheets, word processing, browsing the internet, and playing games. Raspberry pi is the best epitome for studying embedded system as, embedded system are designed for performing dedicated function with often real time operations. Given the limitations that embedded system do not possess their own operating system, they also need a programmed ARM assembly for programs hence we can compiling our assembly into our own kernel that the Pi will boot . To accomplish this, we will end up stripping all the data off the Pi's SD card to load our kernel onto it. Typically, a kernel acts as a bridge between hardware and software. The Raspbian kernel makes it easy for us to grab data from the keyboard or monitor and manipulate it. Hence, pi and embedded system can be easily used to achieve any functionality. Raspberry Pi can be accessed from anywhere around the world, which questions the security of Pi. PORT FORWARDING is one method where we forward all inbound traffic from the internet on a specific port to the local IP address of your Raspberry Pi. the disadvantage of port forwarding is that it exposes a network port on your private LAN to the public internet. This is known security vulnerability. There are number of sites like yaler.net, dataplicity, losant remote iot which can help access raspberry pi after gaining its ip address, which is easy to get. Also services like: SSH on port 22 – You can login to your Pi from anywhere over SSH. Web (http) on port 80 – You can view a web page your Raspberry Pi serves from anywhere Web IOPI on port 8000 – Control your Raspberry Pi GPIO pins using their custom software.

II. SOCIAL NETWORKS WITH CLOUD

Cloud is a network of networks over the Internet which provides scalable, reliable, expeditious and cost-effective IT resources. Thus, cloud computing is a form of Internet-based

computing that provides computing services like servers, databases, networking, storage etc. over the Internet, also known as the cloud [3]. These services are charged as per the usage . Companies providing these services are called cloud provider. Typically, there are 3 types of cloud services which are being used:

A.   Types of Cloud Services

1)   Infrastructure-as-a-service (IaaS)
It is the most basic type of cloud service. It allow a consumer to hire IT infrastructure related services like servers, storage, network, virtual machines, operating systems, data center space etc. from a cloud provider on a pay as per consumption basis.

2)   Platform-as-a-service (PaaS)
It provides a consumer an environment consisting of application development environment and tools like programming languages, libraries, services, software, hardware etc. Thus, saving the consumer from the underlying cost and intricacies of purchasing and managing the infrastructure required to develop and support an application.

3)   Software-as-a-service (SaaS)
It is a software delivery model which allows a consumer to code, deploy and run their application over the Internet. The cloud provider takes care of the hosting, managing and maintaining of the underlying software and infrastructure.

B.   Relation between cloud and social networking
Social network is one of the most burgeoning areas in today's IT world. The data in social media is increasing at a huge rate so internet usability can be bolstered by storing heavy multimedia content in cloud storage system. As social media sites have large number of users present across the world, this makes them ideal for cloud adaption. Big data analytics can also be applied to social media for performing trend analysis, decision making etc. Furthermore, cloud computing [3] can be beneficial as it minimizes the cost of data backup and recovery in case of a disaster.

C.   Security in cloud
Cloud security falls into two broad categories: security at cloud providers' end and security at consumers' end. The cloud providers need to ensure that their infrastructure, software and platform is secure so that consumers' data and application is protected while consumers, on the other hand, must take necessary steps to protect their application and use robust passwords and authentication measures [4]. Key areas in cloud computing and the associated security mechanisms used in them –
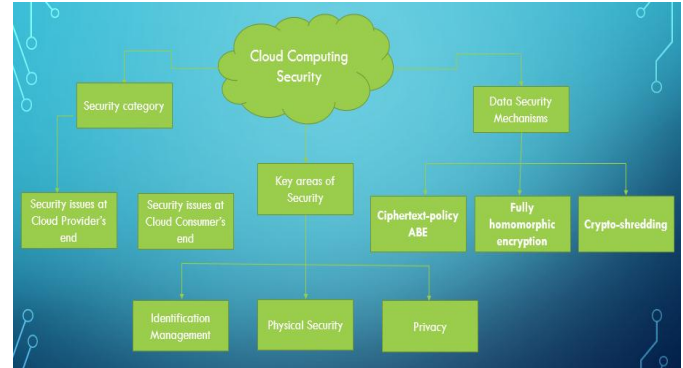

Figure 1:

1)   Identity management – Every enterprise has its own Identity management system for controlling access to information and resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, a biometric-based identification system for example, or provide an identity management system of their own. CloudID, for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification. It links the confidential information of the users to their biometrics and stores it in a searchable encrypted form.

2)   Physical security – Cloud service providers physically ensure securing of IT hardware from unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption by using top-notch data centers.

3)   Privacy – Cloud provider ensure that all the critical data is encrypted and only the authorized users have access to data.

D)   Encryption mechanisms used for securing cloud data –

1)   Ciphertext-policy ABE (CP-ABE) – It's an attribute-based encryption algorithm that uses attributes as the public key and associates the cipher text and user's secret key with attributes, so that it can support expressive access control policies [5][6][7]. This reduces the cost of network

bandwidth and sending node's operation in fine-grained access control of data sharing [8] [9][10][12].

2) Fully homomorphic encryption (FHE) – It is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

Crypto-shredding- It is a mechanism of deleting the data, which is in encrypted form, by deliberately deleting or overwriting the encryption keys. Disposing the data, which is no longer required, can be challenging when confidentiality of the data is of paramount importance. Crypto-shredding ensures smooth disposal of data when data is not required.

III. EXISTING EMBEDDED APPROACH WITH SOCIAL NETWORKING

A) Implemented work

In this experiment, temperature of some material will be displayed with a DS18B20 digital temperature sensor connected to the GPIO pins of a Raspberry Pi. In this article we will take things one step further, automatically publishing the temperature at regular intervals to Twitter so that they can be viewed from anywhere in the world. Hence, we need create a new Twitter account, create a Twitter application via Twitter Application Management, and add a new Python package called tweepy which enables Raspberry Pi (or other Linux computer) to Tweet. Setting up the Twitter Application First goes to Twitter.com and create your account. Next is click to go to Twitter Application Management, and click to Create New App.

Figure 2:

Then you need to fill in the website associated with the application. If you do not have a website, then type anything

Lastly you can fill in a callback URL, but this can just be left blank. After agreeing to the terms and conditions, click the button to Create Your Twitter Application.

Figure 3 :

Clicks modify app permissions and then select Read and Write from the displayed options. Click on Update Settings to save the changes. Now click on Keys and access token. Your API key and API secret tokens will be displayed as well as some other information. Scroll down and click on the Create my access token. After a few seconds (you may need to refresh your browser), these tokens will also be displayed. So, you now have the four tokens required to enable the Python script you will write on your Raspberry Pi to send tweets to your new Twitter account – API key, API secret, Access token, and Access token secret.

1) Raspberry Pi – Python, and Twitter

Do the sudo apt-get update and sudo apt-get upgrade commands on your Raspberry Pi to make sure everything is up to date. Next enter the following commands to add the Python package tweepy.
sudo apt-get install python-setuptools
sudo easy_install pip
sudo pip install tweepy
In order to test that everything is working as it should, type python at the command prompt. Then when Python runs, type import tweepy. If that does not lead to any error messages, then the tweepy Python package has been successfully installed. (enter exit() to quit Python.)

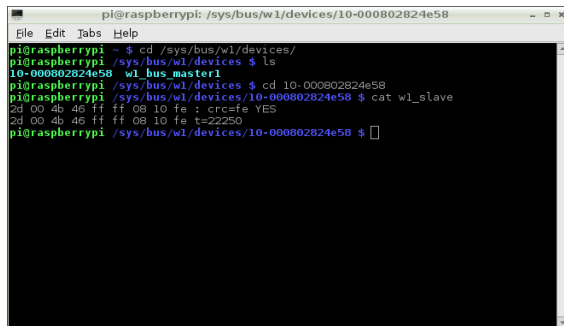**Figure 4:**

Reading the Sensor from the Terminal
Turn on the Pi.

Once a user is logged on to the Pi, type these commands into a terminal, or just at the prompt given upon login and beforetyping"startx":

sudo modprobe w1-gpio
sudo modprobe w1-therm
cd /sys/bus/w1/devices/
ls

The entry on the screen that is mostly numbers is the serial number of the sensor. The sensor used here has the serial number "10-000802824e58". Replace the serial number in the next command with the one for the sensor used.
cd10-000802824e58
cat w1_slave

Two lines of text will be printed. On the second line, the section starting "t=" is the temperature in degrees Celsius. A decimal point goes after the first two digits, so the example value of "t=22250" is in fact "t=22.250" degrees Celsius:

Figure 5:

we can now write the Python script which will read in the temperature from our DS18B20 sensor and send it to Twitter nano DemoTweet.py to create a Python file called DemoTweet.py.
The following code helps to link our twitter application to the raspberry pi:

```
#! /usr/bin/env python
import tweepy
from datetime import datetime
API_KEY = 'YOUR API KEY'
API_SECRET = 'YOUR API SECRET'
ACCESS_TOKEN = 'YOUR ACCESS TOKEN'
ACCESS_TOKEN_SECRET = 'YOUR ACCESS TOKEN SECRET'
Auth=tweepy.OAuthHandler(API_KEY,API_SECRET)auth.set_access_token(ACCESS_TOKEN,ACCESS_TOKEN_SECRET)
api = tweepy.API(auth)
tempfile=open("/sys/bus/w1/devices/2800000XXXXXX/w_slave")
thetext = tempfile.read()
tempfile.close()
tempdata = thetext.split("\n")[1].split(" ")[9]
```

```
temperature = float(tempdata[2:])
temperature = str(temperature / 1000)
thetime = datetime.now().strftime('%-I:%M%P on %d-%m-%Y')api.update_status(temperature + " C at " + thetime)
```

Here 28-00000xxxxx is the address of the temperature sensor

Save the script and now we can test that everything is working as it should. Enter the command:
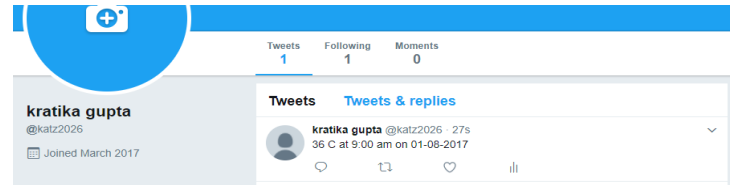sudo python DemoTweet.py

Figure 6

Finally we need to automate this whole process so that the temperature of our sensor will be sent to Twitter at regular intervals. The easiest way to achieve this is with cron, a software utility included with all linux distributions which will automatically run jobs at certain times of day or at certain time intervals.
At the command prompt enter:
sudo crontab -e
 Scroll down to the bottom of the cron file and enter the following after the last line and save the file:
*/80 * * * * python /home/pi/DemoTweet.py
This will automatically run the temperature reading Python script REUK-Tweet.py on the hour every hour.
This is how the hourly tweet can notify the plant owner about the temperature of the soil, so that he can monitor the watering of plants. Here humidity temperature can also be added in the same way as the temperature sensor.

B) Other appliances

1) Get International Space Station Alerts
To get the location of International Space Station at any time or any day, this Raspberry Pi Twitter bot project uses an RSS feed generated by Nasa's ISS spotting web page to predict when the space station will be visible from your part of the world, and send a tweet the day before, so everyone who is interested in looking to the skies will be able to get ready for some astro observation.

2) *Get Earthquake Warning Tweets*

Many lives were saved during Japan's devastating earthquake and tsunami in March of this year by the country's earthquake warning system, which sent messages to mobile

phones in time for people to prepare for the temblor. The USA does not have that system a series of Twitter feeds that automatically tweet earthquakes in areas such as San Francisco and Los Angeles.

3) Home automation

People can now get the information of ON fans or light or electric geyser on their tweeter account. With the number of user increasingly using twitter we can help apply this system at homes to save money and electricity.

4) Smart agriculture:

The idea of planting can be extended to smart agriculture where the plants and crops can be monitored with simple twitter notification. The automatic motor ON and OFF function can be collaborated so that farmer would not have to manually monitor anything.

IV.   PROPOSED RESEARCH APPROACH

Proposed approach is defined to highlight the importance of sensor reading values. In this paper, work shows that how water plantation can be improved using raspberry pi based IoT [13][14[15]. Based on sensor reading value, further process starts. Means on first sensor reading value further step depends. Like in chemical industry, based on the first sensor reading value, the proportion of chemical is finalized basis of which its quantity is finalized. Its first sensor value may be temperature or thickness of solution or density of color of solution and so on. Based on such a sensor reading value, next process depends. It may be mixing some solution or boiling some solution. In similar way in agricultural area, based on sensor readings, water usage may be dependent. So based on sensor reading, ON/OFF status may be dependent or the quantity required may be dependent. Hence sensor reading values should be verified or checked once before applying to existence. Its delivery should be secured enough to enhance its accuracy level. If its value is changed for some hazardous intention then its impact will be more dangerous in further stages. Hence in such a cases, high secured medium should be established to deliver the sensor values securely.

V.   CONCLUSION

IoT information delivery is important aspect in latest trend. Its transport methods should be secured enough to deliver sensor readings. Embedded approach is incorporated with computing which can be concluded that its working may be related to some hardware or physical model. Malfunction in its working may impact negatively on human life. Sensor reading value matters in computing approach. Sensor values should be delivered safely. Sensor readings delivery should be delivered through secured medium. Also, sensor reading values should be applied after verifying its accuracy and correctness.

REFERENCES

[1]   Zhang, Zhi-Kai, et al. [2014] IoT security: ongoing challenges and research opportunities. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. IEEE

[2]   Jing, Qi, et al. [2014] Security of the internet of things: Perspectives and challenges, Wireless Networks 20.8 Springer : 2481-2501.

[3]   VS. Rasal, SU. Rasal, ST. Shelar "A Cryptographicaly Imposed DCP-ABE-M Scheme with Attribute Based Proxy Re-Encryption and Keyword Search in Untrusted Public Cloud", The IIOAB Journal, Vol.8, Issue.2, pp.21-26, Feb 2017

[4]   VT. Mulik, K. Saritha, SU. Rasal, "Privacy Preserving Through Mediator in Decentralized Ciphertext policy Attribute Based Encryption", IJRET: International Journal of Research in Engineering and Technology, Vol.5, Issue.6, pp. 535-540, 2016

[5]   Stallings, William. [2006] Cryptography and network security: principles and practices. Pearson Education India.

[6]   SU. Rasal , R. Redhu , VS. Rasal , ST. Shelar "Improving Source Code Encryption using Proposed Cipher Logic",   IJCSE: International Journal of Computer Sciences and Engineering, Vol.5(4), Apr 2017, E-ISSN: 2347-2693.

[7]   Suraj U. Rasal , Raghav Agarwal , Varsha S Rasal , Shraddha T. Shelar, "IOT Appliance Access Structure using ABE Based OTP Technique" The IIOAB Journal, Vol. 7 , Suppl 1, 180–186 , Sept 2016

[8]   Yao Xuanxia, Zhi Chen, and Ye Tian. [2015] A lightweight attribute-based encryption scheme for the Internet of Things." Future Generation Computer Systems 49 Elsevier: 104-112.

[9]   Touati, Lyes, Yacine Challal, and Abdelmadjid Bouabdallah. [2014] C-cp-abe: Cooperative ciphertext policy attributebased encryption for the internet of things, Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on. IEEE.

[10]   SU. Rasal, ST. Shelar, VS. Rasal, "Securing Internet Banking Using Multiple Attributes Scheme And OTP", The IIOAB Journal, Vol.7, Issue.10, pp.26-30, 2016.

[11]   S. Rasal, S. Relan, K. Saxena, "OTP Processing using UABE & DABE with Session management", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.6, Issue.5, pp.57-59, 2016.

[12]   VS. Rasal, SU. Rasal, AK. Joseph, NK. Joseph "Amelioration of Decentralized Cipher Text Policy Attribute Based Encryption with Mediator technique by adding Salt"; IJARCS: International Journal of Advanced Research in Computer Science, Volume 8, Issue. 5, PP. 1709-1713, May – June 2017

[13] Suo, Hui, et al. [2012] Security in the internet of things: a review, Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. IEEE Vol. 3.

[14]   Sicari Sabrina et al. [2015] Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 Elsevier 146-164.

[15] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. [2013] On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57.10 Elsevier: 2266-2279.

Authors Profile

Ms. K. Gupta pursed Bachelor of technology from Bharati Vidhyapeeth College of Engineering, Pune in 2017. She will be joing TCS as Assistant system trainee from month of december. She has published 3 research papers in reputed international Journals. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education.

Mr A. Kumar pursed Bachelor of technology from Bharati Vidhyapeeth College of Engineering, Pune in 2014. He is currently working as System Engineering in TCS. His main research work focuses on Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 3 years of professional experience.

Mr. Suraj U. Rasal pursed Master of Science in Computer Science from University of Bedfordshire, England and Bachelor of Engineering degree in Information Technology from University of Mumbai. Now he is working as Assistant Professor at Bharati Vidyapeeth University College of Engineering Pune. He has published seventeen research papers since doing research work. He is also working as a reviewer for some Scopus indexing journals. For more info Google scholar link: https://scholar.google.co.in/citations?user=nTZcfh8AAAAJ&hl=en

Mrs.Varsha S. Rasal received the Bachelor of Engineering degree from Anna Univeristy,Tamilnadu,India in Computer Science and Engineering and Masters in Computer science and Engineering from Calicut University, Kerala, India. She has published thirteen research papers in international journals and conferences in the same domain since doing research work.