IoT based Smart Home using Hardware Security

Nagachethana V
Student, IV SEM
M.Tech, DECS
PESU
Bangalore, India

Rajeshwari B
Associate Professor
Department of ECE
PESIT
Bangalore, India

Abstract: **The Internet of Things (IoT) deals with the interaction and cooperation among smart objects surrounding us (such as home appliances, mobile devices). IoT comprises of interconnected smart objects with access to the Internet, provided by networking technologies. The pervasive presence of these devices and their connectivity requirements generate very large amounts of data transmissions, which require guarantees of confidentiality, integrity, authenticity and reliability.**

The objective of this project is to offer a Smart Home providing additional security through hardware generated key (Unique ID). An attempt to address few of the security issues by making use of hardware is highlighted in this work. The application is hosted on the global server to make it work globally. The sensor data's are stored on cloud, which can be viewed from anywhere anytime. These data's can also be saved onto Excel sheet. Two levels of security are included through login. The first level login is through software security. But, the second level login to homepage is through hardware generated key. E-mail notification for successful login and also for access denial is included. Thus, the system provides hardware security for IoT smart home and this prototype implementation can be further extended to other applications of IoT as well.

Keywords- Internet of Things (IoT), Wi-Fi module, global server, Hardware security

I. INTRODUCTION

Internet is not just a platform for humans to communicate with one another, it is also a platform for the devices around us to talk to each other, talk to us by working according to the command given and send the data as required by the user. All these things are now possible with the concept of Internet of Things (IoT), i.e., all the devices are connected to internet and these devices can talk to cloud. Smart health, Smart city, Industrial automation and Smart home are a few applications of IoT. The main challenges of IoT are: Data in cloud, mobility, etc. Smart home makes life easier and an intelligent home by itself makes life simple, but security is the main issue when it comes to IoT application. The login credential gets stored in the database and it is possible to hack the entries made in the database, i.e., the data in cloud. Due to the sheer volume of data in cloud, software security cannot be relied upon and there has to be a co-operation between software and hardware security and thus security based on hardware is necessary. *Shane dyer-Founder of IOT platform, Arrayent*, quoted that: “Hardware based security is necessary because of sheer volume of data within IoT”. *Diana Stapley-Enterprise Tech*, quoted that: “IoT faces four main challenges and they are: Mobility, Data in cloud, Consumerisation of IT and Advanced, persistent threat. Thus, security cannot rely on just software. There needs to be co-operation between hardware and software”.

II. RELATED WORK

[1] In this paper, author has proposed home monitoring and control system using an embedded web-server based on arduino Ethernet. An android based smart phone app is developed in JAVA programming language to control and remotely access the devices and appliances. The connection between home server and appliances is wired-Ethernet. The Ethernet module establishes connection with LAN using a static IP address.

[2] This paper deals with distributed home automation system. It consists of server and sensors. Various sensors are controlled and monitored by the server. The system is accessible remotely from any PC/mobile handheld devices connected to internet through server real IP or from web-browser of any local PC in same LAN using server IP. All the sensor data are sent to the web-browser and is stored in cloud.

[3] The authors of this paper have proposed a home automation scheme to distantly control domestic objects and measure the electrical parameters. This system assists the inhabitants to avoid multiple systems to monitor their domestic utilization. The system can be run with the help of inhabitant laptop/i-pad devices. Zigbee communication is used to remotely measure and control the domestic devices. This is achieved by integrating WSN zigbee network with an internet gateway.

[4] The authors of this paper have designed and implemented a Wi-Fi based IOT smart home system. To enable secure communication between IOT devices, a gateway is used. It also allows the user to configure, access and control the system through user friendly interface running on mobile. Public key mutual authentication protocol is used, with pre-shared keys between a gateway and a new device for authentication. This protocol uses elliptic curve cryptography.

III. SYSTEM ANALYSIS

A. Problem Definition

Design and development of secured smart home using hardware generated unique ID to control the devices and monitor the sensor outputs. Sensor data's are stored in the database, which can be viewed and saved onto Excel sheet and the devices can be controlled anytime, anywhere.

B. Proposed System Feature

The proposed system monitors the sensor data and controls the devices at home using the concept of IoT. An attempt to security based on hardware is made, in order to avoid the login credentials being hacked. A hardware module is used, which generates the key (unique ID). This ID is given to the user for login. When the user enters the given ID, it flows from website to the controller through Wi-Fi module. The controller then asks for the ID (key) from hardware module. Only if the user entered ID and hardware module generated ID matches, access is given. After successful login, the user can control the devices and also view the sensor data sent from controller. If required, the user can also save the sensor data's by downloading onto Excel sheet. For every successful login, an E-mail is sent to the user. After three wrong trials of login, the account is locked and the access is withheld. An E-mail about access denial is sent to the user. The locked account is released only after admin resets it. The admin has a separate login page with separate login credentials and only the admin has the right to reset the account when it is locked and also clear the data logging when not required by the user. Thus, there is no involvement of database to store the login credentials as it is stored in the hardware module itself. An additional layer is added to software security through hardware for better security providing a better, secure home.

IV. SYSTEM DESIGN AND IMPLEMENTATION

A. Proposed smart home using security through hardware

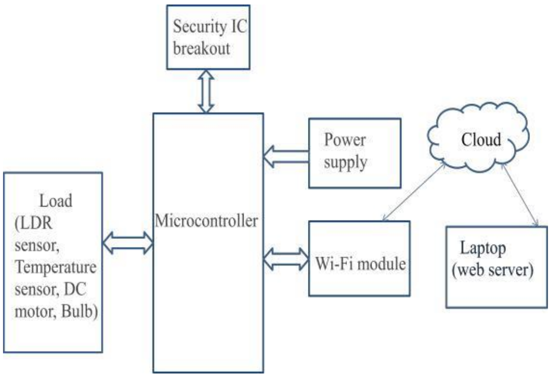


Figure 1: Proposed model of smart home using security through hardware

The proposed model of smart home using security through hardware is as shown in figure1. The controller controls the devices which are connected to it. The controller receives the commands sent by the user and acts according to the command. Any number of devices connected to the controller can be monitored. A Wi-Fi module is connected to microcontroller through UART protocol which wirelessly transmits and receives data and sends it to microcontroller as well as server when required. ESP8266 is the Wi-Fi module used. Security module IC breakout is used which provides additional security to software through hardware. DS28CM00 is the heart of the breakout. It generates a key (unique ID) which is then given to the user. The user enters this ID and only if the ID matches with security module generated ID, the access is given to the user to control or monitor his house. The ID used by the user resides in the hardware and cannot be hacked. The data sent by controller gets stored in the database and whenever the user wants the data, at that time the data can be retrieved. At the same time the user can even control the home appliances. All this can be done remotely from the web-browser through server IP. This design consists of two parts: 1) Arduino web client application which reads the sensor values and sends them to the web-server. 2) PHP application which handles POST and GET requests which are sent to server and it serves the pages to the client who asks for it. PHP uses JavaScript frame work to show the values stored in the database and it also allows to retrieve the readings of past days stored in the database. These records can also be saved onto Excel sheet. It also supports mail transfer with the send mail configuration using SMTP. The interaction between the controller setup and the server and also between webpage to server is using HTTP protocol.

B. Software design

Front End Design:

HTML stands for Hyper Text Markup Language. HTML is a format that tells a computer how to display a web page. HTML file is a text file containing small markup tags. The documents themselves are plain text files with special "tags" or codes that a web browser uses to interpret and display information on your computer screen. The markup tags tell the Web browser how to display the page.

Cloud storage:

Cloud storage is the practice of using remote servers on the internet to manage and store data instead of using a personal computer. Hostinger is an application platform which allows the developers to host their account in the global server. Domain name along with server space is taken and the application is hosted, to make it work anywhere anytime. The domain name is 'smarterhome.tk'.

C. Implementation Setup

Software security is one in which the authentication credentials are verified in the database itself and credentials stored in database can be hacked. In order to address this issue, a hardware is used which generates a unique ID and this ID can be used as password. The difference between software and hardware security is as shown in figure 2.

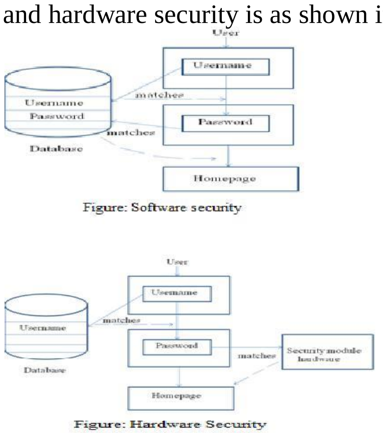


Figure 2: Software & hardware security

The flow diagram of the proposed system is as shown in figure 3. The sequence of activities that take place are the choice of control for bulb, fan and simultaneously to send data to database and the data can be viewed accordingly. The user entered 'username' is verified with the 'username' stored in database. But, the user entered 'password' is verified with the hardware module generated 'password' through Wi-Fi module and then the access is given to homepage.

The process that takes place at after entering the password is:

1) User enters the password.
2) The password is encrypted and flows to controller through Wi-Fi module.
3) At the controller end, password is decrypted.
4) The decrypted password is verified with the security module generated ID.
5) If the ID's match, controller sends a command(YES) to the website through ESP8266 and only after this, the website allows user to enter home page.

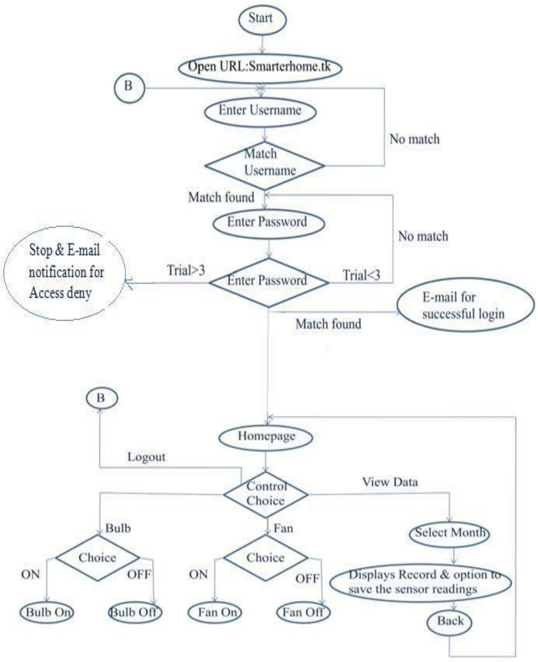


Figure 3: Flow diagram

The experimental setup is as shown in figure 4. The two control devices are: Bulb and fan (motor). Two sensors: LDR sensor and temperature sensors are used. The two sensors send the data for every 60sec and these data's are stored in the cloud. At the same time the devices can also be controlled from anywhere, anytime. This is done by hosting the application on the global server and the process of establishment of connection with global server is as shown in figure 5.

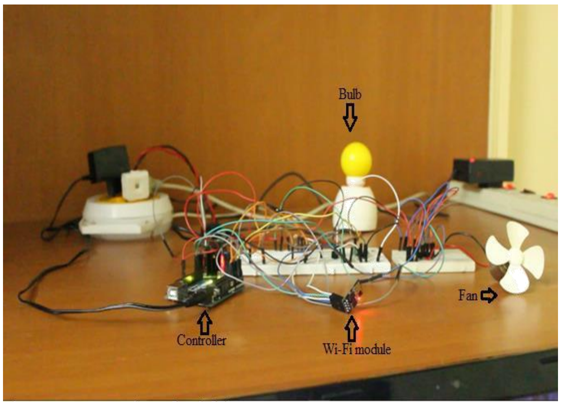


Figure 4: Experimental setup

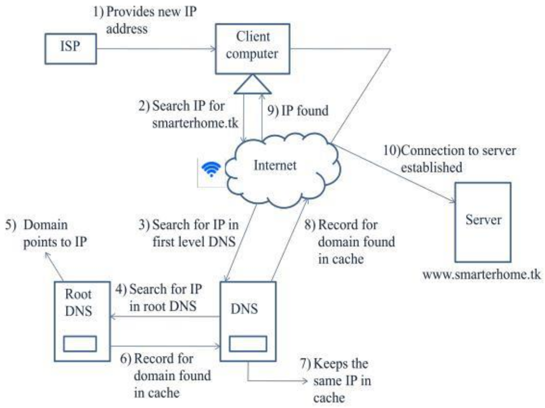

1) Provides new IP address
ISP
Client computer
2) Search IP for smarterhome.tk
9) IP found
Internet
10)Connection to server established
Server
www.smarterhome.tk
5) Domain points to IP
3) Search for IP in first level DNS
8) Record for domain found in cache
Root DNS
4) Search for IP in root DNS
DNS
6) Record for domain found in cache
7) Keeps the same IP in cache

Figure 5: Connection with the global server

V. RESULTS

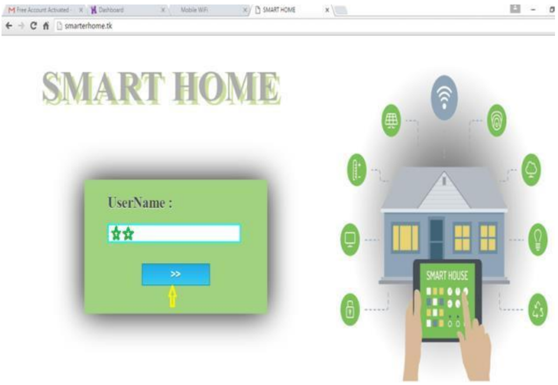


Figure 6: Username page

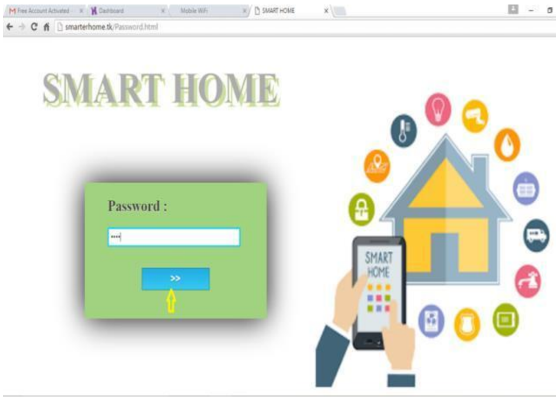
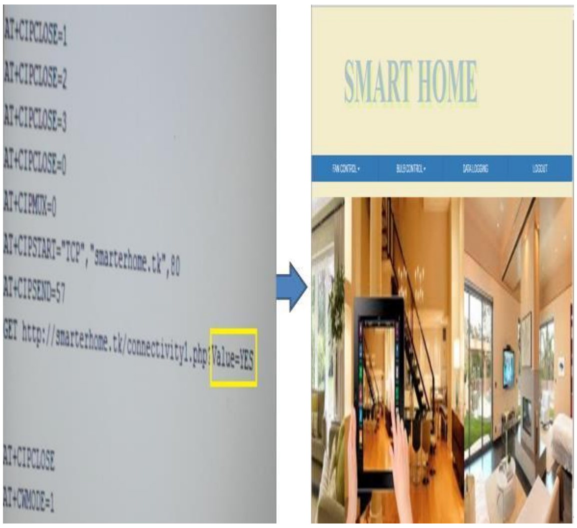


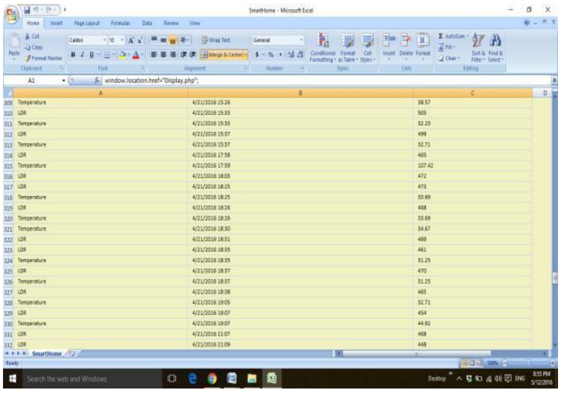
Figure 7: Password page



```
AT+CIPCLOSE=1
AT+CIPCLOSE=2
AT+CIPCLOSE=3
AT+CIPCLOSE=0
AT+CIPMUX=0
AT+CIPSTART="TCP","smarterhome.tk",80
AT+CIPSEND=57
GET http://smarterhome.tk/connectivity1.php?Value=YES

AT+CIPCLOSE
AT+CWMODE=1
```

Figure 8: Home page after response as 'YES' from security module

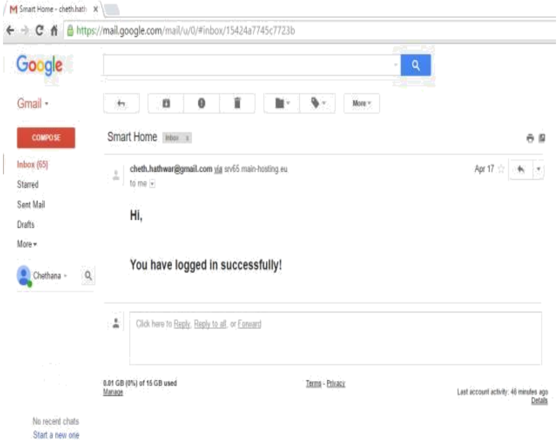


SmartHome - Microsoft Excel

A1 window.location.href="Display.php";

	A	B	C
309	Temperature	4/21/2016 15:26	38.57
310	LDR	4/21/2016 15:33	509
311	Temperature	4/21/2016 15:33	32.23
312	LDR	4/21/2016 15:37	499
313	Temperature	4/21/2016 15:37	32.71
314	LDR	4/21/2016 17:58	465
315	Temperature	4/21/2016 17:59	107.42
316	LDR	4/21/2016 18:03	472
317	LDR	4/21/2016 18:25	473
318	Temperature	4/21/2016 18:25	33.69
319	LDR	4/21/2016 18:26	468
320	Temperature	4/21/2016 18:26	33.69
321	Temperature	4/21/2016 18:30	34.67
322	LDR	4/21/2016 18:31	469
323	LDR	4/21/2016 18:35	461
324	Temperature	4/21/2016 18:35	31.25
325	LDR	4/21/2016 18:37	470
326	Temperature	4/21/2016 18:37	31.25
327	LDR	4/21/2016 18:38	465
328	Temperature	4/21/2016 19:05	32.71
329	LDR	4/21/2016 19:07	454
330	Temperature	4/21/2016 19:07	44.92
331	LDR	4/21/2016 21:07	468
332	LDR	4/21/2016 21:09	448

Figure 9: Sensor data saved onto Microsoft Excel sheet



https://mail.google.com/mail/u/0/#inbox/15424a7745c7723b

Smart Home Inbox

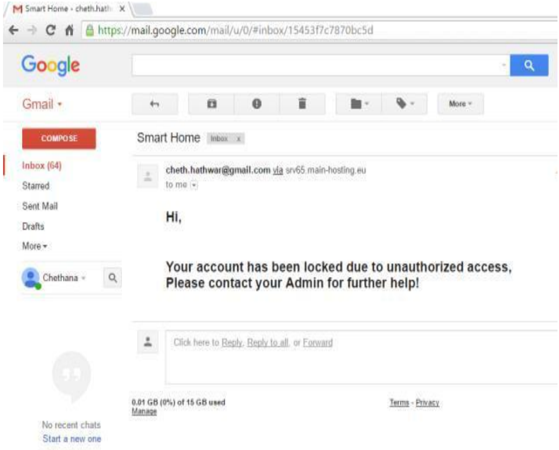
cheth.hathwar@gmail.com via srv65.main-hosting.eu
to me

Apr 17

Hi,

You have logged in successfully!

Figure 10: E-mail notification after successful login



https://mail.google.com/mail/u/0/#inbox/15453f7c7870bc5d

Smart Home Inbox

cheth.hathwar@gmail.com via srv65.main-hosting.eu
to me

Hi,

Your account has been locked due to unauthorized access,
Please contact your Admin for further help!

Figure 11: E-mail notification after three wrong trials of password

The username page is as shown in figure 6. User will have to enter the username first to access the homepage. Once after the authentication of the username through the username stored in database, it goes to password page. The password page is as shown in figure 7. When the user enters the password, it goes to the security module through wifi-module and verifies the password. Only if the password matches, access to home page is given and it is shown in figure 8. The data sent by the sensor is stored in the database and gets displayed on the home page under data-logging column. The data stored in database can also be saved onto Excel sheet for future use, if any. Figure 9 illustrates this. Once after successful login, mail is sent to the user as illustrated in figure 10. Suppose three times wrong password is entered, access is denied and a mail is sent to user about the access denial and is shown in figure 11. Only after the admin resets the account, it is released and the user can access the account.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

A smart home is designed through a security key, using which, a bulb, fan can be controlled and also the temperature and LDR sensor readings are sent to database. This data stored can be read from anywhere, anytime and also can be saved onto Excel sheet. The devices also can be controlled from anywhere anytime. The user is given a key to access the home page and this key is generated by the security module. So, the user entered key is matched with the security module generated key and only then access to home page is given. E-mail notification is sent to the user after successful login and after three wrong trials of the password, account gets locked and an E-mail is sent to the user. Until admin resets the account, it cannot be used. Once after the reset, user gets a mail regarding the release of the account and then the user can access the account. Thus, additional security is provided for smart home application through hardware, which can also be extended to other IoT applications.

B. Future work

Security can be improved by using hardware (IC) which generates different key every time. Monitoring the home appliances to know the status of the device, i.e., whether it is ON or OFF and also the duration as to how long it is ON or OFF. Intimation to the user through message or mail regarding servicing of the faulty devices at home. Analysis of the sensor data's can be done using graphs.

ACKNOWLEDGMENT

We acknowledge the efforts and hard work by the experts who have contributed towards development of the different smart home systems. We also acknowledge the efforts of Dr. T S Chandar, Chairperson of ECE Dept, PESU for his constant support, and suggestions.

REFERENCES

[1] Rajeev Piyare, "Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone", *International Journal of IOT, 2013, pp. 5-11.*

[2] Vinay sagar K N, Kusuma S M, "Home Automation using Internet of Things", *International Research Journal of Engineering and Technology, 2015, pp.1965-1970.*

[3] Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara, Subhas Chandra Mukhopadhyay, "Towards the implementation of IOT for Environmental condition monitoring in homes", *IEEE Sensors Journal, 2013.*

[4] Freddy K Santoso, Nicholas C H Vun, "Securing IOT for Smart Home System", *International Symposium on Consumer Electronics (ISCE), IEEE, 2015, pp. 1-2.*

[5] Andi Adriansyah, Akhmad Wahyu Dani, "Design of Small Smart Home System Based on Arduino", *Electrical Power, Electronics, Communications, Controls, and Informatics Seminar (EECCIS), IEEE, 2014, pp.121-125.*

[6] Meensika Sripan, Xuanxia Lin, Ponchan Petchlorlean and Mahasak Ketcham, "Research and Thinking of smart home Technology", *International Conference on Systems and Electronic Engineering(ICSEE), IEEE, 2012.*

[7] Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang, Chengdong Li, "An IoT based appliance control system for smart home", *International conference on Intelligent Control and Information Processing(ICICIP), IEEE, 2013.*

[8] R.A.Ramlee, M.A.Othman, M.H. Leong, M.M.Ismail, S.S.S.Ranjit, "Smart home system using android application", *International Conference of Information and Communication Technology(ICoICT), IEEE, Bandung,2013, pp.277-280*

[9] Charith Perera, Chi Harold Liu, Srimal Jayawardena, Min Chen, "A Survey on IOT from Industrial market perspective", *IEEE Journal, vol.2, 2014, pp.1660-1679*

[10] Andreas Jacobsson, Paul Davidsson, "Towards a model of privacy and security for smart homes", *IEEE 2nd World Forum on IoT(WF-IoT),Milan, 14-16 Dec. 2015, pp.727-732*

[11] Orlando Arias, Jacob Wurm, Khoa Hoang, Yier Jin, "Privacy and security in IOT and wearable devices", *IEEE transactions on Multi-scale computing systems, vol.1,2015, pp.99-109*

[12] Khusvinder Gill, Shuang-Hua Yang, Wan-Liang Wang, "Secure remote access to home automation networks", *IET Information Security Journal, vol.7,2013, pp.118-125*

[13] N. Komninos, E. Philippou, A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures", *IEEE Journal, IEEE communications surveys and tutorials, vol.16, 2014, pp.1933-1954*

[14] Changmin Lee, Luca Zappaterra, Kwanghee Choi, and Hyeong-Ah Choi, "Securing Smart Home: Technologies, Security challenges and Security Requirements", *IEEE Conference on Communication and Network Security(CNS), San Francisco, CA, 29-31 Oct. 2014, pp.67-72*

[15] Hong-Linh Truong, Schahram Dustdar, "Principles for Engineering IOT cloud systems", *IEEE Journal, vol.2, 2015, pp.68-76*