IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Internet of Things (IoT): A study on Architectural elements, Communication Technologies and Applications

Shruti G Hegde[1], Soumyalatha[2]

Asst Professor, Dept of Computer Science and Engineering, Brindavan College of Engineering, Bangalore, India[1, 2]

Abstract: IoT is an emerging technology wherein billions of sensors from multiple vendors are embedded with the daily objects are interconnected together to sense the data continuously depending on the context and sends these data over the internet to the central database. Data analytics in tern provides the required contextual result. This leads to comfortable life with minimum or without human intervention. This paper addresses working of IoT, general IoT architecture by considering two scenarios where we have also differentiated number of layers required for the different applications. The most important factor of IoT is to understand the essential components required to build IoT and the integration of different communication technologies. For such a scenario, our study paper mainly concentrates on the essential elements to build IoT, different IoT communication technologies and different application domains, which helps the students, researchers and those who can further contribute.

Keywords: Blutooth , Cellular Network, RFID, Sensors, Wi-Fi, ZigBee

I. INTRODUCTION

Internet of things (IoT) is collection of daily life objects which are embedded with sensors, which sense the data based on the context and sends to the central database system through wired network or wireless Network such as Bluetooth, wireless Fidelity(Wi-Fi), 3G or 4G. Recently IoT is gaining popularity mainly because of low cost sensors, improved technology, reduced storage cost and efficient analytical tools. According to Cisco Internet Business Solutions Group (IBSG) study [1], by the year 2020, world population will be 7.6 billion and around 50 billion devices will be connected to the internet. This shows that IoT has a broad platform which will improve the normal human life style by connecting daily life objects to the internet and doing task whatever human does. Every device such as phones, laptops, tablets, desktops, TV, Microwave oven, Fan, door, bulb, Fridge, different parts of human body are capable of connecting to the internet by embedding sensors into them and making them the smart devices.

Each of these smart devices requires unique IP address to connect to the internet. With the use of Internet Protocol Version 4(IPv4) only 4.3 billion unique addresses can be generated, which is lesser than the world population and even than the number of devices connected to the internet as per IBSG. So IPv6 is used which gives $3.4x10^{38}$ unique addresses [2,3]. General block diagram of working of IoT is show in the Fig.1. As shown in the diagram, different context aware sensors are attached to AC, Gas Cylinder and Door. Each sensor senses the data and sends through Wi-Fi through Internet. All these sensed data are stored in server database. Server processes the data and analyses and sends the result to the user smart phone or user laptop.

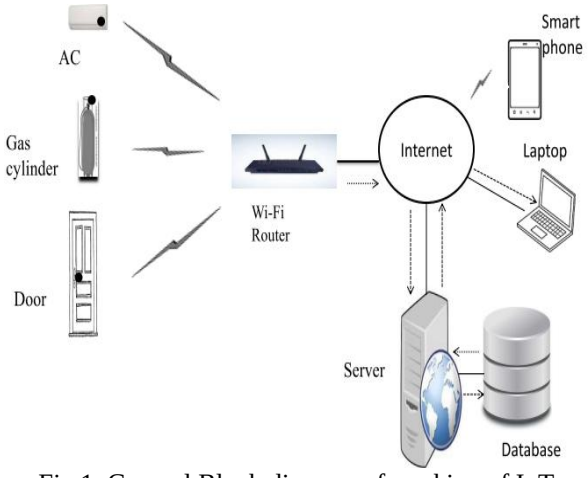

Fig.1. General Block diagram of working of IoT

In this paper we have discussed Architecture of IoT in section II, Elements of IoT in section III, communication Technologies in section IV and Application domains in section V.

II. ARCHITECTURE OF IoT

Architecture of IoT [4] depends on various applications of IoT. For e.g. consider two scenarios.

Scenario-1: Let's consider smart devices for pollution, wherein sensors sense the amount of carbon monoxide, nitrogen dioxide, sound level etc. and sends these data continuously to the central database. These data will be analysed by using analytical tools and gives information about amount of air pollution in that particular city to the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

traffic police. This information helps to take the precaution when it exceeds the normal level. In this scenario Fig.2b architecture hold good. Here sensor layer indicates sensors will be continuously sensing the air and sends the data through Wired or wireless communication to the database.

This data will be processed and analysed and final consolidated result will be send to the user smart phone through the Air pollution control application. Hence four layers architecture is required.

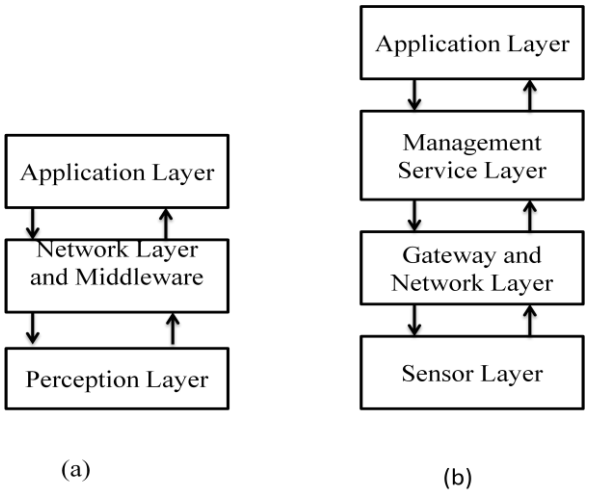

Fig.2. General 3 Layer/ 4 Layer architecture for IoT

Scenario-2:
Let's consider a sensor is attached near the kitchen or gas cylinder with context to find the gas leakage. In this whenever sensor detects gas leakage it has to alert the surrounding immediately and then has to send the message to the owner.

In this case analysing has to be done in the sensor layer itself. Hence architecture shown in fig.2a hold good.

III. ELEMENTS OF IOT

Essential components[5] which are required to build IoT are i) hardware components such as sensors, actuators, ii) Middleware components such as database for storage and data analytical tools iii) Visualization through different applications. This section explains important IoT key elements which are used to build IoT as shown in Fig.3.

A. Unique identification for each smart device
IoT consists of huge number of smart devices. Each of this device requires a unique identification for communication and also helps to control and access remote devices through internet.Ipv4 addressing supports limited number of unique addressing for smart devices.

IPv6 provides large set of unique address. Apart from this unique address, each of these devices also has object id. This object id is used to refer the smart device within the communication network.

B. Sensing devices
Each object embedded with sensors continuously sense the data based on the context. Context may be sensing humidity or temperature or sound level, amount of air pollution or motion etc.

C. Communication
Sensed data from smart devices are sent to the database through the communication technologies. This communication technology may be Radio Frequency Identification (RFID), Bluetooth, Near Field Communication (NFC), Wi-Fi, ultra-wide bandwidth(UWB), Z-wave, 3G, 4G and Long Term Evolution-Advanced(LTE-A). In detail communication technologies are explained in section –IV.

D. Data storage and analytics
In IoT smart devices produces large amount of data, which has to be stored in the storage device. These stored data has to be analysed to extract the meaningful information.

To do this, analytics or analytical tool which incorporates intelligent algorithm has to be developed to extract the useful information from raw data. This analytical tool has to support interoperability with different platforms. In the IoT architecture middleware represents the both storage and analytical tools. A centralized infrastructure is required to support both Storage and analytical tools.

E. Visualization
Nowadays the world has become smart with smart phones. By using smart phones or laptops user has to download the required application and through which user can interact with centralized database and get the useful information about the actual environment

Fig.3. Essential Key elements of IoT

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

IV. COMMUNICATION TECHNOLOGIES/PROTOCOLS

The IoT communication technologies support heterogeneous smart devices or smart objects to communicate to provide smart services. These smart devices should work efficiently with low power consumption and high battery life. This Machine to machine communication is divided into two categories.

A. Capillary M2M network

There are many Short-range M2M wireless technologies or protocols are used in IoT. Each of this is used to communicate one device with another device for M2M communication. Each of this is explained below.

1) RFID

RFID devices are wireless microchips which can identify objects wirelessly without line-of-sight and supports communication range up to 100m.This is used for automated identification of tagged objects.

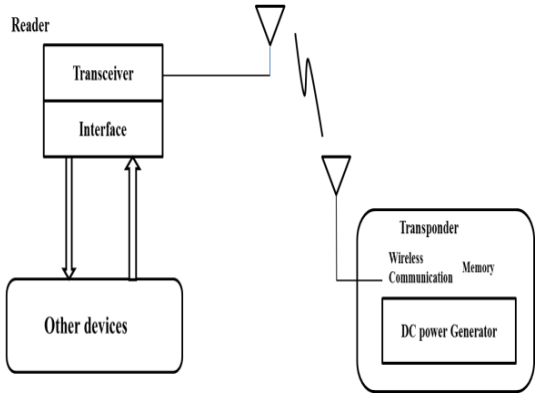

Fig.4. General Architecture of RFID tag and RFID reader

Whenever RFID tag receives query request signal from RFID reader; it sends back a signal with a unique ID; with this all the details of that object is available through the database. Based on the power source the RFID tags are classified into active tags, Passive tags and Semi passive/active RFID tags. IoT based RFID can be broadly classified into three components i) RFID system with readers, tags and antennas. ii)A middleware system for data transmission and data classification and iii) Internet system for providing services to the by processing, control, analysis and decision making.[6][7]

2) BLUETOOTH

Bluetooth is a wireless technology for exchanging data over short distance with data throughput of 720Kbps. Communication range varies from up to 100m and operates at 2.4GHz frequency band.. This is designed with intension of exchanging bulk continuous data at short range and hence consumes lot of battery power. Bluetooth low energy (BLE) indicated by Bluetooth smart or Bluetooth 4.0 is a low power consumption wireless technology; which is capable to run the device with tiny battery for long time. In IoT, smart devices send the information through Bluetooth through which it will be connected to the internet. Since IoT requires low power wireless connection to the internet, by using BLE all smart devices will be connected to the internet. [8, 9].

3) NFC

NFC is a short range wireless communication technology to exchange the data between two devices up to 10 cm with short setup time and data rate up to 424kbps. This operates at very high frequency of 13.56MHz. In many IoT applications NFC acts as a bridge between IoT-smart devices and internet, through which smart devices sends the data to the server. Using IoT concept Many integrated NFC sensor are used for Industrial, Medical purposes.

4) Wi-Fi

This is a wireless communication technology which allows smart devices to connect to a wireless networks and allows high speed data transfer by using radio waves over short range. In Indoor environment this provides internet access up to 38metres and for outdoor 140m. Since Wi-Fi is used in Home, large offices and campuses, this allows smart devices to exchange the data using Wi-Fi Router. Because of low cost, low power; in IoT many application domain uses Wi-Fi for transferring the data.

5) ZigBee

This is a wireless communication technology uses mesh network protocol to transfer small amount of packets over short communication range of 70metres. Profiles of Zigbee such as ZigBee-Pro, ZigBee Remote control operates at 2.4GHz and used for the application which requires battery operated smart devices, low level throughput and low power consumption. This is used in home automation applications.

6) 6LoWPAN

6LoWPAN[10] combines IPv6 and Low-power Wireless Personal Area Network (LoWPAN) is a network protocol; which is used for the application which has smallest device with limited processing ability. This is used in IoT applications with the main intension that even smallest devices and low power device can participate in IoT.

7) UWB

The UWB communication technology is designed to support communications within a low range coverage area up to 70m using low power, high bandwidth and 100Mbps of high speed transmission.

8) Z-Wave

Z-Wave is an inexpensive, low power wireless communication protocol. Now a day's millions of Z-Wave devices are deployed for smart home automation and for business automation etc. Z-Wave supports 30meters point to point communication and operates at 900MHz frequency and allows data transmission range 40kbps to 200kbps.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

B. Cellular M2M network

This type of network supports long range communication by using cellular network by the service provider. Although 2G and 3G cellular networks are mainly used in cellular IoT services, the LTE is an emerging technology for M2M communication. 2G or 3G enabled SIM card has to insert into smart phones or to tablets which through which smart devices communicates to the internet. Long-Term Evolution –Advances wireless communication technology for high-speed data transfer. This supports bandwidth up to 100MHz. Comparison of different communication technologies by considering its Frequency, Range and Data rate are given below.

TABLE I
COMPARISON OF COMMUNICATION TECHNOLOGIES VS PARAMETERS

	Frequency	Range	Data Rate
RFID	125kHz/2.45 GHz	Up to 100m	Up to 640 kbps
Bluetooth	2.4GHz	50-100m	1Mbps
NFC	13.56MHz	10cm	100-420 kbps
WiFi	2.4GHz	~50m	600mbps
ZigBee	2.4GHz	10-100m	250kbps
6LoWPAN	2.4Ghz	200m	250kbps
UWB	3.1-10.6 GHz	~70 m	480Mbps-1.6Gbps
Z-Wave	900MHz	30m	40kbps-200kbps
3G	1.8-2.5GHz	-	385kbps-2Mbps
4G	2-8GHz	-	20-100Mbps

V. APPLICATIONS

With large number of self-organized sensors and communication technologies IoT can be used in different areas. We have explained different applications of IoT by considering different domains as shown in Fig.5.

A. Home IoT

Home IoT consists of three components [11] such as server, network gateway and smart devices. Smart devices are sensors embedded with TV, or Sensors embedded with Doors. Consider motion aware context based sensors are attached to TV. This sensor senses the motion of person and sends the data to the server through Wi-Fi. These raw data are analysed such that if long for a long time there is no motion it has to reduce the volume of the TV or switch off the TV. So Home IoT gives more comfort to people life.

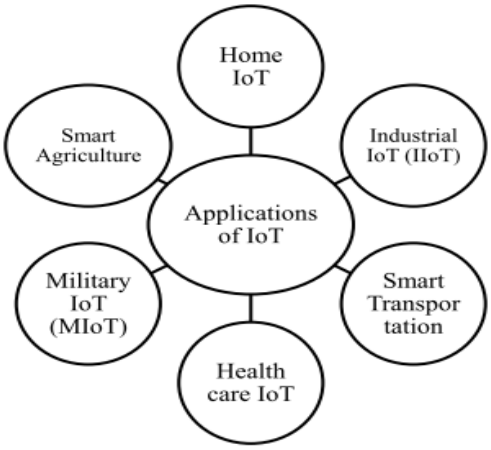

Fig.5. Application of IoT

B. Industrial IoT

IoT in industries lead to Industrial Internet of Things(IIoT) which has added more value to industry. Sensor and actuators are used in industrial environment to improve manufacturing process intern to reduce the cost, to increase efficiency of providing services to customer [12] and also provides safety measures to the manufacturers. For e.g. consider incense sticks industry where-in many places temperature measuring sensors has to be attached.

These sensors continuously sense the temperature. If fire exists in the industry temperature will be very high. In this case when temperature crosses the normal limit, the warning bell will be ringed and immediately owner gets the message. In the supply chain, RFID will be embedded with each product, by this way we can see the status of the product in each stage. Gartner predicts during 2020, by using IIoT $309 billion additional revenue will be produced for suppliers [13].

C. Military IoT

IoT concept is introduced into Military domain by integrating sensors to military things for the purpose of military, formed Internet ofMilitary Things (IoMT) or military internet of Things (MIOT)[14,15]. In IoMT Sensors or actuators, RFID are embedded to military equipment or within the military information infrastructure. These smart devices sense and send the data, which has to process and relevant data will be extracted. So IoMT is interconnection of unique sensors or RFID integrated devices which gives the information such as location, Threat recognition, attacker movement etc. This information helps proper utilization of resources and efficient military operation.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

D. Health care IoT

Wearable devices [16] are small in size and sensors are embedded within it. These wearable are placed in end-user or patient, which sense physiological data and movement. By using communication technology such as Bluetooth or Wi-Fi or 3G or 4G, these data will be sent to remote data centre. By using data analysis techniques, these data will be analysed and clinically relevant information will be extracted. This information will be sent to doctor and he treats accordingly. The IoT has central decision unit [17] which gives immediate alert bell if it detects dangerous condition based on the generated data.

E. Smart Transportation

Sensors, RFID, Speed sensor, Camera, Vehicle monitoring equipment[18], Payment devices etc. are embedded within the different part of vehicle to sense the data continuously during the movement and even after parking the vehicle. These data will be sent using communication technology to the central database. These data are extracted to get the relevant information. This provides information regarding real-time safety protection, fuel advice, vehicle condition, fuel consumption, road condition, driving distance etc.

F. Smart Agriculture

In the greenhouse[19,20], sensors which collects information such as temperature, pressure, light, humidity, CO2 etc. of plants will be collected and sent to the server. This server processes the data and decides type of action to take on plant such as sprinkling water, switching on fan, curtain control to control heat from direct sun light etc. With this it reduces human resources and saves energy.

VI. CONCLUSION

With the reduced sensors cost, storage, improved communication technologies and efficient data analytical tools IoT has gained significant attention over the years. In this paper we have discussed various communication technologies that are used for communication between the heterogeneous smart devices. We also discussed different layered architecture which differs based on the application domain. We also generalized the essential components to build IoT and also briefed out different application domains of IoT with a related scenario. Byall accounts, IoT has a vastopportunity for research, cost savings, new revenue generation and adding comfort to humans.

REFERENCES

[1] Dave Evans,"The Internet of Things How the next evolution of the internet is changing everything",,white paper , 2011.
[2] Ahmad El Kouche ,"Towards a Wireless Sensor Network Platform for the Internet of Things", IEEE ICC 2012-Ad-hoc and sensor Networking Symposium,978-1-4577-2053-6/12, 2012 IEEE.
[3] Andrej Mihailovic, Marko Simeunoviü, NedjeljkoLekiü, "A strategy for deploying diverse sensor-based networks as an evolution towards integrated Internet of Things and Future Internet", 22nd Telecommunications forum TELFOR 2014, 978-1-4799-6191-7/14, IEEE 2014
[4] JayavardhanaGubbi,RajkumarBuyya,SlavenMarusic,MarimuthuPalaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems 29 (2013) 1645–1660, 2013 Elsevier
[5] Ala Al-Fuqaha,MohsenGuizani,MehdiMohammadi, Mohammed Aledhari , MoussaAyyash,"Internet of Things: A survey on Enabling Technologies,Protocols-and-Applications",IEEE,2015.
[6] JebahJaykumar ,Jebah Jaykumar1, Abishlin Blessy2, ," Secure Smart Environment Using IOT based on RFID", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2493-2496,2014.
[7] "The Research of IoT Based on RFID Technology", 2014 7th International Conference on Intelligent Computation Technology and Automation, KuBo Wuhan Vocational College of Software and Engineering, HuBei 420305, China, 978-1-4799-6636-3/14 $31.00 © 2014 IEEE 2014
[8] Mats Andersson, Use case possibilities with Blutooth low energy in IoT applications, White paper
[9] ShahidRaza, PrasantMisra, Zhitao He, Thiemo Voigt, "Bluetooth Smart: An Enabling Technology for the Internet of Things", Eight International Workshop on Selected Topics in Mobile and wireless Computing, IEEE ,2015.
[10] SatishPhakadePawar,"Home Automation with 6LoWPAN"
[11] Jin-Hee Han, YongSungJeon, JeongNyeo Kim, "Smart Home System in the IoT Environment", IEEE, 2015.
[12] Willian T. Lunardi, Everton de Matos, RamoTiburski, Leonardo A. Amaral, Sabrina Marczak, FabianoHessel," Context-based Search Engine for Industrial IoT:Discovery, Search, Selection, and Usage of Devices", 978-1-4673-7929-8/15, 2015 IEEE
[13] Releasing the Value Within the Industrial Internet of Things, Attunity, White paper.
[14] Jan Chudzikiewicz, JanuszFurtak, Zbigniew Zielinski, " Secure protocol for wireless communication within Internet of Military Things", IEEE, 2015
[15] LanYushi, Jiang Fei, Yu Hui, "Study on Application Modes of Military Internet of Things(MIOT)", IEEE, 2012
[16] Ebrahim AL Alkeem, Chan YeobYeun, M.JamalZemerely, "Security and Privacy Framework for Ubiquitous Healthcare IoT Devices", ICITST, IEEE,2015
[17] HaobijamBasanta, Yo-Ping Huang, Tsu-Tian Lee, "Intuitive IoT-based H2U Helathcare System for Elderly People", International conference on networking , sensing and control, IEEE, 2016.
[18] Building an Intelligent transportation system with the internet of Things(IoT), Solution blueprint, Intel
[19] Ji-chun Zhao, Jun-feng Zhang, Yu Feng, Jian-xinGuo, "The study and Application of the IoT Technology in Agriculture", IEEE, 2010
[20] Liu dan, Cao Xin, Huang Chongwei, JiLiangliang, "Intelligent Agriculture Greenhouse Environment Monitoring System Based on IOT Technology", International Conference on Intelligent Transportation, Big Data & Smart City, 2015.

BIOGRAPHIES

Ms. Shruti G Hegde Received BE and M.Tech degree from VTU, Belgaum. Currently working as an assistant professor in the department of CSE at Brindavan college of Engineering, Bangalore. A research interest includes Big data, Internet of Things and Wireless networks.

Mrs. Soumyalatha Received BE and M.Tech degree from VTU, Belgaum. Currently working as an assistant professor in the department of CSE at Brindavan College of engineering, Bangalore. Research interests includes big data, Internet of Things and Wireless networks