International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 494 – 501

Optimization of A Smart IOT Gateway

Rashida Shujaee
Electronics & Communication
ACET
Nagpur, India
e-mail:shujaee.rashida@gmail.com

Prof. M. Nasiruddin
HOD, Electronics & Communication
ACET
Nagpur, India
e-mail: mn151819@gmail.com

***Abstract*—**In recent years, the Internet of Things (IOT) has attracted many attentions. It allows a number of objects that have been embedded with wired or wireless communication interfaces to automatically communicate and interact with each other. The IOT is a system, combination of embedded controllers, sensors, software's and network. After internet and mobile communication, IOT is regarded as the third wave of information because of its huge market prospects. The development of IOT can support a variety of applications including Intelligent Art, Intelligent Logistics, Intelligent Medicine & Healthcare, Intelligent Transportation, Intelligent Power, Smart Life etc. IOT Gateway plays an important role in IOT applications since it bridges between wireless sensor networks with traditional communication networks or internet. This paper includes an IOT Gateway system based on Zigbee and Wi-Fi protocols according to the presented data transmission between wireless sensor networks and mobile communication networks, typical IOT application scenarios and requirements from telecom operators, protocol conversion of different sensor network protocols, and control functionalities for sensor networks, and an implementation of prototyping system and system validation is given.

Keywords*-Gateway, IOT, WSN, Zigbee*

*****

I. INTRODUCTION

The Internet is a worldwide system of interconnected computer networks. Nowadays, there are several ways that enable us to access the Internet. Technology is keep improving, method to access the Internet also increase. People can now access Internet services by using their cell phone, laptop and various gadgets. Earlier only static web sites and email communication represented the Internet. But now different forms of internet implementations could be seen everywhere around us. Today, internet has become an integral part of our lives that meet each user's needs irrespective of time and place, providing plenty of applications and services. The main reason behind this is the user-friendly automated machines and user digitalization.

The Internet is a technology that has greatly enhanced our lives. The demand of using internet has increased greatly over the years, and it reflects into all of the users' devices respectively in one way or another. Nowadays, it is considered as a mandatory part of our lives that smart devices providing connectivity to the world at each second. Thus, each year the number of connected devices rapidly increases. Therefore, it is required to create an autonomous device communication. Today, Internet of Things (IoT) is one of the promising solutions. The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.The IoT creates opportunities for more direct integration of the physical world into computer-based systems, by allowing objects to be sensed or controlled remotely across existing network infrastructure, and resulting in improved accuracy, efficiency and economic benefit in addition to reduced human intervention.

The applications of Developing and growing Internet of Things (IoT) technology such as the rich connection modes, the traffic data volume from numerous connected IoT terminals, etc. increasingly affects the backbone network development. Several researchers tried to clarify such effects; however most of such contributions are diverse and especially not in a traffic view. Though this is the real case, a special focus have been ignited by them that an IoT gateway (IOTGW) accounts a big part among the effects. Different IoT devices are connected directly to an internet router or by using an IoT Gateway in an IoT network that acts as bridge between the internet and the constrained IoT network. To receive requests from a server and to upload data, IoT devices connect to the internet. Through a web interface, users can upload data from their devices and control them using web applications installed on a server.

The concept of the Internet of Things (IOT) was proposed by the Auto-ID Laboratory of MIT in 1999. A wireless network between objects; usually the network will be wireless and self-configuring, such as household appliances or a network which can connect things identified in the physical world throughout various networks with different protocols is referred as IOT. A system which is a Combination of Embedded controller, sensors, Software's and Network is called the Internet of Things (IOT). The Internet of Things (IoT) has attracted many attentions in the late years. It allows a number of smart objects that have been embedded with wired/wireless communication interfaces to automatically communicate and interact with each other. Unidentifiable

objects can be made identifiable, recognized, interconnected intelligent objects with the help of IoT. Intelligent Power, Intelligent Transportation, Intelligent Medicine and Healthcare, Intelligent Art, Intelligent Logistics, Intelligent Environmental Monitoring, Smart Life, etc. are some of the applications that can be supported by the development of IOT.

Today sensors are everywhere in our smart phones, in our vehicles, even in the ground monitoring soil conditions in vineyards, and in factories controlling CO2 emissions. We take them for granted. Research on wireless sensor networks (WSNs) started back in the 1980s, though it seems that sensors have been around for a while, and WSNs generated an increased interest from industrial and research perspectives only since 2001. This is due to the availability of inexpensive, low powered miniature components like processors, radios and sensors that were often integrated on a single chip (system on a chip (SoC)).

The idea of internet of things (IoT) was developed in parallel to WSNs. These objects can be anything from planes, cars, industrial plants, large buildings, machines, and specific parts of a larger system to human beings, any kinds of goods, animals and plants and even specific body parts of them.

FigureI. Internet of Things Applications

While IoT does not assume a specific communication technology, wireless communication technologies will play a major role, and in particular, WSNs will proliferate many applications and many industries. The small, rugged, inexpensive and low powered WSN sensors will bring the IoT to even the smallest objects installed in any kind of environment, at reasonable costs. A major evolution of WSNs will be the integration of these objects into IOT. A WSN can generally be described as a network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the surrounding environment. In fact, the activity of sensing, processing, and communication with a limited amount of energy, ignites a cross-layer design approach typically requiring the joint consideration of distributed signal/data processing, medium access control, and communication protocols.

Through synthesizing existing WSN applications as part of the infrastructure system, potential new applications can be identified and developed to meet future technology and market trends. For example, Smart grid, smart water, intelligent transportation systems, and smart home are some WSN technology applications that generate huge amounts of data, and this data can serve many purposes.

The number of connected sensors will soon reach trillions, with the advancement of the Internet of Things (IoT), and will drive new consumer and business behavior, working with billions of intelligent systems involving in-numerous applications. The increasingly demand for intelligent industry solutions based on IOT will drive more opportunities for the companies that take advantage of the IoT, and trillions of dollars in opportunity for IT industry.Military applications, notably surveillance in conflict zones inspired the development of WSNs. Today, they consist of distributed independent devices that use sensors to monitor the physical conditions with their applications extended to industrial infrastructure, automation, health, traffic, and many consumer areas.

When the United States Defense Advanced Research Projects Agency (DARPA) carried out the distributed sensor networks (DSNs) programme for the US military in the early 1980s, research on WSNs dates back to that time. At that time, the Advanced Research Projects Agency Network (ARPANET) had been in operation for a number of years, with about 200 hosts at universities and research institutes. Many spatially distributed low-cost sensing nodes, with information being routed to whichever node that can best use the information, and collaborating with each other but operated autonomously were assumed to be contained in DSNs.

Even though early researchers on sensor networks had the vision of a DSN in mind, the technology was not quite ready. Moreover, the number of potential applications was limited, and the sensors were rather large (i.e. the size of a shoe box and bigger). Furthermore, the earliest DSNs were not tightly associated with wireless connectivity. Recent advances in computing; communication and micro-electromechanical technology have resulted in a significant shift in WSN research and brought it closer to the original vision. More and more attention and international involvement has been attracted by the new wave of research on WSNs that started around 1998. The new wave of sensor network research puts its focus on networking technology and networked information processing suitable for highly dynamic ad hoc environments and resource-constrained sensor nodes. Many new civilian applications of sensor networks such as environment monitoring, vehicular sensor network and body sensor

networks have emerged, since the sensor nodes have been much smaller in size (i.e. from that of a pack of cards to dust particle) and much cheaper in price.

One of the top most initiatives in the form of Digital India Program of the Government which aims at 'transforming India into digital empowered society and knowledge economy', is expected to provide the required impetus for development of the IoT industry ecosystem in the country .In October, Deity had invited public opinion on how to improve the draft policy to create ecosystem for IoT industry in the country. To increase the connected devices from around 200 million to over 2.7 billion by 2020 and to increase the connected devices from around 200 million to over 2.7 billion by 2020 is the objective of the policy.

II. RELATED WORKS

In 1999, Auto-ID Laboratory of MIT introduced a concept known as Internet of Things IOT. As the popularity of IOT is growing up abruptly, It is expected that more and more no. Of devices will be connected to the Internet in upcoming years. In this section, we will take a brief review of some existent Internet of thing (IOT) gateways. As listed below-.

Shang Guoqiang, Chen Yamming, zuo Chao, Zhu Yanxu [1] – In this paper, the author has specified a pluggable gateway system which would run on high power also has an external interface for software development.

Qian, Ruicong, Yan, and Weijun [2] - In this paper the author specified a gateway for interconnection .different protocols like ZIGBEE, BLUETOOTH etc, but they are not that flexible just due to their customization for different applications.

Emara, K. A., Abdeen, M., &Hashem [3] - proposed gateways for interconnection.Those gateways connect networks with different protocols such as ZigBee, Bluetooth, GPRS and Ethernet transparently. But those gateways are not flexible, because they cannot be customized for different applications.

L.Wu, Y. Xu, and F.Wang [4] - designed a plug-configurable-play service-oriented gateway, aiming to make it fast and easy to employ various external sensor network applications. The gateway encapsulates data, capabilities and information of heterogeneous sensor networks to homogenous resources. It provides external applications with access of corresponding resources through friendly and uniform interfaces, which are independent of types of sensor networks. The gateway is not for specific kinds of sensor networks or applications. The feature of plug-configurable-play is achieved by separating the universal program from sensor network specific information. But the gateway is running on PC, and demands for higher hardware environment. So the advantages in the actual IoT applications are not obvious.

Jong-Wan, Yong-ki, Choon-Sung, & Dong-Rye [5] - proposed a system composing of a main server and several sensing servers connecting with different sensor networks. But in their system, most tasks are completed by different network-dependent sensing servers other than a smart gateway. This indicates the hardware cost will be too high.

Shan Yin,YuemingLu,Yonghua Li [6] - In this paper author specified a system based on IOT which will connect all home appliances together and a centralized gateway based on RFID. So that they would communicate properly but linkage policy used here is manual, not feasible.

III. PRELIMINARY

A. Basic Architecture of IOT

The architecture of an IoT, which comprises of sensing layer, network layer and application layer, is shown in Figure 3. In the sensing layer, substantial numbers of identifiers and sensors are placed in the object or environment to detect events, scenarios, motions of objects or collect environmental information. Through the transmission technologies provided in the network layer (such as wireless ZigBee, Bluetooth, Wi-Fi or wired networks), sensors transmit the detected data to the back-end management system for processing. The collected data are then analyzed, extracted and integrated in the application layer before being converted into value-added services for application in various IoT areas, such as medical care, transportation, healthcare, environmental surveillance, and arts and humanities.

The sensing layer enables "things" to be identified, sensed and evolved in communication infrastructures with a variety of sensor devices. These devices are connected together through Wi-Fi, Ethernet, bus, 3G/4G/LTE, ZigBee, RFID or other modes in the network layer. The data can be utilized and communicated for users in the application layer. All the three layers form a complete application scenario. In the three-tier architecture of IoT, a smart gateway plays an important role between the sensing layer and network layer, which can shield the heterogeneity of the sensor networks, especially on the Internet. Owing to a variety of sensor devices, the gateway is often complex and expensive. At present, different applications usually use different kinds of gateways with poor compatibility.

Because of the advancements in sensing, identification, and network communication technologies, the diverse services have been gradually extended from internet to the IoT. IoT-based service provides human with obtaining and controlling the status of the smart object through internet. Currently, people can communicate via the internet; however, people live in the physical world, whereas the internet is part of the digital world. Thus, connecting various smart objects into a human interactive network, enabling internet access for smart objects, is the basic principle for establishing an IoT service. Thus, developing a method by which people can be provided with superior control over the internet and be

informed of the status of interactive objects in the physical world will be the main focus of IoT. IoT technology can be used to efficiently manage, control and monitor for the state of smart objects. Thus, relevant applications of IoT have recently received much international attention as a high-tech industry with unlimited potential and opportunities. Additionally, substantial resources have been invested to facilitate the promotion, research and development of this industry.

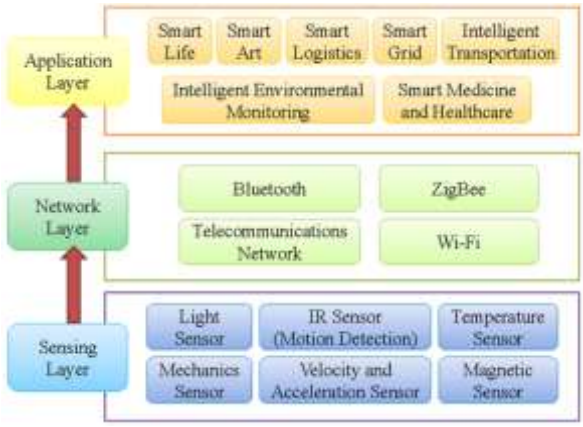

Figure2. Basic Architecture of an IOT

B. Introduction to IOT Gateway

There are many sensors and actuators that interact with the machinery, in an industrial IOT scenario. Each machine would typically have multiple sensors tracking its health and monitoring the key parameters related to the production. The sensor and actuator that are responsible for acquiring the data or controlling a switch through a pre-defined instruction set, is each attached to a microcontroller. A sensor node is a microcontroller along with the sensors, power and a radio. It is a self-contained, deployable unit that captures the data generated by sensors. The sensor node cannot deal with the data locally, because it doesn't have enough processing power, memory, and storage. To send the data to a central location, a low-energy radio communication network is used. The communication link between the central hub and the sensors' nodes bases on ZigBee, Bluetooth Low Energy (BLE), or Power over Ethernet (PoE). An IOT gateway is a hub that acts as an aggregator of multiple raw datasets generated by the sensor nodes.

AnIoTgatewayhasmultiplerolestoplay.To transform and normalize the data is one of the first jobs of the gateway. The sensor nodes that generate the datasets will be in disparate form. The contemporaryonesmayrelyonJSONorCSV, while some ofthelegacy nodesuseproprietary protocols.The gateway converts heterogeneous datasets into a standard format, which it acquires from multiple sensor nodes, in a format thatisunderstoodbythe next stageof thedata processingpipeline.

Protocol transformation is the second role of an IoT gateway. Sensor nodes use low-powered communication networks, since they cannot use power hungry Wi-Fi or Ethernet. For accepting the inbound data sent by the sensor nodes, a gateway supports multiple communication protocols. It uses a variety of protocols for the outbound communication, which typically connects the gateway to a process running in the cloud. REST, MQTT, CoAP, STOMP and even SMS are some of the popular outbound protocols used in the context of IoT. The gateway may also process the data and raise alerts in real time in some scenarios. But this is best left to the powerful stream processing pipelines running in the cloud. By translating between the two networks, the integrated platform requires IoT gateway to connect the WSN with Internet. The gateway needs an interface to the WSN, and an interface to the internet. The interface to the WSN is a hardware based as it needs to interface with an ZigBee coordinator for the ZigBee based system, or a radio transceiver for the 6LoWPAN system. This means that a suitable hardware platform is required to support network interfaces and hardware interfaces.

Gateways act as an edge device, obscuring the sensor nodes from the public internet. The sensor nodes cannot be accessed directly though it can make outbound connections to the internet and cloud through the gateway. Therefore, Securing the sensor nodes and internal network, gateways play the dual role of routers and firewall.

Sensor nodes still need a gateway for data aggregation and transformation, although they are capable of connecting to the Internet. They connect an appliance running in the cloud called a cloud gateway. A field gateway is the local edge device running on-premises.

Figure 3. Whole processing of Gateway and WSN

Above figure shows overall system hardware of the project .includes microprocessor of ATMega 328P, is dedicated to controlling the operation of entire data acquisition .system is used to collect data from different sensors, process them and sent it to open source data platform.In this system, the Zigbee would be the radio transceiver responsible for data transmission with many other nodes. WIFI unit will function as its own with lower cost and less space requirement.ESP 8266EX gives a standaloneWi-Fi network solution.

C. IOT Communication

The WSN will allow packets form the WSN to be sent and received. These packets need to be processed in order to provide the WSN with internet access. The processing will involve address translation of addresses, encapsulation of data to form an internet packet and unpacking of internet packets to form a WSN packet. The address translation requires the translation of WSN network addresses to an Internet addresses and vice-versa. The extraction of data from a WSN packet and encapsulation of this data in an internet packet is required for the encapsulation of data. The encapsulation of this data in a WSN packet and the extraction of data from an internet packet are required by the unpacking of internet packets.

D. Wi-Fi Technology

To provide wireless network connections and high-speed internet, radio waves are used by Wi-Fi which is a wireless networking technology. Wi-Fi is form of low power wireless communication and many electronic devices such as laptops, smart phones etc.; use Wi-Fi. Wi-Fi has no physical connection between the sender and the receiver. Wi-Fi is capable of operating at 2.4 and 5 GHz. Since it has no physical connections, it is more likely to be attacked than wired connections, such as Ethernet. In a Wi-Fi setup, a wireless router serves as the communication hub. Allowing users to connect only within close proximity to a router or signal repeater, these networks are extremely limited in range due to low power of transmission. Within a range of tens of meters, Wi-Fi equipped devices are capable of connecting to the internet wirelessly. Smart phones, Digital Living Network Alliance-supported televisions (TVs) and digital video disks are some of the devices which are equipped with Wi-Fi technology and are currently available on the market. However, communication among heterogeneous networks is not supported and their functionality to communicate with other Wi-Fi equipped devices is limited, for most Wi-Fi devices. With WLAN and wireless access point, Wi-Fi compatible devices can be connected to the Internet. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. By using multiple overlapping access points, hotspot coverage can be as large as many square kilometers, or as small as a single room with walls that block radio waves. Digital cameras, tablet computers, smart phones, digital audio players, video-game consoles, modern printers, personal computers and smart TVs are some of the devices that can use Wi-Fi technology.

Wi-Fi works on physical and data link layer. Wi-Fi is the generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (WLANs). Wi-Fi is commonly used for connecting devices in wireless mode, and is an alternative to wired technology. To ensure compatibility and co-existence of devices, to make access to information easier, eliminate switches, adapters, plugs pins and connecters and to eliminate complex cabling are the main aims of Wi-Fi. Wi-Fi network connect computers to each other, to the internet and to the wired network. To hide complexity by enabling wireless access to applications and data, media and streams, is the purpose of Wi-Fi. Wi-Fi technology builds on IEEE 802.11 standards. The IEEE develops and publishes these standards, but does not test equipment for compliance with them. In terms of radio, Wi-Fi technology is easiest to understand, the only difference is in the strength of the signal, otherwise it is similar to walkie-talkies. To transmit data between its nodes (Sender & Receiver), Wi-Fi uses radio networks. These networks are made up cells that provide coverage across the network. The coverage on the radio network is stronger and greater with more number of cells.

E. Zigbee Technology

Zigbee is an IEEE 802.15.4-based specification that provides numerous advantages such as high reliability, multi-network topology, low power consumption, bidirectional transmission and low cost. The superb characteristics of ZigBee technology makes it best suited for industrial control, home automation, several embedded applications, and so on. ZigBee technology is much simpler and less expensive than other wireless personal area networks (WPANs) such as Wi-Fi or Bluetooth. For various IoT micro sensors, ZigBee is widely used as the communication standard. By passing data through a mesh network of intermediate devices, Zigbee devices can transmit data over long distances to reach more distant ones. Zigbee is typically used in Low data rate applications that require secure networking and long battery life. ZigBee is associated with two roles of hardware and network architectures. There are two types of devices in hardware architectures, a full function device (FFD) node and a reduced function device (RFD) node. FFDs serve as coordinators and communicate with other devices, and can support any network topology architecture. On the other hand, RFDs can only communicate with the coordinator but cannot serve as a coordinator, and only exists in star networks. Electronic devices can communicate through the ZigBee network, when IoT technologies and ZigBee are combined and applied in smart homes. However, the data can be accessed and the statuses of smart objects can be monitored immediately by the user. For master to master or master to slave communications, different network configurations is supported by Zigbee. For building a wider area network, ZigBee networks allow many nodes to interconnect with each other and are extendable with the use of routers. ZigBee serves the three functions of coordinator, router and end device in network architecture. The coordinator is responsible to manage the entire ZigBee network, the role of the router is to extend

the scalability in the entire network, and the end device is responsible for the network end devices. ZigBee communication is divided into 16 channels with 5-MHz intervals numbered from 11 to 26, and operates at the 2.4 GHz Industrial Scientific Medical (ISM) frequency band. The bandwidths of the channel do not overlap. The bandwidth per channel is 2 MHz

IV. SOFTWARE AND HARDWARE IMPLEMENTATION OF AN IOT GATEWAY

A. Hardware and Software Requirements

Hardware:

1. To propose overall architecture for gateway.
2. To design Printed Circuit Board (PCB) Layout for Gateway.
3. Hardware implementation of Microcontroller (ATMega328P), Wi-Fi module (ESP8266) and ZigBee of Gateway on PCB.

Software:

1. To develop a C code for SPI communication between sensor node and Microcontroller in arduino IDE.
2. Log the sensor data onto ThingSpeak (Open source data platform and API for the Internet of Things).
3. Continuous monitoring of real time data.

B. Gateway Hardware

There are already some academic and industrial works on standardization and design of IOT Gateway system. Domestic and international telecom operators have launched related business in applications combining WSN and telecommunications networks, conducted active exploration according to the demands of industrial users. Among the foreign standardization organizations, ETSI M2M TC and 3GPP are all established related standards. ETSI M2M TC's main goal is to do some research on M2M (Machine-To-Machine) standardization, who have already further their works on the existing achievements of 3GPP and ETSI. ETSI M2M TC now focuses on M2M's definition and application examples, with this basis, proceeds business requirements and standardization, but didn't address any specific technology yet. 3GPP launched research team on M2M in 2005. Its main work is to discuss the demands, feasibility and framework. Meanwhile, domestic enterprises also carried out equipment specification work in accordance with the standardization work abroad.

Along the developing route of the traditional IOTGWs, many studies tried to invent novel categories of IOTGWs to pave the way of IOT to exploit current infrastructure by taking new applications and the effects into account. However, the proposed IOTGWs are not consistent in architecture. Eventually, there is not any design guideline worked out from a traffic perspective. Concluded from previous studies, a capable IOTGW, an open research problem, is suggested to have the architecture, where the control signaling standard plays a significant role and information is either processed or transferred by the capable IOTGW. As consequently, the communication detail is known well by an IOTGW and the signaling can be explained well to manage the IOT objectives. Combining these facts with the results that the behaviors in IOTGWs are strongly related to the applications, IOTGW is a suitable point to monitor the effects, which matches well the potential focus we mentioned above. By take this advantage, some innovative projects have been carried out to measure and exploit the traffic characteristics. Furthermore, both function and performance for IOT applications are paid much attention to in the new tide, and they are tried to be introduced to evaluate the effects. Such works form a new measure that can be easily understood as in conventional applications.

C. Wi-Fi Module

The ESP8266 Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor. Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, you can simply hook this up to your Arduino device and get about as much Wi-Fi-ability as a Wi-Fi Shield offers (and that's just out of the box)! The ESP8266 module is an extremely cost effective board with a huge, and ever growing, community.

This module has a powerful enough on-board processing and storage capability that allows it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development up-front and minimal loading during runtime. Its high degree of on-chip integration allows for minimal external circuitry, including the front-end module, is designed to occupy minimal PCB area. The ESP8266 supports APSD for VoIP applications and Bluetooth co-existence interfaces; it contains a self-calibrated RF allowing it to work under all operating conditions, and requires no external RF parts.

D. Flow Diagram

Following flowchart shows operation of data received from sensor nodes and sending to the internet from ThingSpeak platform.

Before sending data to internet, data is checked by checksum bit. Checksum bit is transmitted by sensor and this

 ISSN: 2321-8169
494 – 501

bit again calculated at Gateway. If checksum bit calculated and sent by sensor nodes are equal then data is sent to internet.

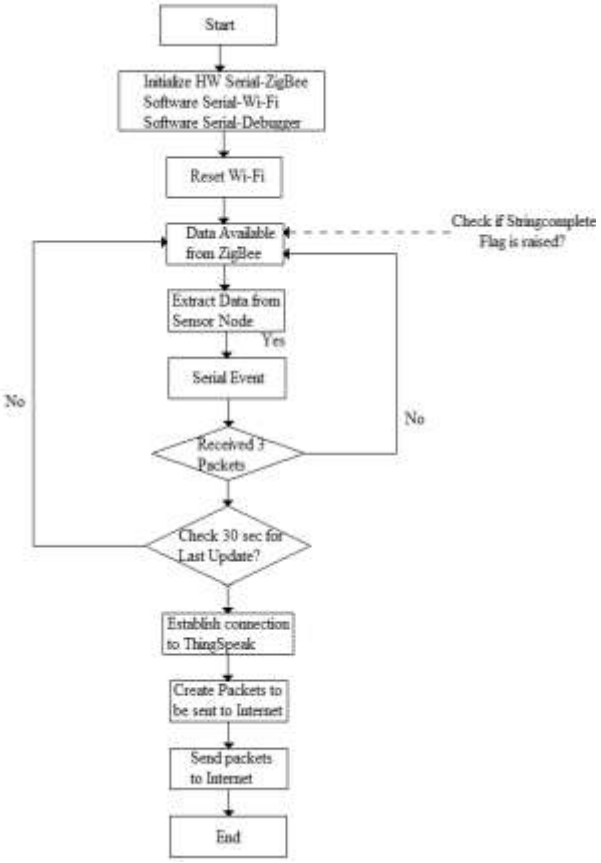

Figure 4.Flowchart of acquiring data and sending to Internet

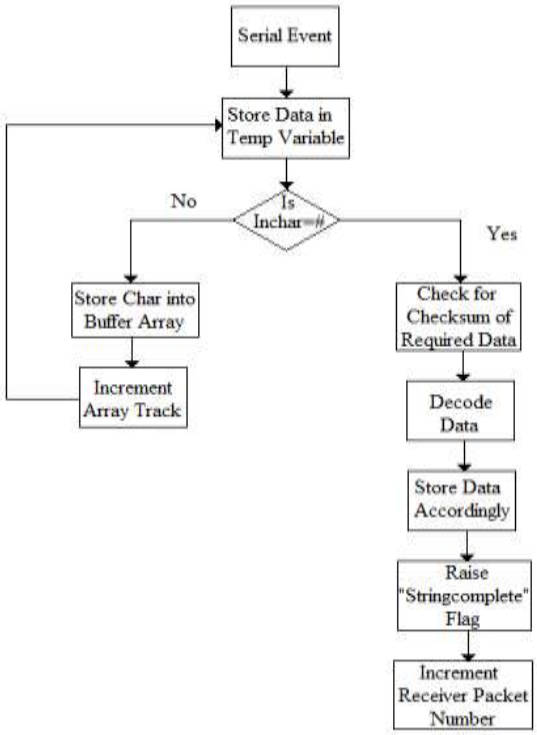

Figure 5. Flowchart of Serial Event

E. Software Implementation

ThingSpeak is a platform providing various services exclusively targeted for building IoT applications. It offers the capabilities of real-time data collection, visualizing the collected data in the form of charts, ability to create plugins and apps for collaborating with web services, social network and other APIs. We will consider each of these features in detail below.

The core element of ThingSpeak is a 'ThingSpeak Channel'. A channel stores the data that we send to ThingSpeak and comprises of the below elements:

- 8 fields for storing data of any type - These can be used to store the data from a sensor or from an embedded device.
- 3 location fields - Can be used to store the latitude, longitude and the elevation. These are very useful for tracking a moving device.
- 1 status field - A short message to describe the data stored in the channel.

To use ThingSpeak, we need to sign up and create a channel. Once we have a channel, we can send the data, allow ThingSpeak to process it and also retrieve the same.

Figure 6.DHT11 Relative Humidity reading

Figure 7.Temperature reading

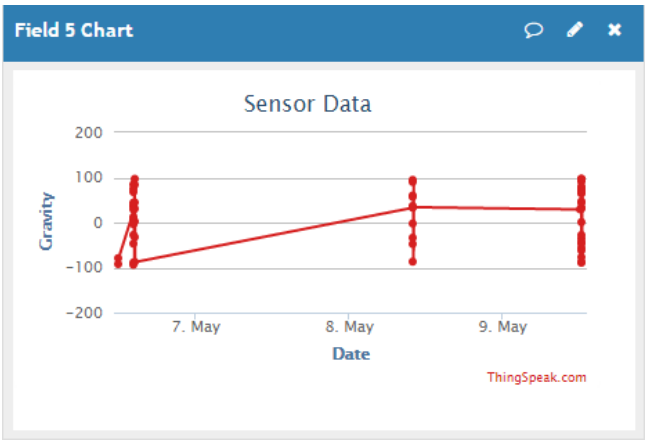

Figure 8.Accelerometer reading

V. CONCLUSIONS AND FUTURE WORKS

Nowadays the internet is very common and is available everywhere and online all time due to its growth in the technology. Sensor node has enabled things to be connected easily due to its low power consumption, flexibility to connect to other devices, low cost, and ease of programming, and thus corresponding information is available globally. The Internet of things (IoT) facilitates the ability to internetwork heterogeneous smart devices easily and ease the availability of data anywhere, with its key features of effective power consumption, scalability and fault tolerance. Internet of Things is the new transformation of the internet and is a fundamental research topic for information technology, embedded area because of its varied application areas and heterogeneous mixture of various communications and embedded technology in its architecture. The aim of the proposed method is to design an IOT Gateway system based on Zigbee and Wi-Fi protocols according to the presented data transmission between wireless sensor networks and mobile communication networks, typical IOT application scenarios and requirements from telecom operators, protocol conversion of different sensor network protocols, and control functionalities for sensor networks, and to give an implementation of prototyping system and system validation.The advantages of the developed system are to have greater control over routing of packets (security and customization) and ability to adapt to other wireless sensor networks.

There is a tradeoff between output power and range for transceivers. Therefore in order to interface, Body Sensor Networks (BSNs) to the cloud for real-time patient monitoring and notification, another transceivers with less output power and less range can be used efficiently.

The developed sensor node can be utilized in developing wireless sensing network in some of the key aspect of Govt. of India's Smart City Project which would boost IOT industry. Few of these are listed as follows:-

1. Smart Parking
2. Smart Urban Lighting
3. Waste management
4. Tele Care
5. Water Management

VI. REFERENCES

[1] Shang Gguoqiang; Chen Yanming; Zuo chao; Zhu Yanxu, “Design and implementation of a smart IOT gateway.” In 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[2] Qian, Z., Ruicong, W., Qi, C., Yan, L., & Weijun, Q. IoT gateway: bridging wireless sensor networks into internet of things. In 2010 IEEE/IFIP 8th International Conference on the Embedded and Ubiquitous Computing (EUC’2010), pages 347-352.

[3] Emara, K. A., Abdeen, M., & Hashem, M. A gateway-based framework for transparent interconnection between WSN and IP network. In EUROCON '09, pages 1775-1780.

[4] L.Wu, Y. Xu, C. Xu, and F.Wang, “Plug-configure-play service oriented gateway for fast and easy sensor network application development,” in Proceedings of the 2nd International Conference on Sensor Networks (SENSORNETS ’13), 2013.

[5] Jong-Wan, Y., Yong-ki, K., Choon-Sung, N., & Dong-Rye, S. Sensor Network Middleware for Distributed and Heterogeneous Environments. In International Conference on New

[6] Shan Yin1, 2, Yueming Lu1, 2*, Yonghua Li1, 3,” Design and implementation of IoT centralized Management model with linkage policy”, IEEE-2015

[7] Zhi-yong Bai; Chin-Hwa Kuo; Tzu-Chia Wang, “Design and implementation of an IoT multi-interface gateway for establishing a digital art interactive system,” Int. J. Ad Hoc and Ubiquitous computing, Vol. 21, No. 3, 2016.

[8] P. Friess and P. Guillemin, "Internet of Things strategic research roadmap," The Cluster of European Research Projects, 2009.

[9] I. f. Akyildiz, Y. Weilian, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, no. 8, pp.102-114, August 2002.

[10] O. corcho and R. Garcia-Castro, "Five Challenges for the Semantic Sensor Web," Semantic Web, vol. 1, no. 1,2, pp.121-125, 2010.

[11] L. Atzori, A. lera and G. Morabito, "The Internet of Things: A Survey," computer Networks, vol. 54, no. 1, pp.2787-2805,2010.

[12] H. Sundmaeker, P. Guillemin, p. Friess and S. Woelffle, "Vision and challenges for realising the Internet of Things," Luxembourg: European Union, 2010.