Architectural Survey of Internet of Things with Research Challenges

Niharika Atri, and Mukesh C. Verma
Department of Computer Science, Uttarakhand Technical University, Dehradun,Uttarakhand,India
Department of Computer Science, Himgiri Zee University, Dehradun, Uttarakhand,India
niharikatri@gmail.com, mukeshverma20@yahoo.com

Abstract: The Internet of Things (IoT) is a computing phenomenon that extends internet interactivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices, machines, everyday objects and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the internet. IoT provides innovative services, new sources of revenue that gives better efficiency and productivity.This work presents an implementable IoT structural system model described as layered architecture, technological challenges related to the structure and future research areas in the domain of IoT.

Keywords- Internet of Things (IoT), Layered Architecture, Protocols, Smart Things**.**

1 INTRODUCTION

The Internet of Things (IoT) is a computing concept where smart machines having unique identities, connects to the Internet and interacts with other machines, everyday objects, environments and infrastructures. They can share data, communicate with each others, which give immediate access to information about the physical world and the objects in it, leading to quality of services. The basic idea of the IoT is that virtually every physical thing in this world can also become a computer that is connected to the Internet.

Internet of Things enables things to be connected anytime, anywhere, with anything and everything ideally using some specific path or network with number of services. Where services can provide security features, techniques for energy-saving, automation, telecommunication, where services notifies and let computers, devices to be integrated into a single system with a shared user interface.

*A.*Smart Cities:

A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. By using digital technologies or information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. Some major areas that can be improved and contribute to the betterment of smart cities are: Structural Health of Buildings, Waste Management, Air Quality, Noise Monitoring, Traffic Congestion, City Energy Consumption, Smart Parking, Smart Lighting, Automation of Public Buildings [1].

1.2 Things:

In the context of "Internet of Things" a "thing" could be defined as a real/physical or digital/virtual entity that can be uniquely identified. Things can be identified either by assigned unique Ids (identification numbers), names and/or location addresses (IP address).

Physical entities have digital counterparts and virtual representation as shown in Fig. 1. Things become context aware and they can sense, communicate, interact and exchange the data.

Figure 1 : Internet of connected things

C. M2M Communication:

A machine to machine communication may take place between two or more devices. Where the communication requires little or no human intervention. The devices can either connect directly to the network or via an m2m gateway [3].

An IoT system can be either M2M or machine to human interaction.

2 ARCHITECTURE:

In this paper, the IoT architecture as layered structure, where all the layers describes their working in the making of an IoT system. Proposed architecture offers six layers where each layer contains basic functions and quality of service can be achieved by suggested protocols.
Each layer with its features is described as following :

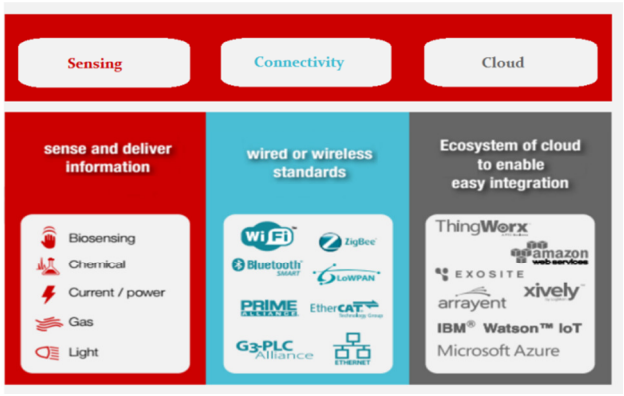

Figure 2: IoT Architecture

2.1 Object Layer

First layer of the IoT model is object layer, which can also be called "thing" layer in IoT terms. object layer (sometimes called hardware layer) includes the main component of IoT, i.e. the "THING".A thing could be real-physical or virtual-digital entity which has an existence. It is the main part of whole IoT concept which is used for collecting Data. A thing can be uniquely identified by an identification number, name, address etc. given by the manufacturer. It should also be able to connect through internet [4] .
We basically include Sensors and Actuators as IoT Things. Where a device which is used as Thing can contain inbuilt sensors. Sensors are the basic "Senses" for a device that is used for collecting any data .The basic aim of this layer is to collect information among physical sensors. Sensors and actuators play a vital role in this layer and performed different functionalities such as location, temperature, weight, motion, etc.

RFID tags and ARDUINO Sensors are mainly named as IoT Things.

A. **RFID Tags** - A technology that was used to track cattle is now one of the fastest emerging technology in the realm of IoT. RFID stands for Radio-Frequency Identification. the ubiquitous Universal Product Code (UPC) bar code is used. It is a small electronic tag/ device that consist of a small chip and an antenna. The chip typically is capable of carrying approx 2,000 bytes of data. RFID tags are intelligent bar codes that can communicate to a networked system to track other devices, products, things [5].

B. **ARDUINO** –It is a small device which contains some sensors and can easily be programmed to make interactive projects. Arduino contains multiple types of sensors like

- Accelerometer, Gyro sensor
- Switches and physical input
- Cameras and vision
- Distance ,range and object detection
- Environment sensor
- Motion, temperature sensor
- Ultrasonic, Pir sensor
- Voltage and current sensors etc.[2]

- ***C.*** **Small OS for IoT:** real-time multi-threading component based open source operating systems with very small memory footprint, low overhead, and very fast execution. They are designed to operate in devices with small limited memory and low processing capabilities. Works with Standard programming in C, C++. Specifications and requirements are very less with devices based on IPV4 or IPv6 networking with RPL routing and less than 5-10 k RAM and 5-30 k ROM. Supports fully standard IPv6 and IPv4, along with the recent low-power wireless standards: 6lowpan, RPL, CoAP, TCP, UDP etc. Contiki, google's BRILLO, RIOT ,TINY OS are some of the examples [6].

D. Challenges to Things

The main issue with IoT things is battery life. When a tag is enabled in wild animals or natural habitats, it will not be provided frequent battery charging. So we need to use devices and system that use very less amount of battery. Some companies like Atmel have developed batteries with 10 years of life. Apart from devices, wireless connectivity tradeoffs like NFC which provides P2P communication, has developed scheme with zero or very low battery consumption.
One solution for the low battery life is using Rechargeable battery using ambient energy harvesting that lasts the life of the battery. Energy Harvesting is achieved by using solar, thermal, wireless/RF Energy Harvesting etc .Energy Harvesting-based power solution cost effective, especially when the life cycle costs of changing batteries are taken into account .

2.2 Communication Layer

2.2.1 Energy efficient wireless standards:

When the data is gathered using things, it need to be sent to other devices. This is done by networking layers.
After collecting data, it need to be sent using a network (Here we talk about wireless network).IoT system can use many networking protocols to share the data.
IoT uses ZigBee,Wi-Fi,Bluetooth smart technologies for connection establishment. These technologies can use some of the protocols like HTTP, CoAP, MQTT etc. These protocols have been built for super high volumes and large networks of things. This uses low energy and provides better connection for large data. One can still find older protocols like FTP, Telnet and SSH, even though they are working very well, they are resource intensive, power intensive, and do not fit well with the low power, unreliable bandwidth of the IoT realm.
But considering the main issues in IoT, In this paper we have included few important protocols namely:

A. Wi-Fi:

Wi-Fi is a wireless networking technology, uses radio waves for providing wireless network connections. The access point (AP) in a wireless network broadcast a wireless signal, which can be detected and then connected by any Wi-Fi certified device [7].
Wi-Fi uses radio frequency band 2.5GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a .

B. Wi-Fi Direct:

Connects devices without internet access
Works good for small range. Gives high throughput, security features then its compotator Bluetooth. Only one device needs Wi-Fi Direct, other end can be Wi-Fi compatible only [2].

C. Bluetooth Low Energy:

Bluetooth low energy (**Bluetooth LE**, **BLE**, marketed as **Bluetooth Smart**) is a wireless personal area network. Bluetooth Smart provides considerably reduced power consumption and less cost while maintaining a similar communication range.
Bluetooth Smart uses the same 2.4 GHz radio frequencies as Classic Bluetooth that let dual-mode devices share a single radio antenna. Features like low power requirements (Serves for months on a single button cell), small size and low cost makes it suitable option for IoT [2].

D. ZigBee:

ZigBee is a specification for a group of communication protocols based on an IEEE 802.15 standard that specifies transmission distances 10-20 meters. Fig. 3 shows the comparison of these layer protocols.

- Provides low-power consumption and open global wireless networking standards focused on monitoring, control and sensor applications.
- Small sensor and mesh network provides self healing mechanism for network.
- Allows products to run on harvested energy or batteries for years with its low-power wireless standards.
- Connects many different types of devices into a single network
- Offers a variety of intelligent features designed to ensure devices communicate in any environment [8].

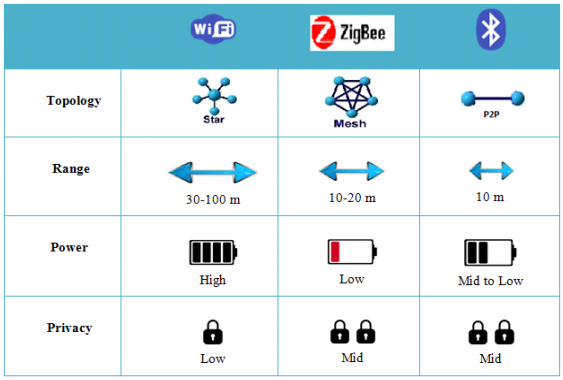

Figure 3: comparing link layer protocols

C. Challenges to Communication::

Network Foundation—limitations of the current Internet architecture in terms of mobility, availability, manageability and scalability are some of the major barriers to IoT .

IoT Elements		Samples
Things		Smart Sensors ,Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication	Communication medium	Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect,
	Address	RFID, 6LoWPAN
Computation	Hardware	Smart Things, Arduino , Phidgets, Intel Galileo , Raspberry Pi, Gadgeteer , BeagleBon , Cubieboard , Smart Phones
	Software	OS (Contiki , TinyOS, LiteOS , Riot OS , Android) Cloud (Nimbits, Hadoop etc.)
Services		Identity-related (shipping), Information aggregation (smart grid) , Collaborative-Aware (smart home) , ubiquitous (smart city)

Figure 4: IoT communicational Architecture

2.2.2 Identification/Addressing :

According to Gartner [13],by 2015 there will be 4.9billion connected things and by 2020 this number will reach 50 billion. These things requires uniquely identified addresses, which can be provided by IPV6 protocol.
IPV6 uses 128 bit addressing and has far big address range that according to Steve Liebson, “we could assign an IPV6 address to EVERY ATOM ON THE SURFACE OF THE EARTH, and still have enough addresses left to do another 100+ earths”.
In particular, Route aggregation is achieved by IPV6 using hierarchical address allocation methods, creates less data and provide limits the expanding routing tables. Technologies like 6LoWPAN and RPL is truly based on IPV6.

A. **6LoWPAN:** is an acronym of IPv6 over Low power Wireless Personal Area Networks. 6LoWPAN is the name of a concluded working group in the Internet area of the IETF. The 6LoWPAN was based on the concept of using IP with even smallest devices that consist of low power and limited processing capabilities [14].
The 6LowPAN protocol is an adaptation layer allowing to efficient IPv6 communication over IEEE 802.15.4 LoWPAN links which uses 802.15.4 in unslotted CSMA/CA. 6LoWPAN achieves low overhead by applying cross layer optimizations. Mesh routing support, Low processing / storage costs are some other advantages of 6LoWPAN .

B. **RPL:** IPv6 Routing Protocol for Low power and Lossy Networks. Low power and Lossy Networks (LLNs) mainly contains constrained nodes, lossy, unreliable and unstable links, typically supporting low data rates, relatively low packet delivery rates. Traffic patterns are not simply point-to-

point, but in many cases point-to-multipoint or multipoint-to-point. Potentially comprising up to thousands of nodes Destination Oriented Directed Acyclic Graph (DODAG), which is routed at a single destination, is built for connecting Network devices.

C. Challenges to identity:

Connection security and privacy is the major concerned in IoT. If you can control the whole IoT system,it can be hacked. **Bootstraping** is one of the developing solution to it. Bootstrapping refers to the process of securely connecting a thing to the Internet of Things. Currently, there are a few protocols which help authenticate nodes.
Protocol for Carrying Authentication for Network Access (PANA), Extensible Authentication Protocol (EAP)
Host Identity Protocol (HIP), Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) etc.

2.3 Application Layer :

End users are directory connected to application layer. This layer is responsible for responding for requested by user .It has the ability to provide smart service to user on high scale. It is delivering the smart services in different verticals like smart hospital, smart school, and industrial automation.
Some of the light weight protocols are described here:

A. CoAP (Constrained Application Protocol)

"CoAP is an application layer protocol that is intended for use in resource constrained internet devices for IoT. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. It is also based on REST architecture. The CoRE (constrained RESTful Enviornment) group of IETF has proposed the following features for CoAP:

- RESTful protocol design minimizing the complexity of mapping with HTTP
- Asynchronous transaction support Low header overhead and parsing complexity
- Simple subscription for a resource, and resulting push notifications,
- Simple proxy and Simple caching based on max-age .
- Constrained machine-to-machine web protocol
- URI and content-type support
- UDP binding (may use IPsec or DTLS)
- Reliable unicast and best-effort multicast support
-

Intended to be used in very simple electronics devices, that allows these devices to interact with each other over the Internet. It is particularly made for small low power sensors, switches, valves and similar components that are controlled through internet [11]. CoAP is designed to occupy the basic features of HTTP with additional special features such as multicast support, low overhead, and simplicity. Multicast, very low overhead, and simplicity are essential features for IoT and M2M devices. These devices that are deeply embedded and consist of very small memory and power than any other traditional internet devices have.
CoAP can run on most of the devices that support UDP, providing a high level of communications security. It makes use of requests and responses messages, using a simple binary base header format. The semantic familiarity with HTTP and the RESTfulness makes CoAP easier than HTTP [2].

Advantages over HTTP:

Less delay: Removes the overhead and complexity of TCP protocol by working on UDP. No retransmission of messages, No connection setup overhead and implementing an optional acknowledgements system. Only best-effort messages transmission.
Less overhead smaller data: TCP requires a three-way handshaking mechanism for establishing a connection however with CoAP data can be sent along with the first packet. In most of the wireless sensing applications which use http stateless mapping, the client side does not store any state information about the established connections and can simply discard incoming packets.
Low Header overhead: The data transmission header is short fixed length binary header of 4 bytes, that reduces further data sent with each packet.
Multicasting: CoAP can also be used with multicasting which allows as opposed to a single server, sensor nodes send their updates to a multicast group. This can be used for a server to simply listen to a multicast group and auto-discover and not require the clients to have prior knowledge of the server.
Security: CoAP is optionally bound to DTLS, providing a high level of communications security [11].

B. MQTT(Message Queuing Telemetry Transport)

is a Publish-Subscribe based light weighted messaging protocol operates on TCP/IP protocol. Also used by Facebook for its mobile messanger.
As an M2M Internet of Things (IoT) connectivity protocol, MQTT is designed to support messaging transport from remote locations/devices involving small code footprints (e.g., 8-bit, 256KB ram controllers), low power, low bandwidth, high-cost connections, high latency, variable availability, and negotiated delivery guarantees.
It is designed for low latency, assured messaging and efficient distribution and connections with remote locations where network bandwidth is limited. The Publish-Subscribe messaging pattern uses a message broker. Based on the topic of message a broker distributes the messages to interested clients [2].
MQTT features faster response and throughput with using lower battery and limited bandwidth.
making it well suited to use cases where:

- internet traffic is intermittent and data rate is highly variable.
after once the connection has been established, Reconnecting to a network (with keep alive interval) is easier and less costly in comparison to HTTP.
- an IoT application needs to machine to machine(M2M) interactions.
- IoT hardware layer need to be reliable by sending data without code retry logic.

For IoT purpose MQTT is integrated with messaging middleware for business enterprises. MQTT is used in enterprise-level applications that push data to mobile apps. The protocol can also be integrated to be used with android apps.

Advantages over http:

- MQTT uses less power supply to maintain an open connection
- Fast and reliable message sending and receiving.
- retained messages and multiple subscriptions 'multiplexed' over one connection.

Disadvantage :
establishing the initial connection when flag cleanstart=true, is not durable and all subscriptions will be removed for the client when it disconnects [12].

2.4 Business Layer :

As users utilize apps and devices continue in IoT systems, significant data will be generated. Which needs significant amount of storage, that can be divided on the depending on two types of data **:**
personal data (consumer-driven) and **big data (enterprise-driven)**.

On the basis of storing structure, IoT data can be stored on local servers as well as cloud, depending on the product. But today much bigger problem is the increased size of data, which cannot be fully resolved using local storage. Other issues can be privacy, compliance and control over each type of data.
Cloud may be one perfect solution for the need of expansive infrastructures to deal with storage, access and management of the data collected by the Things in the IoT system.
Cloud solutions are tools for creating and storing content or information, as well as strategies for where and how to consume it. These solutions are used for creating virtual data storage for large organisations and small consumers to host applications or business functions [15].
Cloud structure provides
flexibility, scalability, compliance, security and sophisticated architecture to support precious data. The current cloud computing technology reduces the energy consumption, and prolongs the battery life of IoT devices.
From the user's perspective, cloud storage can be defined in three simple steps:

2.4.1 **Connect*:***

Integrating data from multiple sources
A front end, real-time system that interacts directly with the IoT devices and sensors. The front end system is for communication purpose, which involves the propagation of query requests from sensors and result as reply to preferably the actuators or other smart objects.

2.4.2 Manage:

Automating the collection of data
A back end system that handles the big data storage and management of IoT data.
The back end is for storage purpose used for
Analyzing data to effectively identify actionable insights
involving the big data storage of produced data from "Things". Later on that data can be processed on depending how the user wants it to be processed.

2.4.3 Access:

Turn raw data into information and actionable insights so that whenever the user needs to access the data, the front end interacts with the back end and retrieve data from the backend storage .

Some cloud solution examples are:
NoSQL solutions. Hadoop, HBase, MongoDB , Cassandra, google AppEngine etc
This layer includes end user access to applications by which a user can operate, read, write, share or utilize the data [16]. There are many tools to do so.here are some tools which provides user API, cloud, IDE, hardware and software support etc. To build the whole IoT system, they provide open source business model. ARDUINO, nimbits, ECLIPSE IDE, ThingSpeak, zatar are some of them.

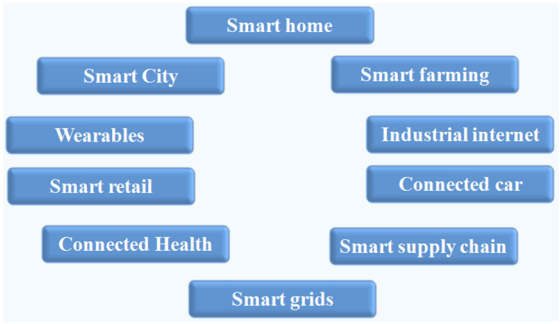

Figure 5. IoT services

3 CONCLUSIONS:

For the better future of IoT, in this paper we have defined a suitable layered architecture. This architecture involves some of the best and optimal protocols used in different levels ultimately enhancing the performance of the whole system. Offered architecture also considers about the problems and issues related to these layers, contributing the present resources and consider the future technology in IoT systems.

4 FUTURE RESEARCH DIRECTION:

In this transformational technology, innovation never ceases. There are areas where research is ongoing in the near future:

- Scalability in networking, storage and computation to handle exponential growth of data volume from sensors
- Interoperability among sensor data sources (physical communication level, network level, data syntax level, and data semantics level)
- Better analytics and visualization (generic, sensor-specific, and domain-specific) provided in real-time, as required
- Distributed intelligence (data representation, object virtualization, multi agent system co-ordination)
- Communication management : energy harvesting, low energy computing architectures, near field communication etc.
- Security: trusted plateforms, data security, confidentiality, authentication, Identity management privacy, low complexity encryption etc.
- Preservation of privacy of the user data and properly balancing between privacy and utility

5 REFERENCES:

[1] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, "Internet of Things for Smart Cities", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014, 2327-4662

[2] Wikipedia

[3] Roberto Minerva,Abyi Biru,Domenico Rotondi, "Towards a definition of the Internet of Things (IoT)"Revision 1 – Published 27 MAY 2015, iot.ieee.org

[4] Yen-Kuang Chen, "Challenges and Opportunities of Internet of Things " ,Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific,IEEE,Jan. 30 2012-Feb. 2 2012 Page(s):383 – 388,ISSN :2153-6961

[5] Kevin Bonsor, Candace Keener and Wesley Fenlon," How RFID Works", available at http://electronics.howstuffworks.com/gadgets/high-techgadgets/rfid.htm

[6] Baccelli, Emmanuel and Hahm, Oliver and Günes, Mesut and W{\"a}hlisch, Matthias and Schmidt, Thomas C, "OS for the IoT-Goals, Challenges, and Solutions", 2013

[7] Beal, Vangie, Wi-Fi—Wireless Fidelity, 4 pages. Last accessed Mar. 13, 2015
at: http://www.webopedia.com/TERM/W/Wi—Fi.html

[8] IoT Meets ZigBee By Gary Audin | November 13, 2014

[9] Leonard Richardson , Sam Ruby, "RESTful Web Services", O'Reilly Media, Inc. year- 2008

[10] Dr. M. Elkstein, Learn REST: A Tutorial 2015, http://rest.elkstein.org/

[11] Z. Shelby, Sensinode, K. Hartke, "Constrained Application Protocol (CoAP)," draft-ietf-core-coap-18. [2013-06--28] http://tools.ietf.org/html/draft-ietf-core-coap-18

[12] Hunkeler, Urs and Truong, Hong Linh and Stanford-Clark, Andy ,"MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks", Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on IEEE , pages-791--798, year-2008

[13] Gartner http://www.gartner.com/newsroom/id/2905717

[14] Hui, Jonathan and Culler, David and Chakrabarti, Samita , "6LoWPAN: Incorporating IEEE 802.15. 4 into the IP architecture",IPSO Alliance White Paper,Vol-3, year-2009

[15] Lori MacVittie, "How Cloud Can Resolve Storage Problems Associated With the Internet of Things", Nov. 2014,http://talkincloud.com/cloud-computing/11242014/cloud-internet-of-things

[16] Bandyopadhyay, Debasis and Sen, Jaydip, "Internet of things: Applications and challenges in technology and standardization", Wireless Personal Communications(springer), vol 58,No 1,year-2011,pages (49-69)