IoT for Everyday Life

Madhavi Dave
Assistant Professor
Department of MCA
Institute of Information & Communication Technology, Indus University, Ahmedabad

Abstract— In today's emerging world of Internet, each and every thing is supposed to be in connected mode with the help of billions of smart devices. By connecting all the devises used in our day to day life, make our life trouble less and easy. We are incorporated in a world where we are used to have smart phones, smart cars, smart gadgets, smart homes and smart cities. Different institutes and researchers are working for creating a smart world for us but real question which we need to emphasis on is how to make dumb devises talk with uncommon hardware and communication technology. For the same what kind of mechanism to use with various protocols and less human interaction. The purpose is to provide the key area for application of IoT and a platform on which various devices having different mechanism and protocols can communicate with an integrated architecture.

Key words: Virtual Private Network (VPN), CoAP, XMPP server

I. INTRODUCTION

As being the global network, IoT need to connect actual and virtual devises with efficient data sharing method, secured data storage using cloud computing and robust inter network connectivity. Iot is responsible to connect millions of objects (things) which can impact major factors like healthcare, home, security, utility and appliances, communication, business, transportation, education, government, science, humanity, retail and emergency services.

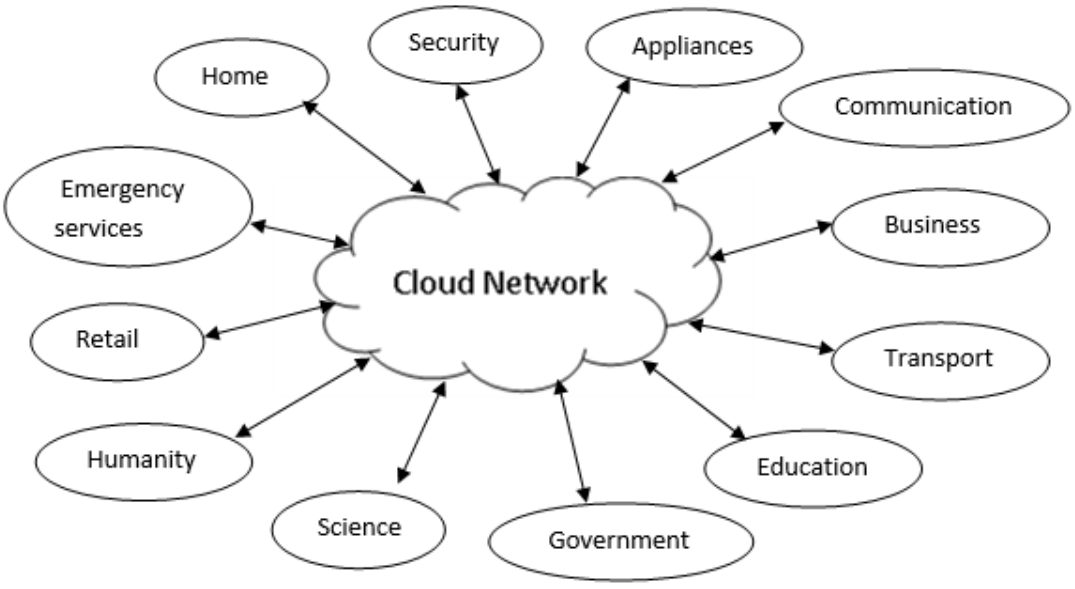

Fig. 1.1: Application areas of Internet of Things

II. REAL TIME APPLICATION

The applications used for Internet are growing by each day and to utilize it properly, they are classified according to its usage. The category domains are,

- Personal / Home
- Mobile
- Utilities
- Business

For Home appliances, mostly WiFi network and sensors are used to connect the devices. The IoT servers are connected with the applications using Apple, iOS, Windows OS, Google Android, etc which are installed and gather raw data from devices. Sore security paradigm also required using the shared cloud for using same information from server and all devices are authenticated to use data from that cloud. The sensors and other devices like refrigerator, air conditioner, and security alarm are connected with cloud so it can take actions for energy savings or other operations.

Mobile communication and its data sharing mechanism are different than other domains thus it is categorized as separate unit of research. Bluetooth and cellular network systems are widely used to connect mobile phones, hands free devices,

positioning systems, etc. With current scenario retails, entertainment, communication and other functionalities can be connected easily with smart mobile devices. It also plays an important role for tracking system for any logistics.

Utilities can be considered for optimal use or allocated resources. Any organization implements utilities to switch between available feasible options, for e.g. any organization can select internet usage medium from Wifi, cellular or any other provided network as per the availability so the resources can be used minimal and profit can be maximized.

For any business or enterprise, some applications are installed for environmental settings. Basic workshop setting, climate change control, security issues, operation for product design and management are the functions which need surveillance of technology under IoT. Local business and government body may have different requirements and thus its setup for the system of Iot.

III. CONTROL INTERFACE

Since IoT applications are required to run on different devices using their own sensors as shown in below figure, the main control to handle all devices would be user's smart phone or any other control which user can carry for remote access. The control interface can be one easily operable UI which can run all application away from home or any work area. The UI should be able to handle various applications with its criteria of functional operation. For example, UI application on smart phone can give you information about traffic, home air condition, health monitoring, pressure of your factory's boiler, etc.

IV. SOFTWARE AND ROBUST APPLICATION

The important role for IoT applications to have smart devices which are required to have smart software to run the functions. Hardware (device) provides the capability for connection of sensor and internet, whereas software provides platform for implementing intelligence to that hardware device. Software assures that the hardware to function properly regardless of any operating environment. The robust system using wireless network can be implemented only with the help of proper software which ensure to send and receive messages, act upon those messages, take decisions depending on the environment, throw exceptions if anything went wrong and resolve the issues without much human intervention.

In today's application driven era, wireless network and sensors have provided the base but the data captured by sensors are meaningless until we know what to do with that data. Thus software enhances communication facility among devices that all connected hardware can share the data and can maintain its functionality. The software need to work on abstract level so any device can install it without worrying about underlying technology. It provides all devices to work on same application layer irrelevant of their transport or any other device details.

V. DATA SECURITY

The journey of internet from closed group of communication to open for accessing all public networks is accelerating at alarming speed. Here the alarm is for making our private data secure from public access and protecting from unauthenticated intruders. As being the embedded system of different types of hardware and software for connection also raise a question mark for unavoidable interference and thus using system with accurate functionality.

Security has been the issue ever since the network had started. Gradually protocols have been invented which can make manageable layered communication. Software with high degree of user authentication mechanism incorporated. While using cloud data, Virtual Private Network (VPN) and its protocols helped to maintain data security which is our highest priority.

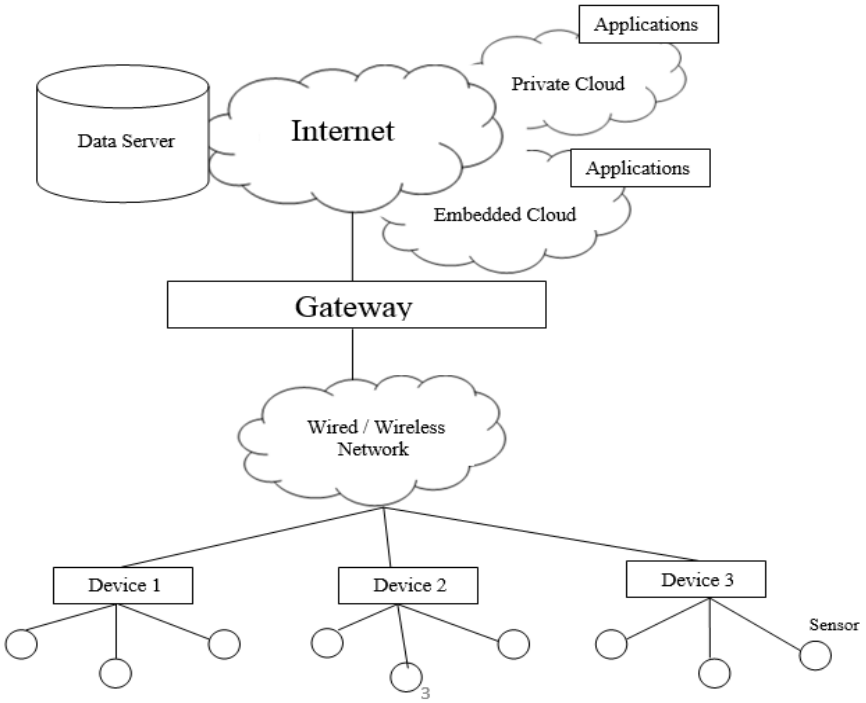

Fig. 5.1: Data Security and Storage in IoT

The system used for home automation, traffic control, heath monitoring, etc are purely embedded devices which have very less storage space and thus it's not appropriate to handle critical task. Also the human interference is very minimal for such devices. For IoT application we require comparatively more storage space and intelligent devices with some human operations.

To overcome such issues, the system needs a connecting device like router or gateway which can integrate all data coming from different embedded devices. These devices are having sensors for accessing and gathering facts from outer environment. The wired or wireless network would connect all devices and then send the data of different formats to one connecting router or gateway. The gateway then stores the data in server and also having various cloud and its appropriate applications to run those devices.

A. Device Authentication

Just as the user requires login name and password before starting any application, device would also need to get authenticated before connecting with the network. Device credentials are stored in its own storage space. The authenticated device reduces the risk of intruder.

B. Access Control

There are different accesses controls can be provided i.e. role based, device based and mandatory. The privileges are given on based the resources can be used by that specific person or device. And if it attempt to use more that what is allowed the all privileges would be rolled back. Any intruders are given minimal access to the shared resources.

C. Firewall

As the embedded devices are having different protocols from each other, the firewall needs to get installed at host side. So the firewall operates at client side helps to find malwares and stop it from getting ahead in the system. It also handles non-IT protocols and communication and data transfer among it.

D. Updates

Software updates and security patches should be installed in such a way that the embedded device need not to compromise on its functionality or services. Some updates makes the system ideal for couple of minutes and thus the functionality of device would suffer. To avoid such trouble, updates and patches need to be implemented in time and without using much bandwidth.

VI. COMMUNICATION ARCHITECTURE

The growth of smart devices in each sector and its massive data requires large and reliable data storage for easy and fast communication. Various devices communicate using different web technologies, thus the integration among them is a major area of research. For example, any sensor gets raw data by sensing the traffic then how it will be converted into knowledge base for the purpose of using the data to reduce traffic and avoid inconvenience. Following are the protocols we are using for communication.

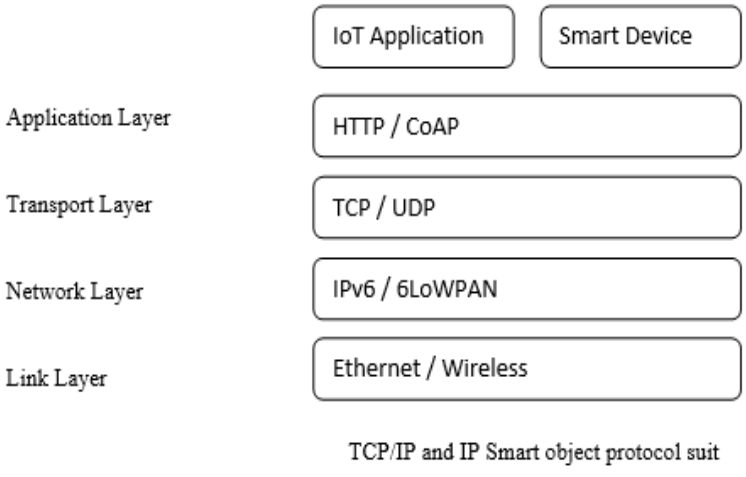

Fig. 6.1: Protocol Suit for Communication Architecture

VII. INTEROPERABILITY THROUGH PROTOCOL

Seamless connection between all devices is the essential requirement for any IoT system. Thus there is no perfect wired / wireless technology that can server across the network without any flaw. At the end of device, the protocols are needed for easy and robust communication. As we mostly use IP protocol for connecting through internet, but it requires high degree of features which is a great overhead for small devices. WiFi can also be used for wireless communication but it is high energy consumers which is again a problem for IoT device.

The ideal combination of technology and application is must for such communication which can be provided by following few application and web protocols and its corresponding layers are shown in above figure.

A. Application Protocol

1) REST API:

Representational State Transfer Application Program Interchange is used for REST web services. REST lies on the top of application layer so can facilitate the user to check the transferred data and allow devices to communicate easily. It allows minimal data to be passed to architecture for working efficiently and shows the user what is necessary.

2) XMPP:

The eXtensible Messaging and Presence Protocol is the TCP protocol based on XML format. The purpose behind using XMPP for IoT application is its working on real time structured message communication between one or more connected devices. Real time communication is the basic necessity of IoT system, thus XMPP is mostly suitable for message transfer.

One more important feature of XMPP is its presence information and contact list maintenance which is again benefit for IoT. XMPP works on decentralized environment so any agent can run their own server and can get message in connected and disconnected mode.

There are few disadvantages of XMPP too. As it is not providing end-to-end encryption while most of the IoT systems requires security for communication. Another drawback is its quality of service (QoS). As it is working as instant messages, the XMPP server will not intimate the device to turn it on for getting message and thus the purpose of the communication may ruined.

B. Web Protocol

1) CoAP:

The Constrained Application Protocol is useful for the devices working on low power sensors and devices need to be controlled by internet. It is invented to work on resource constrained devices to communicate using UDP instead of TCP. The basic client-server model is followed for communication in CoAP for request and response.

CoAP is providing application level QoS for messages as there are received or pending. It also uses RSA key for facilitating basic encryption mechanism. One major disadvantage of CoAP is its one-to-one communication nature. Though with extension one can create a group but it's totally lacking publish-subscriber message queue.

2) MQTT:

Message Queue Telemetry Transport is publish subscribe messaging protocol. It is designed as lightweight structure to save power and memory. MQTT is also having capacity to communicate with constrained device.

The major advantage is having many-to-many broadcast functionality using TCP on simple sending back and forth messages. The drawback of MTQQ is its always on connection, so the devices go in sleep mode sometimes. Another downside is the lack of encryption mechanism for secure communication.

C. Internet Protocol

1) UDP:

User Datagram protocol is connectionless communication protocol. UDP facilitates both multicast and unicast message transmission. It is lightweight protocol and delivers message in time. Disadvantage of UDP is its not providing any flow or error control mechanism like TCP.

2) TCP:

Transmission Control Protocol defines a standard for connected devices that how to communicate. It guarantees that a packet will be surely delivered in order it is send. It can be used for communication between different devices and it is industry standard made protocol which can work without any add on. The drawback of this protocol is its heavy to implement with its suit for complete functionality. TCP is also not a real time protocols so takes time before delivering message.

3) IPv6:

Internet Protocol version 6 is internet layer protocol for end-to-end communication of datagram cross different networks. IPv6 facilitate authentication header, thus the security is handled properly. Using IPv6 one can address number of devices because of its large address space. Due to its feature of indentifying traffic, it can provide quality of service (QoS).

4) 6LoWPAN:

6LoWPAN is the acronym of Low power Wireless Personal Area Network. It is adaption layer of IPv6 and inherits the basic functionality of it. It is advantageous for IoT applications because of its small packet size and can work on typically battery operated devices. Its downside is not all routing protocols can be combined with it and its reliability depends on the device.

VIII. INTEGRATED DATABASE

For IoT application the embedded systems gather the data through sensor and automated application stores the data in server. To make the operation smooth, data is integrated as soon as it's generated. Most of the centralized databases implement indexing and classification on automated data. Properly managed IoT data is most valuable when it is connected to other devices and data sources. The success of IoT can be measured only by secure data storage and continuous flow of information.

IX. CONCLUSION

As we are growing with the emerging world of automation gadgets used in day to day life, IoT plays essential role with all its technologies. Number of hardware and software are devices and applications are invented to make human life easier. Different approaches and researches need to be implemented so the finest of the systems and application create IoT environment around us.

ACKNOWLEDGEMENT

The purpose of this document is to give insight about the basic mechanism any IoT system need to incorporate and some technical aspect of emerging technology. Some details have been referenced from books and few web links mentioned below.

REFERENCES

[1] T. He, J. Stankoviv, C. Lu and T. Abdelzaher, A Spatiotemporal Communication Protocols for Wireless Sensor Networks, IEEE Transaction on Parallel and Distribute Systems, Oct 2005.
[2] B. Brummit, B. Meyers, J. Krumm, A. Kem and S. A. Shafer, Easyliving: Technologies for Intelligent Environments, HUC, 2000.
[3] J. Stankovic, A Vision of Smart City in Future, Smart Cities, Oct 2013.
[4] S. Ravi, A. Raghunathan, S. Chakradhar. Temper Resistance Mechanism for Secure, Embedded System, 17th International Conference on VLSI Design, 2004.
[5] John A. Stankovic, Directions for Internet of Things, University of Virginia, 2014.