INTERNET OF THINGS A HANDS – ON APPROACH –
ARSHDEEP BAHGA, VIJAY MADISETTI

Subject Code: 18KP2CS07

V.kayalvizhy

Asst Professor, Kngac, Thanjavur.

Unit I

Chapter 1

Introduction to Internet of Things

1.1 Introduction

Internet of Things (IoT) comprises things that have unique identities and are connected to the internet.

- Existing devises , such as networked computers or 4G enabled mobile phones already have some form of unique identities and are also connected to the internet, the focus on IoT in the configuration, control and networking via the internet of devices or things , that are traditionally not associated with the Internet. These include devices such as thermostats, utility meters, a blue tooth- connected headset, irrigation pumps and sensor or control circuits for an electric car's engine
- Experts forecast that by the year 2020 there will be a total of 50 billion devices/ things connected to the internet.

- The scope of IoT is not limited to just connected things(Devices, appliance, machines) to the Internet.
- Applications on IoT networks extract and create information from lower level data by filtering, processing , categorizing, condensing and contextualizing the data.
- The information obtained is then organized and structured to infer knowledge about the system and or its user, its environment and its operations and progress towards its objectives, allowing a smarter performance.

Definition and characteristics of IoT:

<u>Definition</u>

A dynamic global network infrastructure with self – configuring based on standard and interoperable communication protocols where physical and virtual "things" have identified, physical attributes, and virtual personalities and use intelligent interfaces, often communicate data associated with users and their environment

<u>Characteristics</u>

- Dynamic and self-Adapting:

IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating condition.Ex: Surveillance cameras can adapt their modes based on whether it is day or night.

- Self – Configuring:
  IoT devices may have self-Configuring capability allowing a large number of devices to work together to provide certain functionality .
- Interoperable communication protocols:
  IoT Devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.
- Unique Identity:
  Each IoT devices has a unique identity and a unique identifier.IPaddress, URI).IoT systems may have intelligent interfaces which adapt based on the context, allow communication with users and the environment contexts.
- Integrated into information network:
  IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

1.2 Physical Design of IoT

1.2.1 Things of IoT

The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, Actuating and monitoring capabilities. IoT devices can exchange data with other connected devices and applications (directly or indirectly), or collect data from other devices and process the data locally or send the data to Centralized servers or cloud based applications back ends for processing the data or from some task locally and other task within the IoT infrastructure, based on temporal and space constraints (ie : Memory, processing calibrators, communication latencies and speed and deadlines).

An IoT device may consist of several interfaces connections to other devices, both wired and wireless. These include I)IoT interfaces for sensors II) interfaces for internet connectivity III) memory and storage interfaces IV) audio video interfaces. An IoT Device can collect various types of data from the the onboard or attached sensors, such as temperature e , humidity, light intensity.
IoT devices can also be varied types, for instance, wearable sensors, smart watches, LED light automobiles and industrial machines. Almost all I would advise generate data in Some form or the other which when processed by Data Analytics systems leads to Useful information to guide further actions locally or remotely.

1.2.2 IoT Protocol

Link Layer:

Link Layer protocols determine how the data is physically sent over the networks physical layer or medium(example copper wire, electrical cable, or radio wave). The Scope of The Link Layer is the Last Local Network connections to which host is attached. Host on the same link exchange data packets over the link layer using the link layer protocol. Link layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached.

802.3 Ethernet:

802.3 is a collections of wired Ethernet standards for the link layer. For example 802.3 10BASE5 Ethernet that uses coaxial cable as a shared medium, 802.3.i is standard for 10 BASET Ethernet over copper twisted pair connection, Standards provide data rates from 10 Mb/s to 40 gigabits per second and the higher. The shared medium in Ethernet can be a coaxial cable , twisted pair wire or and Optical fiber. Shared medium carries the communication for all the devices on the network.

802.1- WI-FI:

IEEE 802.3 is a collections of wireless Local area network.(WLAN) communication standards, including extensive descriptions of the link layer. For example 802.11a operate in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band. 802.11ac operates in the 5G hertz band.

802.16 wiMAX:

IEEE 802.16 is a collection of wirless broadband and Standards, including extensive descriptions for the link layer also called WiMAX wimax standard provides a data rates from from 1.5 Mb/s to 1Gb/s the recent update provides data rates of hundred megabits per second for mobile station.

802.15.4 LR-WPAN:

IEEE 802.1 5.4 is a collections of standard for low rate wireless personal area network(LR-WPAN).These standard form the basis of specifications for high level communication Zigbee. LR-WPAN standards provide data rates from 40 k b/ s. These standards provide low cost and low speed Communications for power constrained devices.

2G / 3G / 4G mobile communications:

These are the different generations of mobile communication standards including second generation (2G including GSM and CDMA). 3rd Generation (3G including UMTS and CDMA2000) and 4th generation 4G including LTE.

Network / internet layer :

The network layer are responsible for sending of IP datagrams from the source network to the destination network. This layer Performs the host addressing and packet routing. The datagrams contains a source and destination address which are used to route them from the source to the destination across multiple networks. Host Identification is done using the hierarchy IP addressing schemes such as ipv4 or IPv6.

IPV4: Internet protocol versions for open parents close (IPV4) is there most deployed internet protocol that is used to identify the device is on a network using a hierarchy latest schemes. It uses 32 bit addresses scheme that allows total of 2^{32} address. As more and more devices got connected to the internet. The Ipv4 has succeeded by IPv6.

IPv6: It is the newest versions of internet protocol and successor to IPv4. IPv6 uses 128 bit address schemes that are lost total of 2^{128} are $3.4 * 10^{38}$ address.

6LoWPAN:
IPv6 over low power wireless personal area networks brings IP protocol to the low power device which have limited processing capability it operate in the 2.4 GHz frequency range and provide the data transfer rate off to 50 kb/s.

Transport layer :
The Transport layer protocols provides end-to-end message transfer capability independent of the underlying network. The message transfer capability can be set up on connections, either using handshake or without handshake acknowledgements. Provides functions such as error control , segmentation, flow control and congestion control.

- TCP: Transmission control protocol is the most widely used to transport layer protocol that is used by the web browsers along with HTTP , HTTPS application layer protocols email program (SMTP application layer protocol) and file transfer protocol. TCP is a connection Oriented and stateful protocol while IP protocol deals with sending packets, TCP ensures reliable transmissions of packets in order. TCP also provide error deduction capability so that duplicate packets can be discarded and low packets are retransmitted

.The flow control capability ensures that the rate at which the sender since the data is now to too to high for the receiver to process.
UDP: unlike TCP, which requires carrying out an initial setup procedure, UDP is a connection less protocol. UDP is useful for time sensitive application they have very small data units to exchange and do not want the overhead of connection setup. UDP is a transactions oriented and stateless protocol. UDP does not provide guaranteed delivery, ordering of messages and duplicate eliminations.

Application layer :
Application layer protocol define how the application interfaces with the lower layer protocols to send the data over the network. Data are typically in files, is encoded by the application layer protocol and encapsulated in the transport layer protocol .Application layer protocol enable process-to-process connection using ports.

Http: Hypertext transfer protocol is the application layer protocol that forms the foundations of world wide web http includes, ,commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS etc. The protocol follows a request-response model where are client sends request to server using the http, commands. Http is a stateless protocol and each http request is independent father request and http client can be a browser or an application running on the client example and application running on an IoT device ,mobile mobile applications or other software.

CoAP: Constrained application protocol is an application layer protocol for machine to machine application M2M meant for constrained environment with constrained devices and constrained networks. Like http CoAP is a web transfer protocol and uses a request- response model, however it runs on the top of the UDP instead of TC CoAP uses a client –server architecture where client communicate with server using connectionless datagrams.It is designed to easily interface with http like http,CoAP supports method such as GET, PUT, DELETE .

Websocket:Websocket protocol allows full duplex communication over a single socket connections for sending message between client and server. Websocket is based on TCP and Allows streams of messages to be sent back and forth between the client and server while keeping the TCP connection open. The client can be a browser, a mobile application and IoT device

MQTT :Message Queue Telemetry Transport it is a lightweight message protocol based on public -subscribe model MQTT uses a client server Architecture by the clients such as an IoT device connect to the server also called the MQTT broker and publishers message to topic on the server. The broker forward the message to the clients subscribed to topic MQTT is well suited for constrained and environments.

XMPP: Extensible Messaging and Presence Protocol it is a protocol for real-time communication and streaming XML data between network entities XMPP powers wide range of applications including messaging, presence, data syndication, gaming multiparty chat and voice / voice calls. XMPP Allows sending small chunks of XML data from one network entity to another in real time. XMPP supports both client to server and server –client communication path.

DDS: Data distribution service is the date centric middleware standard for device-to-device machine to machine communication DDS uses a publish subscribe model where publisher example device that generate data create topics to which subscribers per can subscribe publisher is an object responsible for data distributions and the subscriber responsible for receiving published data. DDS provide quality of service (QoS) control and configurable reliability

AMQP: Advanced Message Queuing protocols. it is an open application layer protocol for business messaging. AMQP support point to point and publish -subscribe model routing and queuing. AMQP broker receive message from publishers example devices or applications that generate data and about them over connections to consumers publishers publish the message to exchange which then distribute message copies to queues.

1.3 Logical design of IoT

Logical design of an IoT system refers to an abstract representation of the entities and process without going into low level specification of the implementations .

1.3.1 IoT functional block

An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification , sensing, actuation ,communication and Management.
The function blocks are described as follows
Devices: An IoT system comprises of the devices that provide sensing, actuation, monitoring and control function

Communication: communication block handle the communication systems

Services : An IoT system uses various types of IoT services such as services for device monitoring ,device control services ,data publishing services and services for device Discovery.

Management: Functional blocks provide various functions to govern the IoT system

Security: Security functional block security IoT system and by providing functions such as application authorization message and content integrity and data security.

Application: IoT application provides and interface that the user can used to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyze the processed to data.

1.3.2 IoT communication model

- Request response: Request-response is a Communications model in which the client sends request to the server and the server responds to the requests. when the server receives a request it decides how to respond, if it shows the data retrieved resources definitions for the response , and then send the response to the client. Access to response model is a stateless communication model and each request response per is independent of others the crime and server interactions in the request response model.

- Publish - Subscribe: Respect is a communication model that involve Publishers brokers and consumers. Publishers are the source of data. Publishers send the data to the topics which is managed by the broker. Publishers are not aware of the consumer. Consumers Subscribe to the topic which are managed by the broker. When the broker receives the data for a topic from the publisher, it send the data to all the subscribed consumers.

- Push pull: Push pull is communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumer. Queues help in decoupling the messaging between the Producers and Consumers . It also act as a buffer which helps in situations when there is a mismatch between the rate at which the produces push data and the rate at which the consumers full the data

- Exclusive pair: Exclusive pair is a bi directional, fully duplex communication model that uses a persistent connections between the client and the server. once the condition is setup it remains open until the client sends a request to close the connection. client and server can send messages to each other after connection setup. Exclusive pair is a stateful Communications model and the server is aware of all the open connections.

1.3.3 IoT communication APIs

REST- based communication API:

Representational state transfer is a set of architectural principles by which you can design web service and Web API that focus on a system resources and how resources states and addressed the transferred. REST API follow the request- response communication model.

The REST architectural constraints apply to the components, connectors, and data elements .

- Client server:
  The principle behind the client-server conference separations of concerns for example client should not be concerned with the storage of data which is their concern of the server. Similarly the server should not be concerned about the user interface which is a concern of the client. separation allows client and server to be independently deployed and updated.

- Stateless: Each request from client to server must contain all the information necessary to understand the request , and cannot take advantage of any stored context on the server .

- Catchable: Catch constrain requires that the data within the response to a request be implicitly or explicitly labeled as catchable or non-catchable. Then a client cache is given the right to reuse that response data for later, equivalent requests. completely eliminate some attractions and improve efficiency and scalability.
- Layered system:
  System constraint come off constraints, constrains the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting. Example client cannot tell whether it is connected directly to the end server or to an intermediary along the way system scalability can be improved allowing intermediaries to respond to request instead of tender server.

- Uniform interface:
  Uniform interface constraints requires that the method of communication between client and server must be uniform. Resources are identified in the request and separate from the representation of the resource that are returned to the client. When climbing holds a representation of your resource it has all the information required to update or delete the resource

- Code on demand : Service can provide executable code script for clients to execute in their context.

WebSocket based communication API:

WebSocket API allow bi directional, full duplex communication between client and server. Unlike request-response API allow full duplex communication and do not require new connection to be set up for each message to be sent. Websocket communication begins with connection setup request send by the client to the server. The request is sent over http and the server interprets it as an upgrade request. If the server support protocol response to the website handshake response after the connection setup the client and the server can send data or messages to each other in full duplex model. WebSocket API reduce network traffic and latency as there is no overhead for connection setup and determination records to each message.

1.4 IoT enabling Technologies

It is enabled by several Technologies including wireless sensor networks, cloud computing big Data Analytics, embedded system, security protocols and architectures, communication protocols, web service, mobile internet and semantic search engine .

1.4.1 wireless sensor network

Wireless sensor network (wsn) comprise of distributed devices with the sensor which are used to monitor the environmental and physical conditions. A WSN consists of a number of end nodes and routers and a coordinator. End nodes have several sensors attached to them. End node can also act as a routers. Routers are responsible for routing the data packet from end nodes to the coordinator. The coordinator node collect the data from all the notes coordinator also act as a Gateway that connects the WSN to the internet. IoT systems are described as follows

- Weather monitoring system using WSN in which the nodes collect temperature, humidity and other data which is aggregated and analyzed .
- Indoor air quality monitoring system using WSN to collect data on the indoor air quality and connections of various gases.
- Soil moisture monitoring system using WSN to monitor soil moisture at various location.
- Surveillance systems use WSN for collecting surveillance data(motion detection data)
- Smart grid use wireless sensor network for monitoring the grid at various point.
- Structural health monitoring systems use WSN to monitor the health of structure by writing vibration data from sensor nodes deployed at various points in the structure.

1.4.2 Cloud computing:

Cloud Computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud Computing involves provisioning of computing networking and storage resources on demand and providing these resources as metered services to the users, in a “ pay as you go” model. cloud Computing resources can be provisioned on demand by the user without requiring interactions with the Cloud Service Provider. The process of provisioning resources used automatic Cloud Computing resources can be accessed then it worked using standard access mechanism that provide platform-independent access through the use of heterogeneous client platforms such as workstations laptops tablets and Smartphones the computing and storage resources provided by Cloud Service Provider our food to serve multiple user using multi Tenancy. Multi-tenant aspects on the multiple users to be served by the same physical hardware .
Cloud Computing services are offered to user in different forms

Infrastructure as a service(IAAS) :
IaaS provides the user the ability provision computing and storage resources. These resources are provided to the users as virtual machine instances and virtual storage. Users can start, stop configure and manage the virtual machines instance on the virtual storage using can deploy operating systems and applications on their choice on the actual resources provisions in the cloud . Cloud Service Provider manages the underlying infrastructure.

Platform as a service(PaaS) :
platform as a service provides the user the ability to develop and deploy application in the cloud using the deployment tool application programming interfaces API, software libraries and services provided by the Cloud Service Provider. The Cloud Service Provider manages the underlying cloud infrastructure including servers, network, operating systems and storage .

Software as a service(SaaS) :
Provide the user a complete software applications of the user interface to the application itself . The Cloud Service Provider manage the underlying cloud infrastructure including server, network storage and application software, and the user is unaware of the underlying architecture of the cloud. Applications are provided to the user through a thin client interface example Browser application. SaaS applications are accessed from various client smartphones running different operating system.

1.4.3 Big Data Analytics
Big data is defined as collections of data set whose volume, velocity in terms of its temporal variations)or variety, is so large that it is difficult to store, manage, process and analyze the data using traditional database and data processing tools. Big Data Analytics involving several steps starting from Data cleaning data munging data processing and visualization.
Some examples of big data generated by IoT systems are described as follows
1. Sensor data generated by IoT system such as weather monitoring stations
2. Machine sensor data collected from sensor embedded in Industrial and energy system for monitoring their files and protecting failure
3. Health and fitness data generated by IoT devices such as wearable fitness band.
4. Data generated by IoT system for Location tracking of vehicle.
5. Data generated by retail inventory monitoring system.

Characteristics of data include:

Volume: Through there is no fixed threshold for volume of data to be considered as big data, however the term big data is used for massive scale data that is difficult to store, manage and process using traditional data bases and data processing architecture. The volume of data generated by modern IT, industrial and Healthcare systems for example is a growing exponentially driven by the lowering cost of data storage and processing architectures and the need to extract valuable insights from the data to improve business processes, efficiency and services to consumer.

Velocity: Velocity is another important characteristics of big data and the primary reasons for exponential growth of data velocity of the data of a store how fast the data is generated and how frequently it varies. Modern IT Industrial and other systems are generating data at increasing the highest speeds.

Variety: Variety refers to the forms of the data. Big data comes in for different forms such as structured or unstructured data including text data, audio, video and sensor data .

1.4.1 Communications protocol:

Communications protocols form the backbone of IoT system and enable network connectivity and coupling to applications. Communications protocols allow device to exchange data over the network. These protocols define the data exchange formats and data encoding schemes for devices and routing of packets from source to destination. Other function of the protocol include sequence control flow control and transmissions of Lost packet.

1.4.5 Embedded systems

An Embedded system is computer system that has computer hardware and software embedded perform specific task. In contrast to general purpose computers or personal computers which can perform various types of tasks, embedded systems are designed to perform a specific set of tasks. Embedded system include Microprocessor and Microcontroller memory Ram ROM cache networking units (Ethernet WI-FI adaptor) input/output unit display keyboard , display and storage such as Flash Memory some embedded system have specialist processes such as digital signal processor DSP graphic processor and application.

1.5 IoT levels and Deployment Templates

In this section we define various levels of IoT systems with increasing completely. IoT system comprises of the following components:

1. Device : An IoT device allow identification, remote sensing, actuating and remote monitoring capabilities.
2. Resources : Resources are software components on the device for accessing and storing information for controlling actuator connected to the device also include software components that enable network access for the device .

3. ontroller service: Controller Service is a native service that runs on the device and interact with the web services. Controller service sends data from the device to the web service receive command from the application from controlling the device.
4. Database: Database can be either local or in the cloud and stores the data generated by the IoT device.
5. Web service: Serve as a link between the device, application database and analysis components. Web Services can be implemented using HTTP and REST principles or using website protocol.

   A comparison of restaurant website is provided below:

   Stateless/stateful: Rest services stateless in nature. Each request contain all the information needed to process it. Request are independent of each other. Website on the other hand is stateful in nature where the server maintains the state and is aware of all the open connections.

   Directional / Bi- directional: REST service operate over http and unidirectional. Request is always sent by a client and the server response to the request. And other hand website is a bi directional product server to send message to each other

   Request response / full duplex: REST service follower request response Communications model where the client sends request and the server response to the request. Website and the other hand Allow full-duplex Communications between the client and server, it means both client and server can send messages to can independently.

   TCP connections: For REST Service each http request involves setting up in a new TCP connections Websocket on the other hand involves a single TCP connection over which the client and server communicate in a full duplex mode.

   Headache Overhead: REST service operate over http , and each request is independent of others . Thus each request carries http header which is an overhead. Due to the overhead of http headers, REST is not suitable for real time applications left hand does not involve overhead of headers. After the initial handshake the client and server exchange messages with minimal frame information.

   Scalability: Scalability is easier in this case of the REST services of request are independent And no state information needs to be maintained by the server. Thus both horizontal out and vertical scaling solutions are possible for REST services. For webSockets horizontal scaling can be cumbersome due to stateful nature of the communication. Since the server maintains the state of our connection, vertical scaling is easier for Websocket than horizontal scaling.

   Analysis component: The analysis component is responsible for analyzing the IoT data and generate results in the form which are easy for the user to understand. Analysis of IoT data can be performed either locally or in the cloud. Analyzed results are stored in the local or cloud database.

Application: IoT applications provide an interface that the user can use to control and monitor various aspects of the IoT system. Applications also allow user to view the system status and view the processed data.

1.5.1 IoT level 1:

Level One IoT system has a single node / device that performs sensing and/or actuation, stores data, reforms analysis and the host to the application. Level 1 IoT systems are suitable for modeling low cost and low complexity solutions where the data involving is not big and the analysis requirements are not computationally intensive.

Let us now consider done example of Level 1 IoT system for home automation. This system consists of the single node that allows controlling the lights and appliances in your home remotely . The device used in this system interface with their lights and appliances using electronic relay switches.

The status information of each light or appliance is maintained in a local database. REST service deployed locally Allow retrieving and updating the state of the each light or appliances in the status database.

The controller service continuously monitor the state of each light or appliance and triggers the relay switches accordingly. The applications which is deployed locally has a user interface for controlling the lights or appliances. since the device is connected to the internet, the application can be accessed remotely as well.

1.5.2 IoT level 2:

Level 2 IoT system has a single node that performs sensing and/or actuation and local analysis. Data is stored in the cloud and application is usually cloud based systems are suitable for solutions where the data in world is big, however the primary analysis requirement is not computationally intensive and can be done local itself.

Construct an example of Level 2 IoT system for smart irrigation.

The system consists of the single node that monitor the soil moisture level and control segregation system. The device used in this system collect soil moisture data from sensor the controller service continuously monitor the moisture level. If the monster level drops below a threshold t , the irrigation system is turned on. For controlling the irrigation system actuators such as solenoid valve can be used.. Rest Web Services is used for storing and retrieving data which is stored in the cloud database. A cloud based application is used for visualizing the moisture level over a period of time, which can help in making decisions about irrigation schedules.

1.5.3 IoT Level 3:

Level 3 system has a single node . Data is stored and analyzed in the cloud application is cloud-based. Level 3 IoT system suitable for solutions where the data involved is big and analysis requirements computationally intensive.
Let us considered example of Level 3 IoT system tracking package handling. The system consists of a single node that monitors the vibration level for package being shipped.

The device in the system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller service send sensor data to the cloud in real time using a website service. The data is stored in the cloud and also visualized using a cloud based application.

The analysis component in the cloud can Trigger alert the vibration level become greater than threshold. The benefit of using websocket service instead of the REST service this example the sensor data can be sent in real-time to the cloud. Cloud based application can subscribe to the sensor data feeds for you in the real-time data.

1.5.4 IoT level 4

A level 4 IoT system has multiple notes that perform local analysis. Data is stored in the cloud and application is cloud based, level 4 contains local and cloud based observer notes which can subscribe to and receive information collected in the cloud from IoT devices. Observer node can process information and use it for various applications, however observer notes do not perform any control function. level 4 IoT systems are suitable for solutions where multiple nodes are required the data involved is big and the analysis requirements are computationally intensive.

let us consider an example of level four IoT system for noise monitoring. The system consists of multiple notes placed in different locations for monitoring noise level in an area. In this example with sound sensor. Nodes are independent of each other each node runs in one controller service that sends the data to the cloud. The data is stored in a cloud database the analysis of the data collected from a number of notes is done in the cloud

1.5.5 IoT Level 5:

IoT system has multiple end nodes and one coordinator notes and notes that perform sensing and / or actuation. Coordinator node collects data from the entry and send to the cloud. Data is stored and analyzed in the cloud and applications is cloud based. Level 5 IoT system are suitable for forest fire detection. The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and carbon dioxide levels in a forest. The endnotes in this example are equipped with various sensors such as temperature humidity and to CO_2. The coordinator node collects the data from the end nodes and act as a Gateway that provides internet connectivity to the IoT system. The controller service on the coordinator device sends the collected data to the cloud .The data is stored in the cloud database. The analysis of the data is done in the computing cloud to aggregate the data and make prediction.

1.5.6 IoT Level 6:

IoT Level 6 system has multiple Independent and nodes that perform sensing and / or actuations and send data to the cloud. Data is stored in the cloud and applications is cloud based .

The analytics component analyze the data and store the results in the cloud database. The results are visualized with the cloud based application. The centralized controller is aware of the status of all the end notes and send control commands to the notes.

Let us consider an example of the level 6 IoT system for weather monitoring. The system consists of multiple nodes placed in different location for monitoring temperature, humidity and pressure in an area. The end nodes are equipped with various sensors such as temperature ,pressure and humidity. The end nodes send the data to the cloud in real time using a websocket service .The data is stored in a cloud database. The analysis of the data is done in the cloud to aggregate the data and make predictions. A cloud based applications is used for visualizing the data.

Unit II
Chapter 2
Domain-specific IoT

2.1 Introduction:

Internet of things applications span wide range of Dubai including homes, cities environment, energy systems, retail, logistics, industry, agriculture and health.

2.2 Home Automation:

2.2.1 Smart lighting :

Smart lighting for homes helps in saving energy by adapting the lighting to the ambient condition and switching on/off or dimming the lights when needed. Key enabling technologies for smart lighting include solid-state lighting such as LED light and IP enabled the lights.

For solid state lighting solution both spectral and temporal characteristics can be configured to adapt illumination to various needs. Smart lighting solutions for Home achieve energy saving by sensing the human movements and their environments and controlling the lights accordingly.

Wireless enabled and internet connected lights can be controlled remotely from IoT applications such as a mobile or web application. Smart lights with sensor for occupancy, Temperature Lux level etc can be configured to adapt the lighting based on the ambient conditions sensed, in order to provide a good ambience. In controllable LED lighting system is presented that is embedded with ambient intelligence gathered from a distributed smart wireless sensor network to optimize and control the lighting system to be more efficient and user oriented, A solid state lighting model is implemented on your wireless sensor network that provide services for sensing illumination changes and dynamically adjusting luminary brightness according to user preferences.

2.2.2 Smart Appliances

Modern homes have a number of appliances such as TVs, refrigerator, music system, washer / dryer etc. Managing and controlling these appliances can be cumbersome with the each appliance having its own controls or remote controls. Smart appliance make the management easier and also provide status information to the user remotely.

Examples smart watches /dryers that can be controlled remotely and notify when the washing / driving cycle is complete smart thermostat Allow controlling the temperature remotely and can learn the user preferences smart refrigerator can keep track of the item stored and send update to the user when an item is low on stock.

Smart TV Allows user to search and stream videos and movies from the internet on a local storage drive, search TV channel schedule and fetch news weather updates and other content from the internet.

Open remote is an open source automation platform for homes buildings. Open remote is platform agnostic and works with standard hardware. With OpenRemote, user can control various appliances using mobile or web publications.

OpenRemote comprises of three components - a controller that manages scheduling and runtime integrations between device, a designer that allows you to create both configuration for the controller and create user interface design and control panel that allow you to interact with the devices and control them.

2.2.3 Intrusion Detection:

Home Intrusion detection system used security cameras and sensor such as PIR sensors and door sensor to detect intrusion and raise alert. Alerts can be in the form of an SMS and an email sent to the user.

Advanced systems can even send detailed alert such as an image grab or a short video clip send to email attachment. cloud controlled intrusion detections system is described in that uses location aware services, where the geo location of each node of your home automation system used independently detected and the stored in the cloud in the event of Institutions the cloud services alert the accurate neighbors who are using the home automation system is independently detected and stored in the cloud.

Event of intrusion, the cloud services after the accurate neighbors or local police. In an intrusion detection system based on UPnP technology is described. The system uses image processing to recognize the Institutions and extract institution subject and to generate Universal plug and play instant messaging for alert .

2.2.4 Smoke / Gas Detector

Smoke detectors are installed in home and buildings to detect smoke that is typically and early sign of Fire. Smoke detectors use optical detection class ionization for sampling techniques to detect smoke.

Alerts raised by smoke detectors can be in the form of signals to fire alarm system. Gas detectors can detect the presence of harmful gases such as carbon monoxide liquid Petroleum gas (LPG).

A Smoke / gas detector raise alerts in human was this describing where the problem is send or an SMS or email to the user or the local fire safety department and provide visual feedback on its status the design of the system that detects gas leakage on smoke and it gives visual level indication.

2.3 Cities:

2.3.1 Smart Parking

Finding a parking space during rush hours in crowded cities can be time consuming and frustrating. Further for the more drivers blindly searching for parking spaces create additional traffic conditions for Star smart parking make the search for parking space easier and convenient for drivers.

Smart parking for powered by IoT system that detect the number of empty parking slots and send the information over the internet to smart parking application back ends.These applications can be accessed by the drivers from smartphones, tablets and in car navigation system .

In smart parking sensors are used for each parking slot, to detect whether the slot is empty or occupied. This information is aggregated by your local controller and then send over the internet to the database.

Design and implementation of a prototype smart parking system based on wireless sensor Network Technology with just like a remote parking monitoring ,automated guidance , and departing reservations mechanism .

2.3.2 Smart Lighting :

Smart lighting system for road parks and building can help in saving energy. According to a IEA report, lightening is responsible for 19 % of global electricity use and around 6% of global Greenhouse gas emission.

Smart lighting allows lighting to be dynamically controlled and also adapted to the ambient conditions. Smart lights connected to the internet can be controlled remotely to configure lighting schedules and lighting intensity.

Lighting configuration can be set for different situations such as a foggy day, a festival etc. Smart. Lights equipped with the sensors and can communicate with other lights and exchange information on the sensed ambient conditions to adapt lightening.

2.3.3 Smart Road

Smart roads equipped with sensors can provide information on driving conditions, travel time estimates and alerts in case of poor driving conditions , traffic congestions and accidents . Such information can help in making the roads safe and help in reducing traffic jams .

Information sense to from the roads can be communicated via internet to cloud based applications and social media and disseminated to the drivers who subscribed to such applications.

Distributed and autonomous systems of sensor networks notes for improving driving safety proposed system can provide the drivers and passengers with a consistent view of the road situations of a few hundred meters ahead of them or a few dozen miles away, so that they can react to potential dangers early enough.

2.3.4 Structural Health Monitoring:

Structural health monitoring system uses a network of sensors to monitor the vibrations levels in the structures such as bridges and buildings. The data collected from the sensors is analyzed to assess the health of The structures .

By analyzing the data it is possible to detect cracks and mechanical breakdown, locate the damage to a structure and also calculate the remaining life of the structure. Using such systems advance warning can be given in the case of imminent failure of the structure.

An environmental effect removal based structural health monitoring schemes is an IoT environment is proposed. Since structural health monitoring schemes use large number of wireless sensor nodes which are powered by traditional batteries researchers are exploring energy harvesting Technologies to harvesting ambient energy, such as mechanical vibrations, sunlight and wind.

2.3.5 Surveillance

Surveillance of infrastructure, public transport and even in cities is required to ensure safety and security. City wide surveillance infrastructure comprising of large number of distributed and internet connected video surveillance cameras can be created. The video feeds from surveillance cameras can be aggregated in cloud based storage solutions. Cloud-based video analytics applications can be deployed to search for patterns for specific events from the video feed.

2.3.6 Emergency Response

IoT Systems can be used for monitoring the critical infrastructure in cities such as building , gas and water pipelines, public transport and power substation systems. IoT systems for fire directions, gas and water leakage directions can help in generating alerts and minimizing their effects on the critical infrastructure.

IoT systems for critical infrastructure monitoring enable aggregations and sharing of information is collected from large number of sensors. Cloud based architecture multi model information such as sensor data, audio, video feeds can be analyzed in near real-time to detect adverse event.

Response to alerts generated by such systems can be in the form of alerts sent to the public , re-routing of traffic, evacuation of the affected areas. Traffic management system for emergency services is describe the system adapt by dynamically adjusting traffic lights, changing related driving policies, recommending behavior change to drivers and applying essential security controls

2.4 Environment

2.4.1 Weather Monitoring:

IoT- based weather monitoring system can collect data from a number of sensor attached such as temperature, humidity, pressure etc. and send the data to cloud based application and storage back-ends. The data collected in the cloud can then be analyzed and visualized by cloud based application.

Weather alerts can be sent to the subscribed users from such applications AirPi weather and air quality monitoring kit capable of recording and uploading information about temperature, humidity, air pressure light levels, UV levels, carbon monoxide Nitrogen dioxide and smoke level to the internet .

2.4.2 Air Pollution Monitoring

IoT based air pollution monitoring system can monitor emission of harmful gases (CO2, CO. NO, NO_2) by factories and automobiles using gases and dermatological sensors the collected data can be analyzed to make informed decisions on pollutions control approaches.

In real time air quality monitoring system is presented that comprises of several distributed monitoring stations that communicate via wireless with a backend server using machine to machine communication. In addition sums of GPRS modem and GPS module.

2.4.3 Noise Pollution Monitoring

Due to growing Urban Development, noise levels in cities have increased and even become alarmingly High in some cities. Noise pollution can cause health hazards for humans due to sleep destruction and stress. Noise pollution monitoring can help in generating noise maps for cities.

Urban noise maps can help the policy makers in urban planning and making policies to control noise level near Residency areas, schools and parks. IoT based noise pollution smart metering system use a number of noise monitoring station that are deployed at different places in a city.

The data on noise levels from the stations is collected on server or in the cloud. The data is then aggregated to generate noise map. In noise mapping study for a city is presented which revealed that the cities suffers from serious noise pollution .In the design of smart phone application is described that allows a user to continuously measure noise level and send it to a central server where all generated information is aggregated and mapped to a meaningful noise visualizations map.

2.4.4 Forest Fire Detection

Forest fires can cause damage to natural resources, property and human life. There can be different causes of forest fires including lightening, human negligence, volcanic eruptions and sparks from rock Falls. Early deduction of forest fires can help in minimizing the damage .

IoT based forest fire detection systems can use a number of monitoring nodes deployed at a different locations in a forest. Each monitoring node collects measurements on ambient conditions including temperature, humidity, light levels.

A system for early detection of forest fire is described in that provides early warning of a potential forest fire and estimate the scale and intensity of the fire if it materializes in a forest fire detection system based on wireless sensor networks is presented.

The system uses multi-criteria deduction which is implemented by the artificial neural network. The ANN fuses sensing data corresponding to multiple attributes of your forest fire such as temperature, humidity ,infrared and divisible light to detect forest fire.

2.4.5 River Flood Detection:

River flood can cause extensive damage to the natural and human resources and human life. River flood occurs due to continuous train for which cause the river level to rise and flow rates to increase rapidly. Early warnings of floods can be given by monitoring the water level and flow rate.

IoT based river flood monitoring system uses a number of sensor nodes that monitor the water level using ultrasonic sensors and flow rate using the flow velocity sensors. Data from a number of such sensor nodes is aggregated in a server or in the cloud.

Monitoring applications raise alert when rapid increase in water level and flow rate is detected in a river flood monitoring system is described that measures river and weather conditions through wireless sensor nodes equipped with different sensors. The systems include water level monitoring module, and data processing module that provide flood information is in the form of raw data, predicted data, and video feed.

2.5 Energy

2.5.1 Smart grid is a data communication network integrated with electrical grid that collects and analyses data captured in real-time about power transmission, distribution and consumption. Smart grid Technology provides protective information and recommendations to utilities, their suppliers, and their customers on how best to manage power.

Smart Grids collect data regarding electricity generation (centralized or distributed conceptions (instantaneous or predictive) storage(or conversion of the energy into other forms), distributions and equipment health data.

Smart fleet use high speed, fully integrated two way communication real time information and power exchange. Smart meters can capture almost real time consumption, remotely control the conceptions of electricity and remotely switch off supply when required.

power thefts can be prevented using smart metering by analyzing the data on power generation, transmission and consumption smart grid can improve efficiency throughout the electric system.

Storage collection and analysis of smart grids data in the cloud can help in dynamic smart grids data can improve energy usage levels via energy feedback to user coupled with real-time pricing information.

Real time demand response and management strategies can be used for lowering peak demand and the overall load via appliance control and energy storage mechanism.
Condition monitoring data collected from power generation and transmission system can help in detecting fault and predicting outage.

2.5.2 Renewable Energy System :

Due to the variability in the output from renewable energy sources such as solar and wind integrating them into the grid can cause grid stability and reliability problems. Variable output produces local voltage swing that can impact power quality. Existing grids were designed to handle power flow from centralized to generation source to the loads through Transmission and distribution lines.

When distributed renewable energy sources are integrated into the grid, they create power bidirectional power flow for which the great were not originally designed to handle power flow from temperature generation sources to the loss through transmissions and distribution lines.

When Distributed renewable energy sources are integrated into the grid is a create power bi-directional power flows for which the grid were not originally designed. IoT based system integrated within Transformer at the point of interconnections measures the electrical variables and how much power is fed into the grid.

To ensure the grid stability one solution is to simply cut of the over protections. For wind energy systems, closed-loop controls can be used to regulate the voltage at points of interconnection

2.5.3 Prognostics:

Energy systems (Smart grids, power plants ,wind turbine forms) have a large number of critical components that must function correctly so that the system can perform their operations correctly.
For example a wind turbine has a number of critical components example bearing, turning gears, for instance that must be monitored carefully as wear and tear in such critical components or sudden change in operating conditions of the missions can result in failures. In system such as Power Grids, real time information using specialist electrical sensor is called phasor measurement unit(PMU) substations.

The information received from PMU must be monitored in real time for estimating the state of a system and for predicting failures. Energy system have thousands of sensors that gather real time maintenance data continuously for condition monitoring and failure prediction purposes. IoT based prognostic real-time health management systems can predict performance of machine or energy Systems by analyzing the extent of deviations of the system from its normal operating profiles.

Analyzing massive amounts of maintenance data collected from sensors in energy systems and equipment can provide protections for the impending failures (potentially in real time) so that their reliability and availability can be improved. Prognostic health Management systems have been developed for different energy systems open PDC set of applications for processing of streaming time series data collected from phasor measurement units PMU in real time.

2.6 Retail

2.6.1 Inventory Management :

Inventory management for retail has become increasingly important in recent years with the growing competition. while over stocking of products can result in additional storage expenses and risk understocking can lead to loss of revenue. IoT system using radio frequency identification RFID tags can help in inventory management and maintaining the right inventory levels .

RFID tags attached to the products allow them to be tracked in real time so that the inventory levels can determined accurately and products which are low on stock can be replenished. Tracking can be done using RFID readers attached to the retail store shelves or in the warehouse. An RFID database inventory management system for time sensitive materials is described.

2.6.2 Smart Payments

Smart Payments solutions contact list payments powered by technology such as near field communication and Bluetooth. Near field communication is a set of standards for smartphones and other devices to communicate with each other by bringing them into proximity or by touching them .

Customers can store credit card information in the NFC enabled Smartphones and make payment by bringing the smart phones and make payments by bringing the smart phones near the point of sale terminals . NFC may be used in combinations with Bluetooth, where NFC initiates initial pairing of devices to establish their Bluetooth connections while the actual data transfer takes place over Bluetooth.

2.6.3 Smart Vending Machines

Smart vending machines connected to the internet allow remote monitoring of inventory levels, elastic pricing of products, promotions, and contact less payments using NFC smart phone applications that communicate with smart vending machine allow user preferences to be remembered and the learnt with the time when a user moves from one vending machine to the other and pass the smartphone with the vending machines using specific interface is presented.

Users can save their preferences and favorite products sensor in a smart vending machine monitor its operations and send the data to the cloud which can be used for predictive maintenance. Smart vending machines can communicate with other vending machines in there vicinity and share their inventory levels so that the customers can be routed to the nearest machines in case product goes out of stock in a machine

2.7 logistics

2.7.1 Route Generation and Scheduling

Modern transportation systems are driven by data collected from multiple sources which is process to provide a new services to the stockholders. By collecting large amount of data from various sources and processing the data into Useful information data driven.

Transportation system can provide new services such as advanced route guidance dynamic vehicle routing anticipating customer demand for pickup and delivery problem, for instance route generations and scheduling systems candidate end-to-end using combinations of road patterns and transportation smooth and feasible schedule based on the availability of vehicles.

2.7.2 Fleet Tracking

Vehicle fleet tracking system using GPS technology to track the locations of vehicle in real time. Cloud based fleet tracking systems can be scaled up on-demand to handle large number of vehicles.

Alerts Can be generated in case of deviation in planned routes. The vehicle locations and routes data can be aggregated and analyzed for detecting bottlenecks in the supply chain such as a traffic conditions or route of elements and generations of alternative route and supply chain Optimization in a fleet tracking system for commercial vehicle is described the system can analyze messages sent from the vehicles to identify unexpected incidence and descriptions is between the actual and applied data.

2.7.3 Shipment Monitoring:

Shipment monitoring solutions for Transportation systems allow monitoring the conditions inside container. For example, containers carrying Fresh Food produce can be monitored to prevent spoilage of food.

IoT based shipment monitoring system you sensor such as temperature pressure and humidity for instance to monitor the conditions inside the container and send the data to the cloud where it can be analyzed to detect food spoilage .

The analysis and interpretation of the data in the environmental conditions in the container and food truck positioning can enable more effective routing decisions and their time therefore it is possible to take remedial measures such as the food that has a limited time budget before it get rotten can be rerouted to a closer destinations, alerts can be raised to the driver and the distributor about the transit conditions, such as container temperature exceeding the allowed limit, humidity levels going out of the allowed limit.

For instance, and corrective actions can be taken before the food gets damaged. A Cloud-based frame work for real time fresh Food Supply tracking and monitoring was proposed . For fragile products vibrations levels during shipment can be tracked using accelerometer and gyroscope sensors attached to IoT device.

A system for monitoring container in integrity and operating conditions described. The system monitors the vibrations patterns on their container and its contents to reveal information related to its operating environment and integrity during transport handling and storage.

2.7.4 Remote Vehicle Diagnostics

Remote vehicle diagnostic systems can detect faults in the vehicles warn of impending fault. These Diagnostic system use on-board IoT devices for collecting data on vehicle operation such a speed, engine RPM, coolant temperature, fault code number ,and status of the various vehicle subsystem such data can be captured by integrating on-board diagnostic systems with IoT devices using protocols such as CAN bus.

Modern commercial vehicles support on-board diagnostics OBD standards such as OBD-II. OBD system provides real time data status of vehicle subsystems and diagnostic trouble code which Allow rapidly identifying the fault in the vehicle. IoT based vehicle diagnostic system can send the vehicle data to centralized serves or the cloud where it can be analyzed to generate alerts and suggest remedial actions.

2.8 Agriculture

2.8.1 Smart Irrigation

Smart irrigation systems can improve crop yield while saving water. smart irrigation system using IoT devices with soil moisture sensors to determine the amount of moisture in the soil and realize the flow of water through the irrigation pipe only when the moisture level go below a predefined threshold. Smart irrigation systems also collect Moisture level measurements on a server or in the cloud where they collected data can be analyzed to plant watering schedule.

2.8.2 Green House Control

Green house structures with glass or plastic roofs that provide conducive environment for growth of plants . The Climatological conditions inside a Greenhouse can be monitored and controlled to provide the best conditions for growth of plants. The temperature , humidity, soil moisture, light and carbon dioxide levels are monitored using sensors and their climatological conditions are controlled automatically using actuation devices.

IoT system plays an important role in greenhouse controlled and help in improving productivity. The data collected from various sensors is stored on centralized servers or in the cloud where analysis is performed to optimize the control strategies and also correlate the productivity with different control strategies.

the system uses wireless sensor network to monitor and control the agriculture parameters like temperature and humidity in real time for better management and maintenance of Agricultural production

2.9 Industry:

2.9.1 Machine Diagnosis and Prognosis:

Machine prognosis refers to predicting the performance of a machine by analyzing the data and the current operating conditions and how much deviations exist from the normal operating conditions. Machine diagnosis refer to determining the causes of a machine fault.

IoT plays a major role in both the prognosis s and Diagnostics of industrial machines . Industrial machines have a large number of components that must function correctly for the machine to perform its operations. Sensors in machine can monitor the operating conditions such as temperatures and vibrations levels. The sensor data measurements are done on time scale of few milliseconds to few seconds, which leads to generations of the massive amount of the data.

Case-based reasoning (CBR) is a commonly used method that find solutions to new problem based on past experience. This past experience is organized and represented as case in a case base. CBR is an effective techniques for problem solving in the field in which it is hard to establish a quantitative mathematical model, such as machine Diagnostics and prognosis .

Since foe each machine, data from a very large number of sensors is collected using search high-dimensional data for creation of a case library reduce the case retrieval efficiency. Data reduction and feature extraction methods are used to find the representatives set of ability as the of features.

2.9.2 Indoor Air Quality Monitoring:

Monitoring indoor air quality in factories is important for health and safety of the workers. harmful and toxic gas such as carbon monoxide, nitrogen monoxide and Nitrogen dioxide etc t can cause serious health problems .IoT based gas monitoring system can help in monitoring the indoor air quality using various gas sensors. The indoor air quality can vary for different locations. Wireless sensor networks based IoT devices can identify the other hazardous zones, so that a corrective measures can be taken to ensure proper ventilation

2.10 Health And Lifestyle:

2.10.1 Health and fitness monitoring

wearable IoT devices that are low non invasive and continuous monitoring of physiological parameters can help in continuous health and fitness monitoring. These wearable devices may can be in various forms such as built under wrist bands.

The wearable devices from a wireless sensor networks called body area networks in which the measurements from a number of wearable device are continuously Send to a master nodes such as a smartphone which then send the data to the server or a cloud end for analysis and achieving. Healthcare providers can analyze the collected Healthcare data to determine any health conditions or anomalies.

2.10.2 Wearable Electronics

Wearable Electronics such as smart watches smart glasses wristband and fashion electronics (with electronic integrated in clothing and accessories ,example Google glass for Moto 360 smart watches provide various functions and future to assist us in our daily activities and making as lead healthy Lifestyle .

.

Smart watches the user can search the internet a play audio video file make calls with or without paired mobile phones, play games and use various kinds of mobile applications smart classes allow users to take photos and record videos ,get map directions check flight status and search the internet by using voice commands

Chapter 3

IoT and M2M

3.1 M2M

Machine to machine (M2M) refers to networking of Machines for the purpose of remote monitoring and control and data exchange. The end-to-end architecture for M2M systems comprising of M2M area networks, Communications Network and application domain.

An M2M area network comprises of machines which have embedded hardware module for sensing actuation and communication. Various Communication protocols can be used for M2M local area network such as Zigbee , Bluetooth , Modbus M –bus, wireless, power LINE Communication ,6LoWPAN.

These Communications protocols provide connectivity between M2M nodes within and M2M area network. The Communications Network provides connectivity to remote m2m area network. communication network can use wired or wireless network. The M2M area network use either proprietary or non IP based protocol.

The communication between the M2M nodes and the M2M Gateway is based on the communication protocol. M2M Gateway protocol translation to enable IP connectivity for M2M . M2M Gateway act as a proxy performing translation from / to native protocol to M2M area network.

M2M data is gathered into point solution such as enterprise applications, service management application for remote monitoring applications. M2M has various application domain such as smart metering, Home Automation , industrial Automation, smart grid.

3.3 DIFFERENCE BETWEEN IOT AND M2M

The difference between m2m and IoT are described as follows :

Communication protocols:

M2m and IoT can differ in how the communication between the machines are device happens. M2M uses other proprietary or not IP based communication protocol for communication with in the M2M area networks. Commonly uses M2m protocol include zigbee, Bluetooth, ModBus, wireless M-Bus ,power line communication.

The focus of communication in M2M is usually on the protocols below the network layer. Focus of communication in IoT is usually a protocol in network layer such as http web sockets, MQTT, XMPP, DDS, AMQP.

Machines in M2M vs Things in IoT:

The " things " IoT refers to Physical objects that have unique identifier and can sense and communicate with the external environment or their internal physical status. The unique identifiers the things in IoT are the IP addresses. Things have software component for accessing processing and storing sensor information on controlling actuator connector. IoT system can include IoT devices of various types such as fire alarms , door alarms, lighting control devices.

Hardware versus software emphasis:

while the emphasis of M2M is more on hardware with embedded modules, the emphasis modules, the emphasis of IoT is more on software . IoT devices run specialist software sensor Data Collection, data analysis and interfacing with cloud through IP based communication.

Data collection and analysis:

M2M data is collected in point solutions and often in on premises storage infrastructure. In contrast to M2M,the data in IoT is connected in the cloud. The analytical component analysis the data and stores the result in the cloud database. Data and analysis results are visualized with the cloud based applications. The centralized controller is aware of the status of all the nodes and send Control Commands to the nodes.

Applications:

M2m data is collected in point solutions and can be accessed by on premises application diagnosis applications, service management applications , and on-premises enterprise application.

3.4 SDN and NFV for IoT :

Software defined networking(SDN) and the network function virtualization(NFV) and their applications for IoT.

3.4.1 Software Defined Networking:

Software defined networking(SDN) is the networking architecture that separates the control plan from the data plan and centralizes race the network controller. Conventional network architecture build with specialized hardware (switches, router etc).

Network device in conventional architectures are getting exceedingly Complex with the increasing number of distributed product has been implemented and the use of proprietary hardware and interfaces. Control plan is the part of the network that carries the signal and routing message traffic while the data plan is a part of network that carries the payload data traffic.

The limitations of the conventional network architecture as follows:

Complex network devices:

Interoperability is limited due to the lack of standard and open interfaces. Network devices use proprietary hardware and software and have slow product lifecycle limiting innovations . The convention networks were well suited for static traffic pattern and had a large number of product was decided for specific applications .which are applied in cloud computing environment traffic patterns are more dynamic. Due to complexity of conventional network devices making changes in the networks to meet the dynamic traffic pattern has become increasingly difficult.

Management overhead:
conventional networks involve significant manager overhead. Network managers find it increasingly difficult to manage multiple network devices and interfaces from multiple vendors. Up gradation of network configuration changes in multiple devices.

Limited scalability:
The Virtualization technologies used in cloud computing environment has increased the number of its host repairing network access Iot applications hosted in the cloud are distributed across multiple virtual machines that require exchange of traffic.

Components of IoT applications run distributed algorithms on a large number of virtual machine that require huge amounts of data exchange between virtual machines.

Such computing environment require highly scalable and easy to manage network architectures with minimal manual configuration which is becoming raising a difficult with a conventional networks.

key Elements of SDN and follow:

Centralized network controller:

with Decoupled control and the data plan and centralized network controller, the network administrator can rapidly configure the network. SDN applications can be deployed Programmable open API. This speed have innovation as the network status no longer need to wait for other device vendors to embed features in their proprietary hardware.

Programmable open APIs:

SDN architecture propose Programmable open API for interface between the SDN application and control layers with these open API is various network services can be implemented such as routing quality of services access.

Standard communication interface(Open Flow)

SDN architecture uses a standard communication interface between the control and infrastructure layers. openflow, which is Defined by the open networking Foundation is the broadly accepted SDN protocol for the southbound interface. Open flow,the forwarding plan of the network devices can be directly accessed and manipulated.

Open floor uses the concept of close try different network traffic based on three different rules. Floor can be programmed statically and dynamically by the SDN controll software. Components of and openflow switch comprising one or more tables and their group table which perform packet lookup and forwarding, and open flow channels to an external Controller System openflow protocol is implemented at both sides of the interface between the controller and the network devices.

3.4.2 network function virtualization:

Network function virtualization is a technology that leverages virtualization to consolidate the heterogeneous network devices on to industry standard high-volume service switches and storage. NFV is complementary to SDN as NFV can provide at the infrastructure on which SDN can run. NFV and SDN mutually beneficial to each other but not dependent. Network functions can be virtualized without SDN which very beneficial to each other but not dependent

Elements of architecture as follows:

Virtualize to network function VNF:

VNF is a software implementations of a network function which is capable of running over the enough Infrastructures

NVF Infrastructure NFVI:

It into Computer Network and storage resources that are visualized.

NFV management and orchestrations: Orchestrations focuses on all visualization specific management task and the covers the orchestrations and lifecycle management of physical and / or software resources that support the infrastructure utilization and the lifecycle management of VNF.

NFV comprises of network functions implemented in software that run on Virtualized resources in the cloud. NFC enabled separations of network function which are implemented in software from the underlying hardware.