INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN

IoT & its applications in AI

ASSIGNMENT

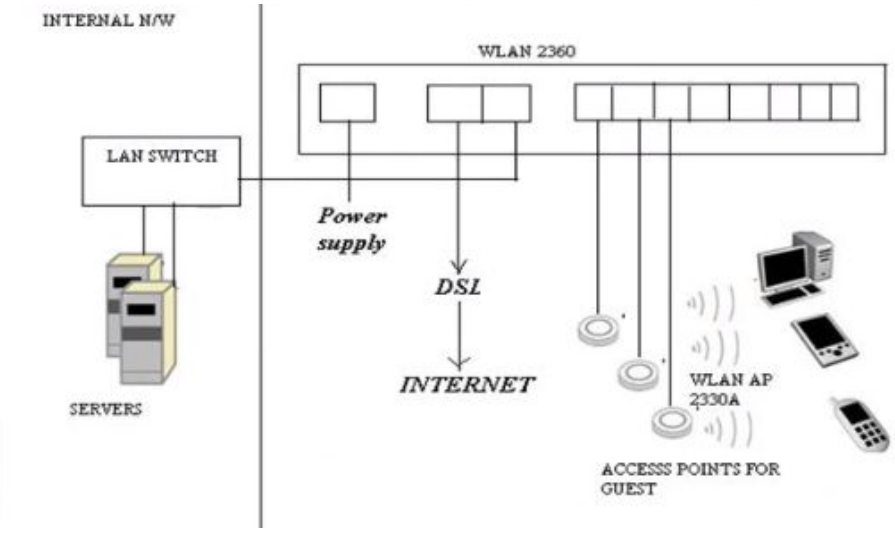
Submitted By:
Anamika Rai
Roll No.- 02802102019
M.Tech. CSE (2nd Semester)

Submitted To:
Prof. SRN Reddy

Q 1. Explain and draw the architecture of WiFi, Bluetooth, and Zigbee.

WiFi

- Wi-Fi is a popular wireless networking technology(alternative to Wired Technology). Wi-Fi stands for “wireless fidelity”.
- Wi-Fi was invented by NCR Corporation/AT&T in the Netherlands in 1991. Wi-Fi (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (WLANs).
- Wi-Fi networks connect computers to each other, to the internet and to the wired network.
- Wi-Fi Networks use Radio Technologies to transmit & receive data at high speed:
  - ➢ Wi-Fi-802.11a
  - ➢ Wi-Fi-802.11b
  - ➢ Wi-Fi-802.11g
  - ➢ Wi-Fi-802.11n



WiFi Architecture

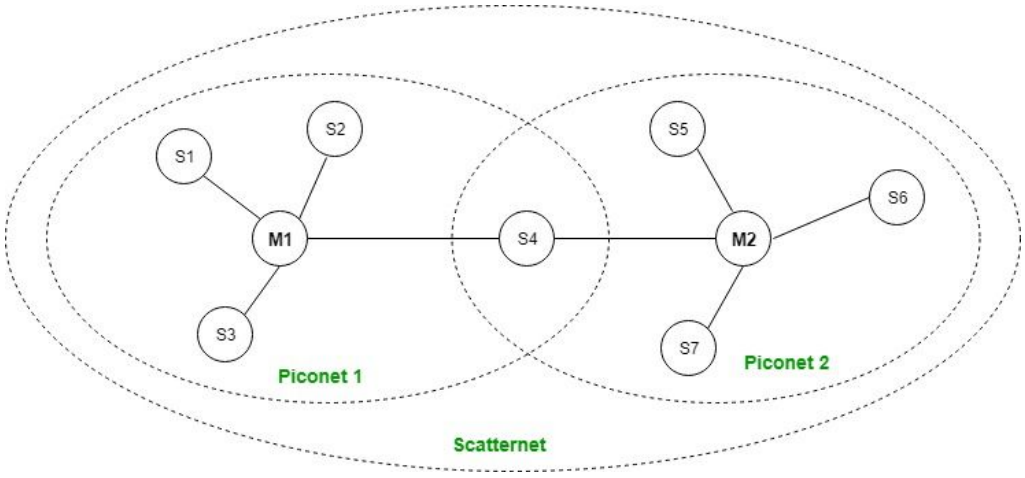
- A Wi-Fi hotspot is created by installing an access point to an internet connection.
- An access point acts as a base station.
- When a Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.
- A single access point can support up to 30 users and can function within a range of 100 – 150 feet indoors and up to 300 feet outdoors.
- Many access points can be connected to each other via Ethernet cables to create a single large network.

Bluetooth

- Bluetooth is a short-range and low power wireless technology originally developed for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs).

- This technology was invented by Ericson in 1994.
- It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz.
- Maximum devices that can be connected at the same time are 7.
- Bluetooth ranges up to 10 meters. It provides data rates up to 1 Mbps or 3 Mbps depending upon the version.
- Bluetooth uses a radio technology called Frequency-hopping spread spectrum(FHSS).
- A Bluetooth network is called a **piconet** and a collection of interconnected piconets is called **scatternet**.

Bluetooth Architecture



Piconets- When more than two Bluetooth devices communicate with one another, this is called a piconet.

- Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave; the specification allows a mechanism for master and slave to switch their roles. And all traffic must pass through the master.
- The device that initializes the establishment of the Piconet becomes the master.
- It can contain up to seven slaves clustered around a single master.

Scatternet- A set of two or more interconnected piconets form scatternets.

- A Bluetooth unit can be a slave in two or more piconets, but it can be a master in only one.
- Devices that participate in two or more piconets may act as “gateways.”
- Bluetooth units can only transmit and receive data in one piconet at a time.
- Piconets may be identified by the master's identity and clock.
- Devices give notification of inactivation to master before becoming inactive in its piconet for a finite length of time.

Zigbee

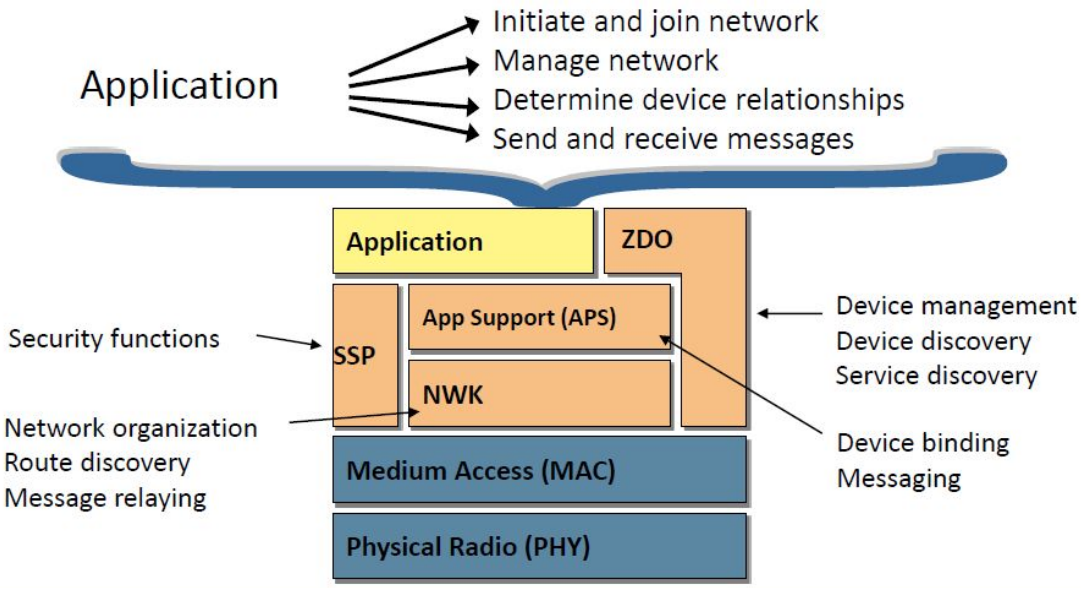
Zigbee technology is built on IEEE standard specification for Wireless Personal Area Networks (WPANs). It is an open standard, packet-based protocol used for more reliable, low power

wireless networks.

- They are designed to operate at 868MHz, 902-928 MHz and 2.4 GHz frequencies that require a low data transfer rate of 250 Kb/sec across 16 different channels.
- The range of Zigbee is between 10 meters and 100 meters. Its wireless networking is simpler to design, less expensive, highly stable and offers more secure networking.
- The discovery of the Zigbee protocol has successfully eliminated the risk of single-point signal failures.

Zigbee architecture (also known as Zigbee Stack)

There are major four layers available in ZigBee stack which are the physical layer, Media access layer, Network layer, and application layer.



Physical Layer: This layer does modulation and demodulation operations upon transmitting and receiving signals respectively. This layer's frequency, data rate and the number of channels.

MAC Layer: This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidances (CSMA). This also transmits the beacon frames for synchronizing communication.

Network Layer: This layer takes care of all network-related operations such as network setup, end device connection, and disconnection to network, routing, device configurations, etc.
Application Support Sub-Layer: This layer enables the services necessary for Zigbee device objects and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

Application Framework: It provides two types of data services as key-value pairs and generic message services. The generic message is a developer-defined structure, whereas the key-value pair is used for getting attributes within the application objects. ZDO provides an interface

between application objects and APS layers in Zigbee devices. It is responsible for detecting, initiating and binding other devices to the network.

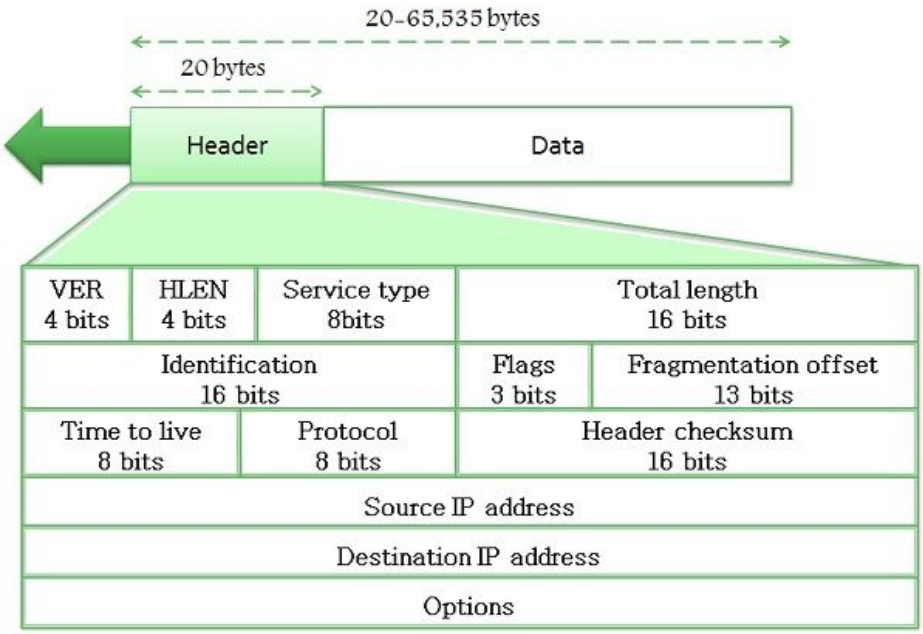
Q 2. Differentiation between WiFi, Bluetooth, and Zigbee.

	Bluetooth	ZigBee	Wi-Fi 802.11
Data rate	1 Mbit/s	20, 40, and 250 kbits/s	11 and 54 Mbits/s
Range	10 m	10 to 100 m	Up to 100 m
Networking topology	Ad-hoc, small networks	Ad-hoc,peertopeer, star, or mesh	Point to hub
Frequency	2.4 GHz	868 MHz (Europe), 900 to 928 MHz (North America), 2.4GHz(worldwide)	2.4 and 5 GHz
Power consumption	Low	Very low	High
Typical applications	Inter-devicewirelesscon-nectivity, e.g., phones, PDAs,laptops,headsets, cameras, printers, serial cable replacements	Industrial control and monitoring, sensor networks, buildingautomation, toys, games	Wireless local-area network (WLAN) connectivity, broadbandInternet, security cameras

Q 3. Draw and explain the datagram header of IPv4 and IPv6. Differentiation between IPv4 and IPv6.

IPv4

- IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is the most widely used IP version. It is used to identify devices on a network using an addressing system.
- The IPv4 uses a 32-bit address scheme allowing it to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic.



Packet Format

An IPv4 datagram is a variable-length packet consisting of a header (20 bytes) and data (up to 65,536 along with header). The header contains information essential to routing and delivery.

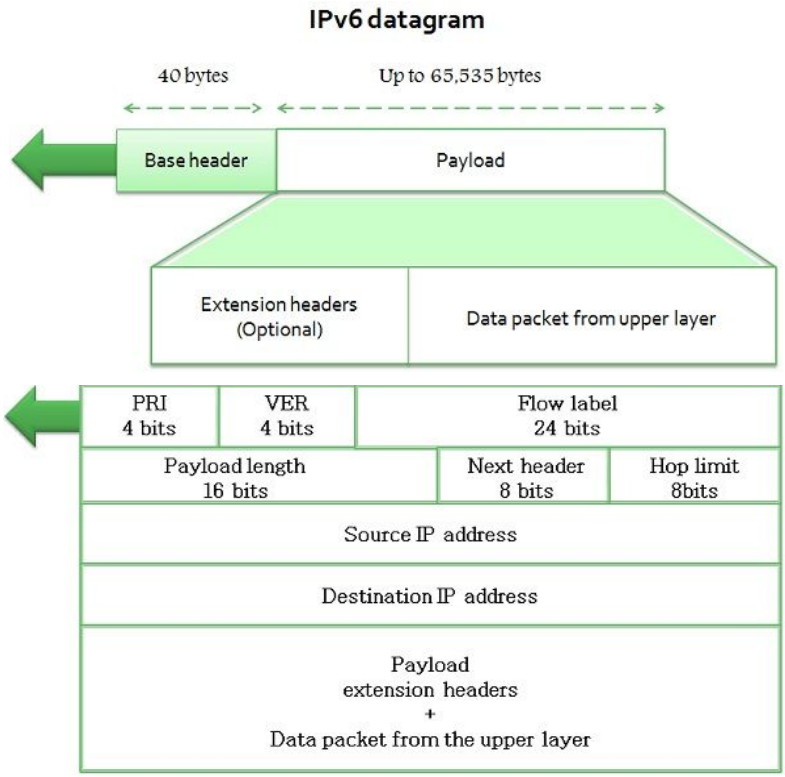
Base Header

- **Version:** It defines the version number of IP, i.e., in this case, it is 4 with a binary value of 0100.
- **Header length (HLEN):** It represents the length of the header in multiple of four bytes.
- **Service type:** It determines how datagram should be handled and includes individual bits such as level of throughput, reliability, and delay.
- **Total length:** It signifies the entire length of the IP datagram.
- **Identification:** This field is used in fragmentation. A datagram is divided when it passes through different networks to match the network frame size. At that time each fragment is determined with a sequence number in this field.
- **Flags:** The bits in the flags field handles fragmentation and identifies the first, middle or last fragment, etc.
- **Fragmentation offset:** It's a pointer that represents the offset of the data in the original datagram.
- **Time to live:** It defines the number of hops a datagram can travel before it is rejected. In simple words, it specifies the duration for which a datagram remains on the internet.
- **Protocol:** The protocol field specifies which upper-layer protocol data are encapsulated in the datagram (TCP, UDP, ICMP, etc.).
- **Header checksum:** This is a 16-bit field to confirm the integrity of the header values, not the rest of the packet.
- **Source address:** It's a four-byte internet address that identifies the source of the datagram.
- **Destination address:** This is a 4-byte field that identifies the final destination.

- **Options:** This provides more functionality to the IP datagram. Furthermore can carry fields like control routing, timing, management, and alignment. IPv4 is a two-level address structure (net id and host id) classified into five categories (A, B, C, D, and E).

IPv6

An IPv6 address is a 128-bit binary value, which can be displayed as 32 hexadecimal digits. Colons isolate entries in a sequence of 16-bit Hexadecimal fields. It provides 3.4 x 1038 IP addresses. This version of IP addressing is designed to fulfill the needs of exhausting IP's and providing sufficient addresses for future Internet growth requirements.



Packet format

Each packet consists of a mandatory base header succeeded by the payload. The payload includes two parts namely optional extension headers and data from an upper layer. The base header consumes 40 bytes, inversely the extension headers and data from the top layer usually hold up to 65,535 bytes of information.

Base Header

- **Version:** This four-bit field specifies the version of the IP, i.e., 6 in this case.
- **Priority:** It defines the priority of the packet concerning traffic congestion.
- **Flow Label:** The reason for designing this protocol is to facilitate special control for a certain flow of data.
- **Payload length:** It defines the total length of the IP datagram accepting the base header.

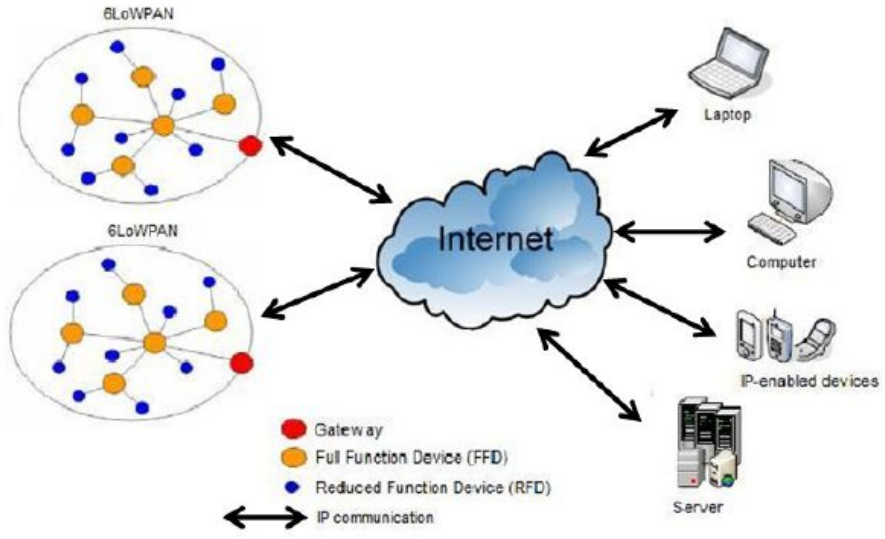
- **Next header:** It's an eight-bit field describing the header that trails the base header in the datagram. The next header is one of the optional extension headers which IP uses or the header for an upper-layer protocol such as UDP or TCP.
- **Hop limit:** This eight-bit hop limit field assists with the same functions at the TTL field in IPv4.
- **Source address:** It is a 16 bytes internet address that identifies the source of the datagram.
- **Destination address:** This is a 16-byte internet address that generally describes the final destination of the datagram.

Differences Between IPv4 and IPv6

- IPv4 is a 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
- IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
- IPv4 has checksum fields while IPv6 doesn't have checksum fields
- IPv4 supports VLSM (Virtual Length Subnet Mask) whereas IPv6 doesn't support VLSM.
- IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Q 4. Draw and explain the 6LoWPAN Protocol.

6LoWPAN is a simple low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements as it provides IPv6 networking over IEEE 802.15.4 networks. It is formed by devices that are compatible with the IEEE 802.15.4 standard and characterized by short-range, low bit rate, low power, low memory usage, and low cost.



6LoWPAN Architecture

- When a lower processing capability sensor node in a 6LoWPAN or so-called reduced function device (RFD) wants to send its data packet to an IP-enabled device outside the 6LoWPAN, it first sends the packet to the higher processing capability sensor node or so-called full function device (FFD) in the same PAN.
- The FFDs which react as a router in 6LoWPAN will forward the data packet hop by hop to the 6LoWPAN gateway.
- The 6LoWPAN gateway that connects to the 6LoWPAN with the IPv6 domain will then forward the packet to the destination IP-enabled device by using the IP address.
- In the model of 6LoWPAN protocol stack, it adopts IEEE 802.15.4 standard PHY and MAC layers which are specified, as its bottom layers while chooses IPv6 in its network layer. Basically, the IEEE 802.15.4 standard specifies PHY and MAC layers for low-rate wireless personal area networks (LR-WPAN).
- The PHY layer specification dictates how the IEEE 802.15.4 devices may communicate with each other over a wireless channel.
- There are a total of 27 channels defined in the PHY layer. These channels are allocated to different frequency bands with varying data rates.
- At the MAC layer, it specifies when the devices may access the channel for communication. The basic tasks provided by the MAC layer are beacon generation and synchronization, supporting PAN association and dissociation, managing channel access via Carriers Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, and etc.

Q 5. Explain and differentiate TCP and UDP.

Transmission Control Protocol (TCP) is a connection-oriented protocol that computers use to communicate over the internet. It is one of the main protocols in TCP/IP networks.

- TCP provides error-checking and guarantees delivery of data and that packets will be delivered in the order they were sent.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in the TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

User Datagram Protocol (UDP) is a Transport Layer protocol that works just like TCP but assumes that error-checking and recovery services are not required. Instead, UDP continuously sends datagrams to the recipient whether they receive them or not.

- UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is unreliable and connectionless. So, there is no need to establish a connection prior to data transfer.

- For real-time services like computer gaming, voice or video communication, live conferences; we need UDP.
- Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
- There is no error checking in UDP, so it also saves bandwidth.
  User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

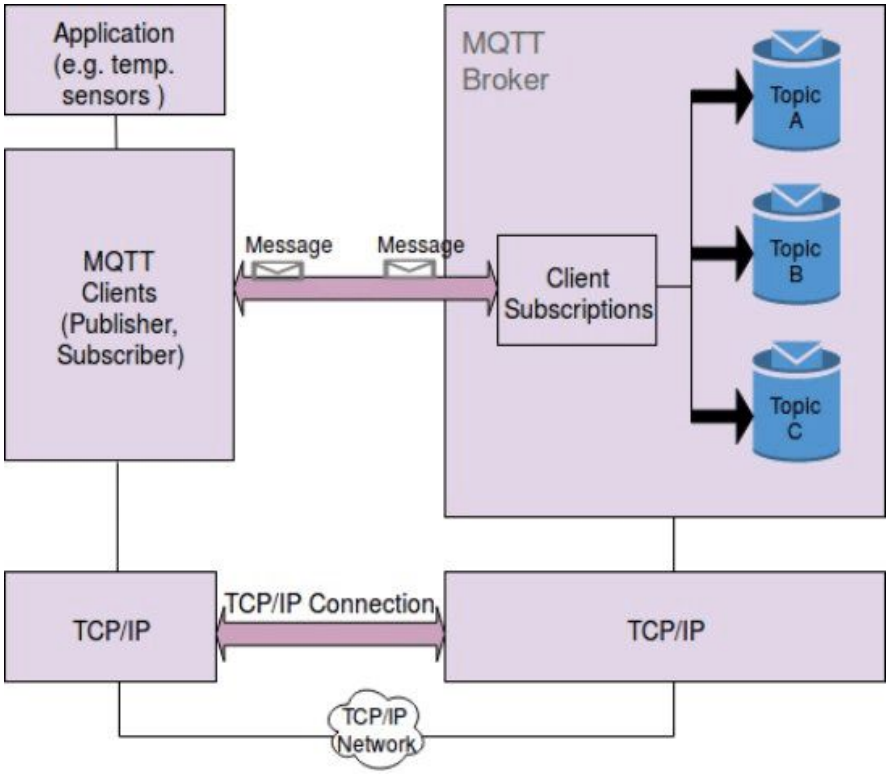
Difference between TCP and UDP

No.	TCP	UDP
1	Connection Oriented Protocol	Connection-less Protocol
2	Connection in byte stream	Connection in message stream
3	It does't support multicasting and broadcasting	It supports broadcasting
4	It provides error control and flow control	Error control and flow control is not Provided
5	Supports full duplex	Does not support full duplex
6	Three way handshake	No handshake
7	TCP header size is 20 bytes	UDP header size is 8 bytes
8	TCP packet is called as segement	UDP packet is called as user datagram

Q 6. Explain the MQTT protocol and its architecture.

MQTT (Message Queue Telemetry Transport) is designed as a lightweight messaging protocol that uses publish/subscribe operations to exchange data between clients and the server. Furthermore, its small size, low power usage, minimized data packets and ease of implementation make the protocol ideal for the “machine-to-machine” or “Internet of Things” world.

- It is created by IBM & Eurotech and donated to Eclipse “Paho” M2M project (OASIS standard in 2014)
- MQTT has been utilized as a part of many IoT gadgets and instant message delivery systems because it was intended to work on low power machines as a light-weight protocol.
- There are two main components in MQTT Architecture, that are
    - Client
    - Broker



MQTT Architecture

The typical MQTT architecture can be divided into two main components as Client and Broker.

Client

Client could be a Publisher or Subscriber and it always establishes the network connection to the Server (Broker). It can do the following things :

1. Publish messages for interested users.
2. Subscribe to interesting subjects for receiving messages.
3. Unsubscribe to extract from the subscribed subjects.
4. Detach from the Broker.

Broker

Broker controls the distribution of information and is mainly responsible for receiving all messages from the publisher, filtering them, deciding who is interested in it and then sending the messages to all subscribed clients. It can do the following things:

1. Accept Client requests.
2. Receives Published messages by Users.
3. Processes different requests like Subscribe and Unsubscribe from Users.
4. After receiving messages from the publisher, it sends it to the interested Users.

Q 7. Write a short note on HTTP, CoAP, XMPP, AMQP.

HTTP (HyperText Transport Protocol)

- HTTP is predominantly a web messaging protocol, which was originally developed by Tim Berners-Lee. Later, it was developed by IETF and W3C jointly and first published as a standard protocol in 1997.
- HTTP supports request/response RESTful Web architecture.
- Analogous to CoAP, HTTP uses a Universal Resource Identifier (URI) instead of topics. The server sends data through the URI and the client receives data through a particular URI.
- HTTP is a text-based protocol and it does not define the size of header and message payloads rather it depends on the web server or the programming technology.
- HTTP uses TCP as a default transport protocol and TLS/SSL for security. Thus, communication between client and server is connection-oriented. It does not explicitly define QoS and requires additional support for it.
- HTTP is a globally accepted web messaging standard that offers several features such as persistent connections, request pipelining, and chunked transfer encoding.

CoAP (Constrained Application Protocol)

- CoAP is a lightweight M2M protocol from the IETF CoRE (Constrained RESTful Environments) Working Group.
- CoAP architecture is divided into two main sublayers: messaging and request/response. The messaging sublayer is responsible for the reliability and duplication of messages while the request/response sublayer is responsible for communication.
- CoAP is mainly developed to interoperate with HTTP and the RESTful Web through simple proxies.
- CoAP is a binary protocol and normally requires a fixed header of 4-bytes with small message payloads up to maximum size depends on the web server or the programming technology.
- CoAP uses UDP as a transport protocol and DTLS for security. Thus, clients and servers communicate through connectionless datagrams with less reliability.
- CoAP offers more functionality than MQTT such as it supports content negotiation to express a preferred representation of a resource; this allows the client and server to evolve independently, adding new representations without affecting each other.
- CoAP has four messaging modes: confirmable, non-confirmable, piggyback and separate.
  - ➢ Confirmable and non-confirmable modes represent reliable and unreliable transmissions, respectively while the other modes are used for request/response.
  - ➢ Piggyback is used for client/server direct communication where the server sends its response directly after receiving the message, i.e., within the acknowledgment message.
  - ➢ The separate mode is used when the server response comes in a message separate from the acknowledgment and may take some time to be sent by the server.

XMPP (Extensible Messaging and Presence Protocol)

- XMPP is a messaging protocol that was designed originally for chatting and message exchange applications.
- It was standardized by IETF more than a decade ago. Hence, it is well known and has proven to be highly efficient over the internet.
- Recently, it has been reused for IoT applications as well as a protocol for SDN. This reusing of the same standard is due to its use of XML which makes it easily extensible.
- XMPP supports both publish/ subscribe and request/ response architecture and it is up to the application developer to choose which architecture to use.
- It is designed for near real-time applications and, thus, efficiently supports low-latency small messages.
- It does not provide any quality of service guarantees and, hence, is not practical for M2M communications.
- Moreover, XML messages create additional overhead due to lots of headers and tag formats which increase the power consumption that is critical for IoT application.
- XMPP is rarely used in IoT but has gained some interest in enhancing its architecture in order to support IoT applications.

AMQP (Advanced Message Queuing Protocol)

- AMQP is a lightweight M2M protocol, which was developed by John O'Hara at JPMorgan Chase in London, the UK in 2003.
- It is a corporate messaging protocol designed for reliability, security, provisioning, and interoperability.
- AMQP supports both request/response and publish/subscribe architecture. It offers a wide range of features related to messaging such as a reliable queuing, topic-based publish-and-subscribe messaging, flexible routing and transactions.
- AMQP is a binary protocol and normally requires a fixed header of 8-bytes with small message payloads up to maximum size depends on the broker/server or the programming technology.
- AMQP uses TCP as a default transport protocol and TLS/SSL and SASL for security. Thus, the communication between client and broker is connection-oriented.
- Reliability is one of the core features of AMQP, and it offers two preliminary levels of Quality of Service (QoS) for delivery of messages: Unsettle Format (not reliable) and Settle Format (reliable).

Q 8. Write down the differentiation between HTTP, CoAP, XMPP, AMQP and MQTT protocol.

	HTTP	CoAP	XMPP	AMQP	MQTT
Transport	TCP/IP	UDP/IP	TCP/IP	TCP/IP	TCP/IP

Interaction model	Request/Response	Point to point message exchange	Point to point message exchange	Point to point message exchange	Publish/subscribe
Scope	Device to cloud, cloud to cloud	Device to device	Device to cloud, cloud to cloud	Device to device, device to cloud, cloud to cloud	Device to cloud, cloud to cloud
Interoperability level	semantic	semantic	structural	structural	foundational
Fault tolerance	Server is SPoF	Decentralized	Server is SPoF	Implementation-specific	Broker is SPoF
Security	HTTPS	DTLS	TLS+SASL	TLS+SASL	TLS
Blessing	IETF	IETF	IETF	OASIS	OASIS

Q 9. Write a detailed case study on any 4 areas: Smart Cities and Smart Homes; Connected Vehicles; Industrials IOT; Agriculture; Activity Monitoring.

i) Smart Cities and Smart Homes

In this case study we are going to talk about how IoT can help in building smart cities and smart homes as you know that throughout the world and even in countries like India, there is a lot of focus on building smart cities. Of course, the scope of smart cities in each of these different countries is different and the scope again depends on the priority areas of each of these countries and their government. Now for instance in India, since the last few years, there have been a couple of cities that have been identified and phase-wise these cities have been given funds to build or to transform them as smart cities.

So, when we talked about smart cities; what is it. So, in addition to the regular infrastructure that is there in any city, for example, the urban infrastructure consisting of office buildings, residential areas, hospitals, schools, transportation police and so on you also need something, in addition, to make the cities smart. So, what is this, in addition, let us talk about it. So, smart means what smart means that it is in terms of the services that are given to the respective stakeholders of these cities. So, citizens are able to do things in a better manner in an improved manner than usual and how is that made possible that is made possible with the help of nothing, but the ICT technologies information and communication technologies which also includes

electronics embedded electronics different other advanced topologies in electrical sciences and so on. So, computers and electronics put together can make these cities smart.

Example: So, first of all, let us consider any smart city. So, if we are talking about a smart city we need to have the basic components, for example, transport there have to be railways there have to be hospitals there have to school there has to be let us say traffic control waste management banking then.

So, like this, these are some of the different things in a smart city right and one thing I have missed which is very much essential is the police. So, as you can see that we have to transform all of these different components of any city to be smart. So, for which the technology is that we have studied. So, far in the previous lectures will have to be taken help of. So, we definitely will have to take the help of sensors sensor networks then actuators than the different other communication technologies RFID, NFC, ZWAVE and so and so forth. So, many different things that we have covered in all these previous lectures of this course on IoT, so, all these will have to be used in order to make this transformation. So, these are the different ICT information and communication technologies that will have to be used right.

Analogy

Humans	Smart Cities
Skeleton	Buildings, Industries, People
Skin	Transportation, Logistics
Organs	Hospital, Police, Banks, Schools
Brain	Ubiquitously embedded intelligence
Nerves	Digital telecommunication networks
Sensory Organs	Sensors, Tags
Cognition	Software

So, all these basically necessitate the building of smart cities using advanced ICT tools. So, let us draw some analogy when we talk about a human humans have the skeleton the skin the organs different types of organs brains nerves sensory organs cognition and so on in the smart city as well in the same way has as a human has a skeleton skin and organs smart cities or rather any city has buildings industries people transportation logistics hospital police banks schools. So, these are there, but on top of that if there is a human with skeleton skin and organs, but no brains no nerves no sensory organs no cognition. So, you do not have to know life in that human, you do not have any life in that human.

Focused Areas:

1. **Application Focus Areas:** These are some of the application focus areas we have a smart economy. So, because of the ever-increasing competitiveness, we need to improve our infrastructure and economy to make it smart. To improve citizen participation in any good

governance. In any good governance, we need to improve you need to increase the citizen participation and how it is that possible we need to take the help of the ICT tools.

2. **Current Focus Areas:-** Now, we have the different focus areas we have smart homes smart parking lots in a smart home situation we need to have I will talk about smart homes in more detail later on, but in a smart home situation we have the health monitoring done in a smart way at home this we know the medical data made available to the doctors whenever there is a health criticality the corresponding house physician would be informed the physician can take requisite action based on the severity of severity or criticality of the health of the patient.

Pollution and calamity Monitoring

- Monitoring for weather or man-made based calamities.
- Alter generation in case of threshold pollution in the air.
- Resource allocation and routine of service in the event of calamities.

Smart energy

- Smart meter system.
- Smart energy allocation and distribution system.
- Incorporation of traditional and renewable sources of energy in the same grid.

Smart vehicle

- Assistance to drivers during bad weather or low-visibility.
- Detection of bed drivers under the influence of substances.
- Auto alert generation during crashes.
- Self-diagnostics.

Smart Health

- Low cost, portable, at-home medical diagnosis kit.
- Remote check-ups and diagnosis.
- On-body sensors for effortless and accurate health monitoring
- Auto alert generation in case of emergency medical episodes.

IoT Challenges in Smart Cities:- There are different IoT challenges in smart cities security and privacies one. So, because you know all these different infrastructures are made available to all different types of citizens. We know to expose ourselves to different types of attacks the government officers there are different files etcetera we make ourselves vulnerable to different types of attacks privacy leaks and so on when we open up more and more.

Security and Privacy

- Exposure to attacks(e.g. cross-site scripting,etc.)
- Exposure to vulnerabilities.
- Multi-tenancy induces the risk of data leakage.

Heterogeneity

- Integration of varying hardware platforms and specifications.
- Integration of different radio specifications.
- Integration of various software platforms.
- Accommodation of varying user requirements.

There are legal and social issues as well, for example, services that are based on users provided information may be subject to local or other national and international laws and that also has to be taken care of in a very smart way individual and informed consent is required for using humans as data sources big data issues are there huge volumes of data coming at high speeds and different types of vary various types of data media text data and so on.

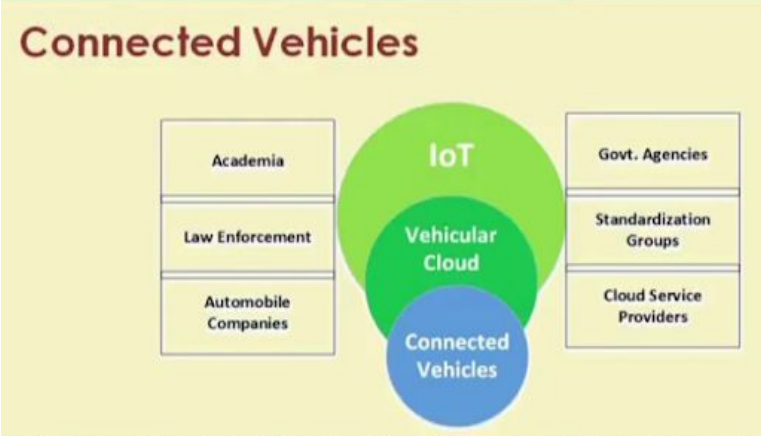
ii) Connected Vehicles

Connected Vehicles are equipped with sensors, networking, and communicating devices that are capable of communicating with other devices within the vehicle, with the other similar vehicles and with fixed infrastructure.
All the different types of communication are going to happen in a connected vehicle scenario. So, issues such as security privacies, scalability, reliability, quality of service and on top of the lack of any singular global standard for connectivity, are some of the challenges that are facing the building of connected vehicles.

Vehicles-to-Everything(V2X) Paradigm

- The main component of the future intelligent Transport System (ITS).
- Enables Vehicles to wirelessly share a diverse range of information.
- Information sharing maybe with other vehicles, pedestrians, or fixed infrastructure (mobile towers, parking meters, etc.)
- Allows for traffic management, ensuring on-road and off-road safety, mobility for traveling.
- It follows a distributed architecture, where contents are widely distributed over the network.

- Not restricted to a single source information provider.
- Designed mainly for highly mobile environments.
- It can share information to nodes in the vicinity, as well as remotely located.
- Has greatly enhanced travel efficiency .as well as safety.
- The network is mainly used as a tool for sharing and disseminating information.



Features of TCP/IP in V2X

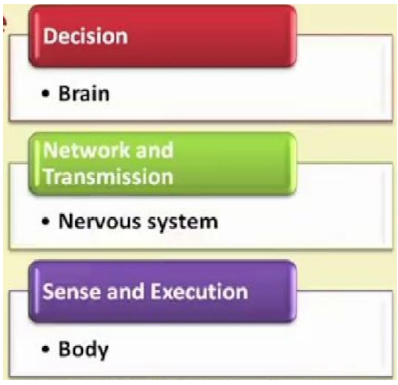
- Designed mainly for handling information exchanging between a single pair of entities.
- Information exchange dependent on the location of data.
- It can only identify the address of endpoints, which alone is not useful for content distribution.
- An increase in the number of wireless devices restricts the mobility of nodes.

Content-Centric Networking (CCN)

- CCN is derived from information Centric Networking (ICN)Architecture.
- It focuses more on the data than its actual location.
- Hierarchically named data.
- Hierarchical data is transmitted directly instead of being part of a conversation.
- Enables scalable and efficient data dissemination.
- In-network caching allows for low data traffic.
- Works well in highly mobile environments.

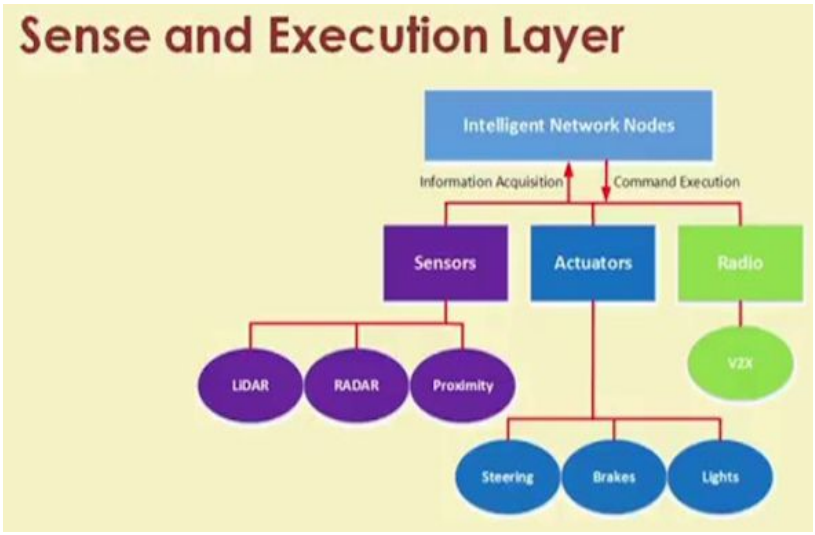
Vehicular Ad-hoc Networks (VANETs)

- Based on:
    1. Dedicated Short-Range Communication (DSRC)
    2. Wireless Access in Vehicular Environment (WAVE)
- Routing protocols derived from MANETs.
- High throughput is achievable in mobile environments.
- Guaranteed low-latency in Mobile environments.



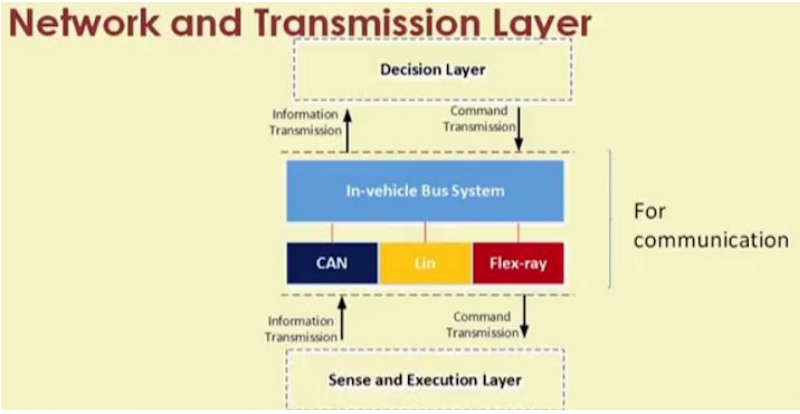
Body and Brain Architecture

- An in-vehicle networking architecture.
- Three-layered Architecture.
- The body consists of intelligent networking nodes (INN) that constantly collect information from the vehicle.
- The brain manages central coordination.

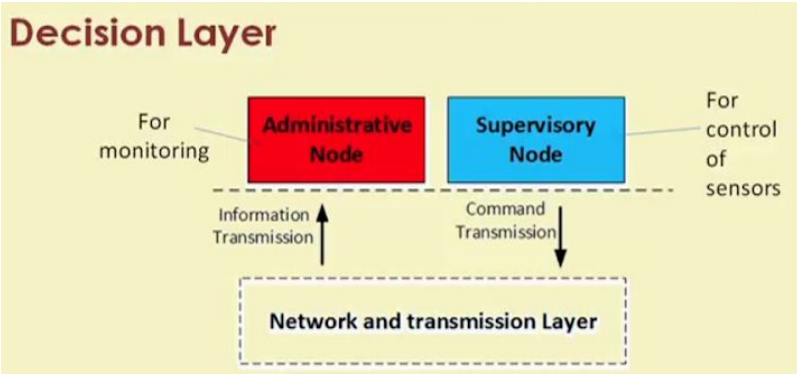


The sense and execution layer. In the sense and execution layer, we have these intelligent nodes. With the help of sensors actuators different radios, the information is acquired with the help of different other devices like LDAR, RADAR proximity sensors and different other sensors plus actuators such as steering brakes lights etcetera the information is acquired.

The network and transmission layer looks like this and as this name suggests we have for communication, this is used primarily for communication. The sense and execution layer on the very bottom and on the top and the decision layer and in between there is the communication in the communication layer.



Where there is a vehicle bus system bus means that it is a collection of ware. So, all these together will comprise the network and transmission layer which is used for communication. And that basically sits in between the sensing and execution layer and the decision layer.



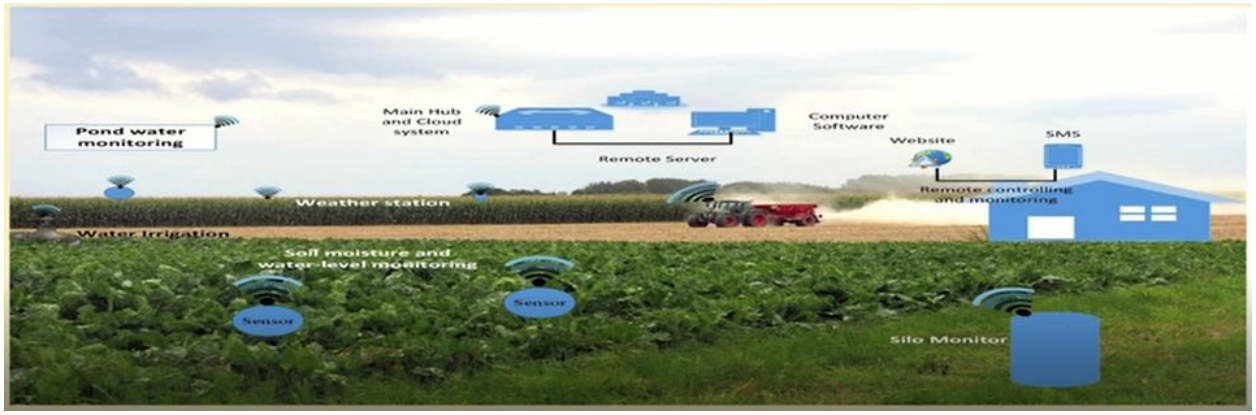
In the decision layer which sits on top of the network and transmission layer. The information is transmitted for monitoring to the administrative node and for control of the sensor nodes, the supervisory node basically sends the command to the network and the transmission layer, for further sending to the actuators underneath.

iii) Agriculture

Another important domain for IoT is the agriculture domain where the IoT system plays a vital role in soil and crop monitoring and provides a proper solution accordingly.

Using smart farming through IoT technologies helps farmers to reduce waste generation and increase productivity.

Agricultural use of IoT more specifically on the use of IoT for smart irrigation. A smart irrigation management system.
What is going to happen to the use of IoT in agriculture and what is going to happen in the future. So, the picture that we see in front of us is an agricultural field, a hypothetical one where there are different types of sensors that are planted sensors such as for soil, moisture and water level monitoring for automated irrigation performance performing automated irrigation.



Automated recycling of organic waste, vermicomposting automated sowing and weeding and so on and so forth, so many different things automated systems fitted with sensors fitted with different actuators are going to be used for making agriculture smarter.

So, the objectives of this smart water management system, the AgriSens system are how less water can be used for getting more yield in terms of crop productivity; that means, and typically you know. So, what happens is for plants such as rice; that means, paddy plants wheat and so on. These basically are dependent on the soil moisture, the water level in the soil and so on and so forth and many other climatic factors.

Smart Water Management using a loT

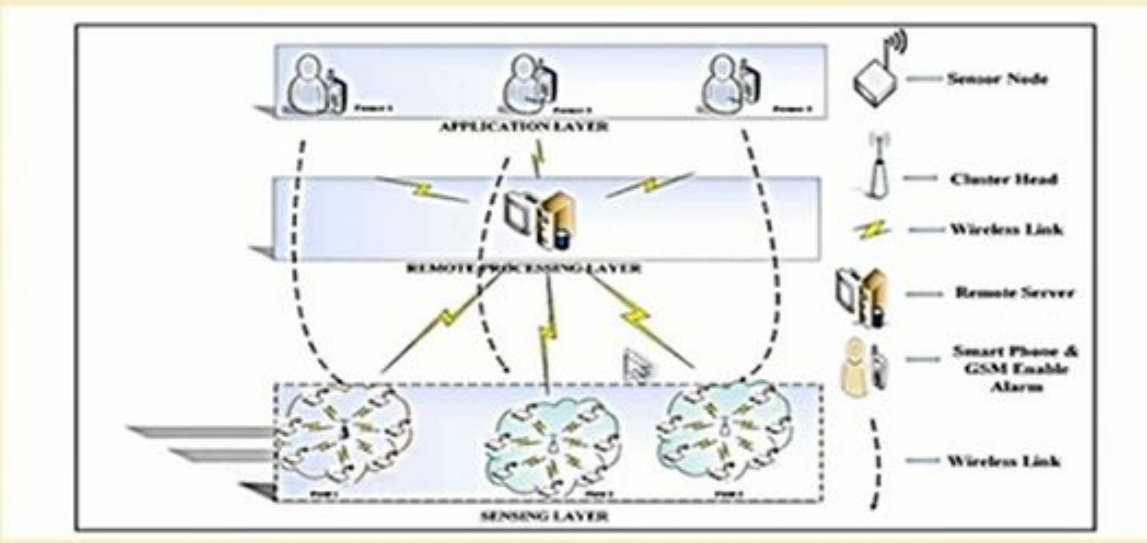
Objectives

- More yields with less water
- Save limited water resource in a country
- Automatic Irrigation
- Dynamic irrigation treatments in the different phases of a crop's life cycle
- Remote monitoring and controlling

Proposed architecture

- Sensing and actuating layer
- Processing, storage, and service layer
- Application layer

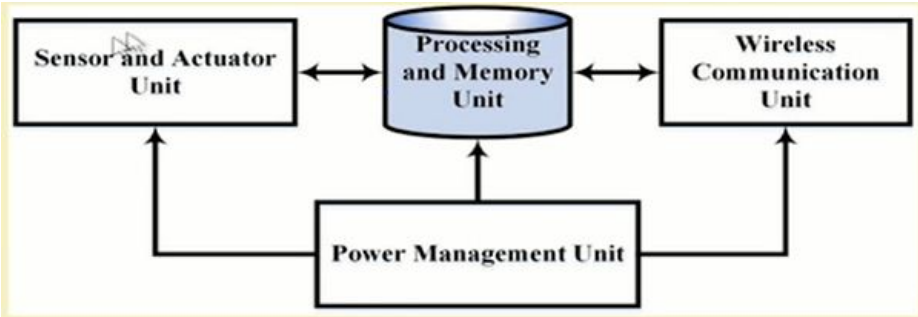
The proposed architecture of the AgriSens system for offering smart water management. So, we have different layers of the system so we have the sensing layer the remote processing layer and the application layer the sensing layer basically has different types of sensors soil moisture water level etcetera which through data from different clusters this through data through their cluster heads to the remote processing server and different analytics and run and those data are made available to the different applications in the application layer.



Design

- Integrated design for sensors
- Integrated design for sensor node
- Integrated design for remote server

The EC 05 soil moisture sensor has been put there and has been dug inside the surface of the earth. So, the soil moisture sensor is basically put inside and is installed inside the level of the mud level of mud or level of the earth. So, it is inside it is dug inside.



So, this is the overall design of the sensor node. So, here basically what we have is apart from the sensors and actuators we have a processing unit and the memory unit we have wireless communication unit and we have the power management unit.

Integrated design for remote server

- Repository data server: Communicates with the deployed loT gateway in the field by using GPRS technology.
- Web server: To access field data remotely.

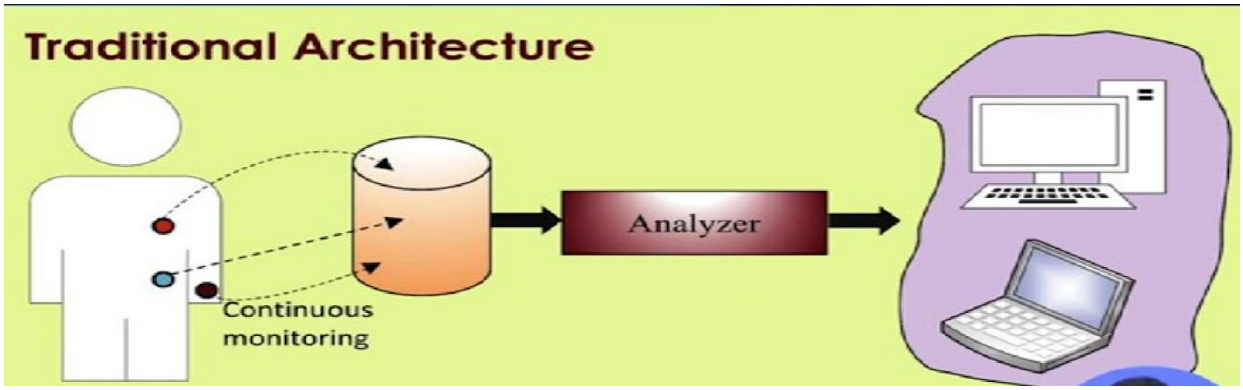
- Multi-users server: Sends field information to the farmer's cell using SMS technology and also executes the farmer's query and control messages.

There are different sensors, one is a soil moisture sensor which is basically buried in the ground and there is another sensor which is the water level sensor. So, the soil moisture sensor basically as this name says that it basically sensors the soil moisture and the water level sensor is how much is the stagnant water level in this particular grid. So, this is what it measures. And these two sensor data are sent to this particular node.

iv) Activity Monitoring

Wearable sensors have become very popular for different purposes such as medical, child care, elderly care, etc. These sensors help in monitoring the physical activities of humans.
Particularly in IoT scenarios, activity monitoring plays an important role in providing better quality of life and safeguarding humans. Provides information accurately in a reliable manner and provides continuous, monitoring support.

Suppose a person is walking, running, lying down, is talking maybe a person is fighting or had an accident and so on and the sensor values keep on changing especially the smartphone sensors since we are talking about or the case study we are talking about smartphone sensors. So, we have taken the inbuilt sensors in the smartphone. So, those sensorial values are transmitted over the network to a remote server, where they can be used for a multitude of applications ranging from normal activity monitoring fall detection you can even use an offline non-smartphone sensor like a standard accelerometer or Imo based sensors integrated to a small processor board, and the same operation can be performed for those sensors also. So, these non-smartphone based activity monitors have been given the common name wearables.



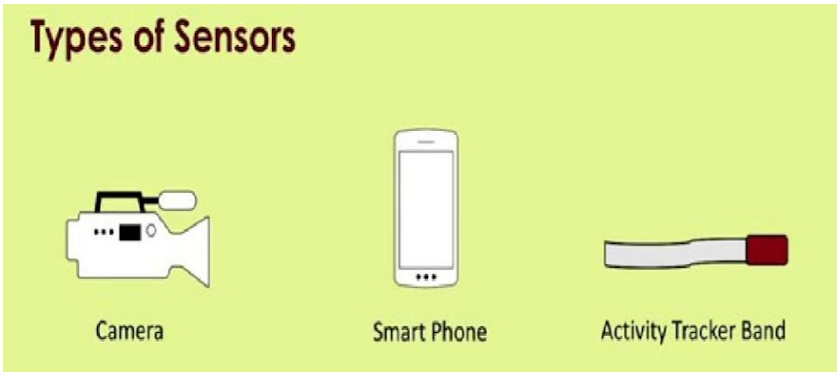
Typical architectures deal with suppose you have this person and he is equipped with multiple wearables, one is tracking the heartbeat, one is tracking the body temperature, one is tracking the activity on the wrist and all this data is being forwarded may be to a remote router or a network server, and then an analyzer analyses the activities and instead of transmitting the raw data, the analyzer transmits the analyzed activities to various connected stations that may be a home computer to which the family members are keeping track of view, that may be a laptop or a

mobile computer or even a cloud or maybe your medical doctors or consultants are keeping track of your activities.

Advantages

- Continuous monitoring of activities in daily observation of human behavior and repetitive patterns in their activities.
- Easy integration and fast equipment.
- Long term monitoring
- Utilization of sensors of handheld devices
    1. Accelerometer
    2. Gyroscope
    3. GPS
    4. others

some of the basic human activities which these market available devices do are they can distinguish, actions they can distinguish gestures like for actions they can distinguish between running jumping or whether a person is lying down or sitting, and what gestures you can have if a person is holding his or her legs if a person is moving his or her hands and suppose if a person is dancing right. So, that would be considered as an action, but there will be gestures involved also. So, maybe a person is dancing peacefully or a person is dancing aggressively, you can detect that using various gestures you can detect you can maybe predict the intent of a person using the gestures the person is providing, maybe a person is threatening, someone maybe a person is trying to please someone and so on.



Data Analysis Tools

- Statistical: sensor data
- Machine Learning-Based: Sensor data
- Deep Learning-Based
    - Sensor data
    - Images
    - Videos

Approaches

- In place
    - On the device
    - Power intensive
    - No network connection required
- Network-Based
    - Larger and processing-intensive methods can be applied
    - Group based analytics possible
    - Low power consumption
    - Average to good network connection

Q 10. write security issues in IoT.

As more and more IoT devices make their way into the world, deployed in uncontrolled, complex, and often hostile environments, securing IoT systems presents a number of unique challenges. Some of the challenges for IoT security:

- Secure constrained devices
- Authorize and authenticate devices
- Manage device updates
- Secure communication
- Ensure data privacy and integrity
- Secure web, mobile, and cloud applications
- Ensure high availability
- Detect vulnerabilities and incidents
- Manage vulnerabilities
- Predict and preempt security issues

Ques. Differentiate between HTTP, AMQP, and MQTT.

	HTTP	AMQP	MQTT
Get	Yes	Yes	No
Caching Read	Yes	No	Yes
Put	Yes	No	No
Post	Yes	Yes	No
Delete	Yes	No	No
Content filtering	No	Yes	No
Typed headers	No	Yes	No
Resumeable transfer	Yes	Yes	Yes
Transactions	No	Yes	No
SSL/TLS	Yes	Yes	Yes
Kerberos	Yes	Yes	No
SASL	No	Yes	Yes
Symmetric Protocol	No	Yes	No
Socket Multiplexing	No	Yes	Yes
Out-of-order messaging	No	Yes	Yes
Server initiated transfers	No	Yes	No
Single packet send	Yes	Yes	Yes
Store-and-forward	No	Yes	Yes
Publish-and-subscribe	No	Yes	Yes
Defined error recovery	No	Yes	No
Well defined addresses	Yes	Yes	Yes
Content-based routing	No	Yes	No
Credit-based flow control	No	Yes	No