MODULE-1

1.What is IOT? explain evolutionary phase of the internet. Explain in detail on Genesis of IOT. +1 (06 MARKS) (8 MARKS)

- IoT is a technology transition in which devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.

  Genesis of IOT

- The age of IoT is often said to have started between the years 2008 and 2009. During this time period, the number of devices connected to the Internet increased.
- The evolution of the Internet can be categorized into four phases. Each of these phases has had a profound impact on our society and our lives

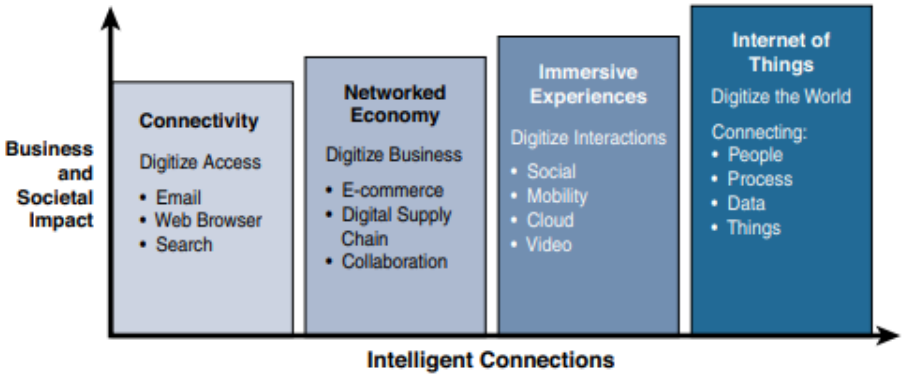


Figure 1-1 *Evolutionary Phases of the Internet*

Table 1-1 *Evolutionary Phases of the Internet*

Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

Connectivity

- It began in the mid-1990s.

- In the beginning, email and getting on the Internet were luxuries for universities and corporations.
- Getting the average person online involved dial-up modems, and even basic connectivity was rare.

Networked Economy

- Here, e-commerce and digitally connected supply chains increased, and this caused one of the major disruptions of the past 100 years.
- Vendors and suppliers became closely interlinked with producers, and online shopping experienced incredible growth.
- The victims of this shift were traditional brick-and-mortar retailers.
- The economy itself became more digitally intertwined as suppliers, vendors, and consumers all became more directly connected.

Immersive Experiences

- It is characterized by the emergence of social media, collaboration, and widespread mobility on a variety of devices.
- Connectivity is now universal, using multiple platforms from mobile phones to tablets to laptops and desktop computers.
- This connectivity in turn enables communication and collaboration as well as social media across multiple channels, via email, texting, voice, and video.
- person-to-person interactions have become digitized.

Internet of Things

- Machines and objects in this phase connect with other machines and objects, along with humans.
- Business and society have already started down this path and are experiencing huge increases in data and knowledge.
- In turn, this is now leading to previously unrecognized insights, along with increased automation and new process efficiencies.

2.Explain the access network sublayer with a neat diagram. (6 MARKS)

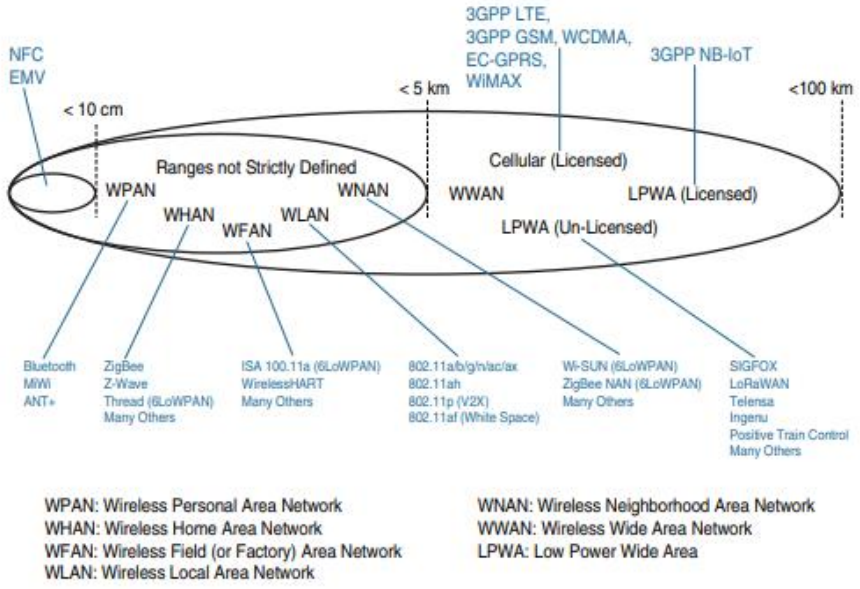


Figure 2-9 *Access Technologies and Distances*

- One key parameter determining the choice of access technology is the range between the smart object and the information collector**.**
- Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected. Common groups are as follows:
- **PAN (personal area network):** Scale of a few meters. This is the personal space around a person. A common wireless technology for this scale is Bluetooth.
- **HAN (home area network):** Scale of a few tens of meters. At this scale, common wireless technologies for IoT include ZigBee and Bluetooth Low Energy (BLE).
- **NAN (neighborhood area network):** Scale of a few hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.
- **FAN (field area network):** Scale of several tens of meters to several hundred meters. FAN typically refers to an outdoor area larger than a single group of house units
  The FAN is often seen as “open space” (and therefore not secured and not controlled).
- **LAN (local area network):** Scale of up to 100 m. This term is very common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used.

Other networking classifications, such as MAN (metropolitan area network, with a range of up to a few kilometers) and WAN (wide area network, with a range of more than a few kilometers), are also commonly used.

3.What are the elements of one M2M IOT architecture? Explain. +1 (8 MARKS)

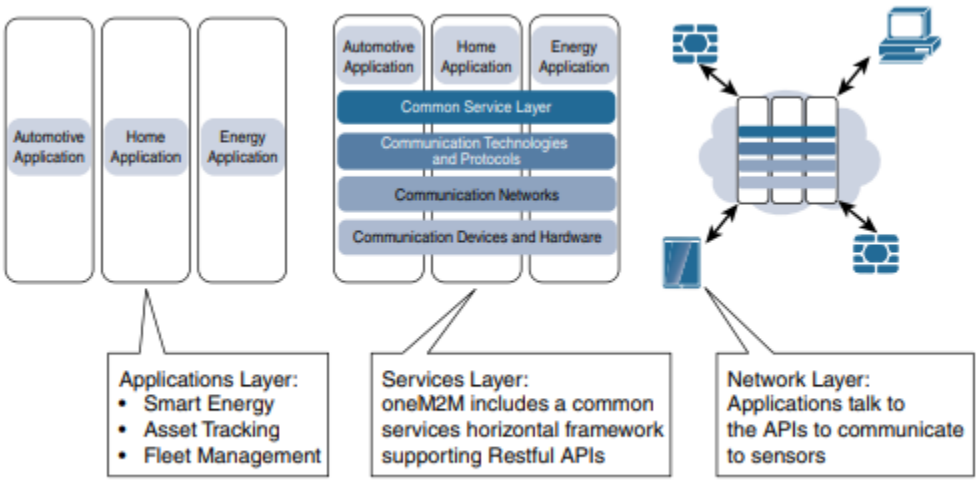


Figure 2-1 *The Main Elements of the oneM2M IoT Architecture*

1. **Applications layer:**

- The oneM2M architecture gives major attention to connectivity between devices and their applications.
- This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems.
- Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

2. **Services layer:**

- This layer is shown as a horizontal framework across the vertical industry applications.
- At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the hardware.
- Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on.
- Riding on top is the common services layer.
- This conceptual layer adds APIs and middleware supporting third-party services and applications.

3. **Network layer:**

- This is the communication domain for the IoT devices and endpoints.
- It includes the devices themselves and the communications network that links them.
- Embodiments of this communications infrastructure are wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11.
- Also included are wired device connections, such as IEEE 1901 power line communications.

4.Explain the functionality of IOT network management sublayers. (5 MARKS)

- Upper-layer protocols need to take care of data transmission between the smart objects and other systems.
- Multiple protocols have been leveraged or created to solve IoT data communication problems. Some networks rely on a push model whereas others rely on a pull model and multiple hybrid approaches are also possible.
- Some IoT implementers have suggested HTTP for the data transfer phase. The sensor could use the client part to establish a connection to the IoT central application (the server), and then data can be exchanged. But, HTTP is a fat protocol and was not designed to operate in constrained environments with low memory, low power, low bandwidth, and a high rate of packet failure.
- Hence, other web-derived protocols have been suggested for the IoT space. One example is WebSocket. WebSocket is part of the HTML5 specification, and provides a simple bidirectional connection over a single connection.
- WebSocket is often combined with other protocols, such as MQTT (described shortly) to handle the IoT-specific part of the communication.
- With the same logic, **Extensible Messaging and Presence Protocol** (XMPP) was created.
- XMPP is based on instant messaging and presence.
- It allows the exchange of data between two or more systems and supports presence and contact list maintenance.
- A limitation of XMPP is its reliance on TCP, which may force subscribers to maintain open sessions to other systems and may be a limitation for memory-constrained objects.
- **Constrained Application Protocol (CoAP**)- CoAP uses some methods similar to those of HTTP (such as Get, Post, Put, and Delete) but implements a shorter list, thus limiting the size of the header.

- CoAP also runs on UDP (whereas HTTP typically uses TCP).
- CoAP also adds a feature that is lacking in HTTP and very useful for IoT: observation. Observation allows the streaming of state changes as they occur, without requiring the receiver to query for these changes.
- **Message Queue Telemetry Transport (MQTT) -** MQTT uses a broker-based architecture.
- MQTT runs over TCP.
- A consequence of the reliance on TCP is that an MQTT client typically holds a connection open to the broker at all times.
- This may be a limiting factor in environments where loss is high or where computing resources are limited.

5.Describe IOT World Forum (IOTWF) Standardized architecture. (7 MARKS)

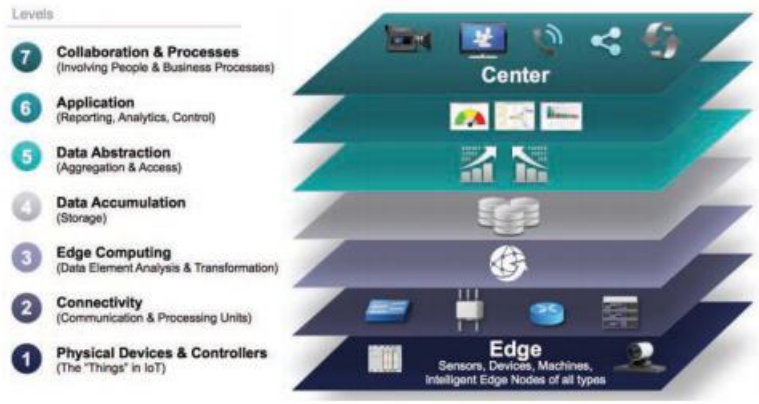


Figure 2-2 *IoT Reference Model Published by the IoT World Forum*

Layer 1: Physical Devices and Controllers Layer

- The first layer of the IoT Reference Model is the physical devices and controllers' layer.
- This layer is home to the "things" in the Internet of Things, including the various endpoint devices and sensors that send and receive information.
- The size of these can range from almost microscopic sensors to giant machines in a factory.
- Their primary function is generating data and being capable of being queried and/or controlled over a network.

Layer 2: Connectivity Layer

- In the second layer of the IoT Reference Model, the focus is on connectivity.
- The most important function of this IoT layer is the reliable and timely transmission of data. This includes transmissions between Layer 1 devices and the network and

between the network and information processing that occurs at Layer 3 (the edge computing layer).

- The connectivity layer encompasses all networking elements of IoT and doesn't really distinguish between the last-mile network (the network between the sensor/endpoint and the IoT gateway, discussed later in this chapter), gateway, and backhaul networks.

Layer 3: Edge Computing Layer

- Edge computing is the role of Layer 3.
- Edge computing is often referred to as the "fog" layer
- At this layer, the emphasis is on data reduction and converting network data flows into information that is ready for storage and processing by higher layers.
- One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible.

Upper Layers: Layers 4–7

- The upper layers deal with handling and processing the IoT data generated by the bottom layer.

6.Compare and contrast IT and OT. (4 MARKS)

Table 1-3 *Comparing Operational Technology (OT) and Information Technology (IT)*

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible

Criterion	Industrial OT Network	Enterprise IT Network
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

(EXTRA)

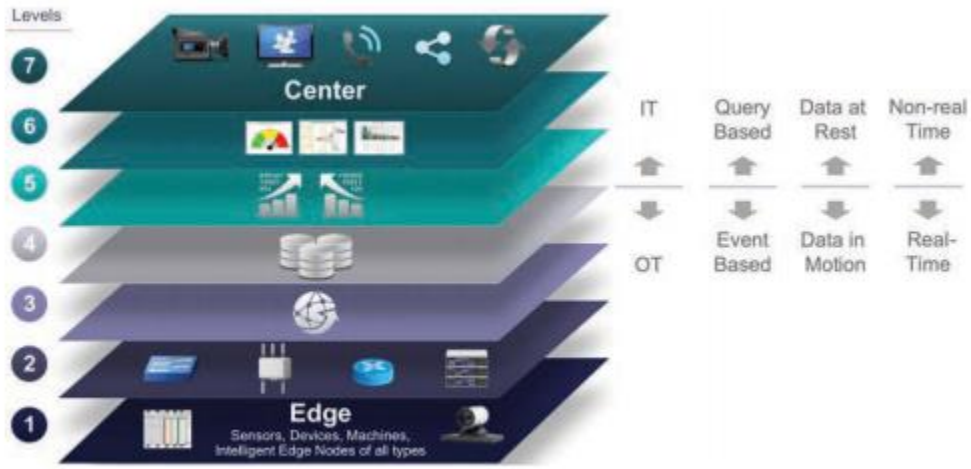


Figure 2-5 *IoT Reference Model Separation of IT and OT*

- IoT systems have to cross several boundaries beyond just the functional layers. The bottom of the stack is generally in the domain of OT.
- The top of the stack is in the IT area and includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT.
- At the bottom, in the OT layers, the devices generate real-time data at their own rate—sometimes vast amounts on a daily basis.
- The huge amount of data transiting the IoT network and huge volume of data suggests that applications at the top layer will be able to ingest that much data at the rate required.
- To meet this requirement, data has to be buffered or stored at certain points within the IoT stack.
- Layering data management in this way throughout the stack helps the top four layers handle data at their own speed.
- The IT and OT organizations need to work together for overall data management.

7.What does IOT and digitization mean? Elaborate on his concept. (4 MARKS)

- IoT focuses on connecting “things,” such as objects and machines, to a computer network, such as the Internet. IoT is a well-understood term used across the industry as a whole.
- Digitization can mean different things to different people but generally encompasses the connection of “things” with the data they generate and the business insights that result**.**
- In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable.
- A good example of this that many people can relate to is in the area of home automation with popular products, such as Nest. With Nest, sensors determine your desired climate settings and also tie in other smart objects, such as smoke alarms, video cameras, and various third-party devices.
- In the past, these devices and the functions they perform were managed and controlled separately and could not provide the holistic experience that is now possible.
- Nest is just one example of digitization and IoT increasing the relevancy and value of networked, intelligent connections and making a positive impact on our lives.

8.Write a short note on “IOT” impact in “Real WORLD”. (04 MARKS)

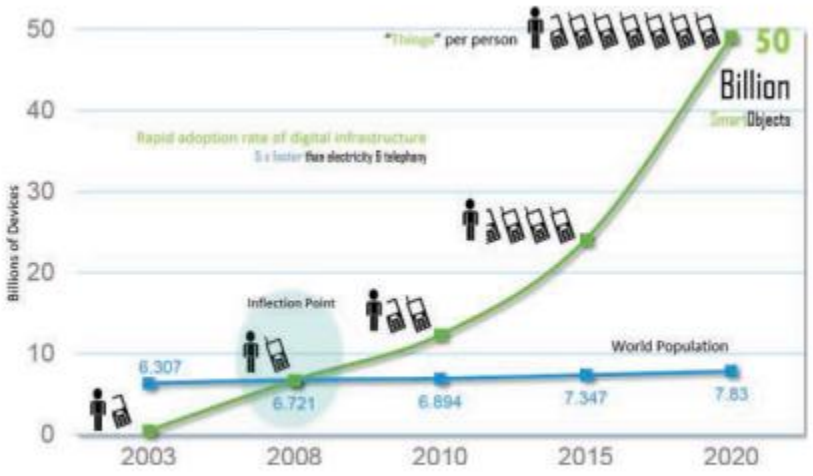


Figure 1-2 *The Rapid Growth in the Number of Devices Connected to the Internet*

The following examples illustrate some of the benefits of IoT and their impact:

Connected Roadways

- Connected roadways is the term associated with both the driver and driverless cars fully integrating with the surrounding transportation infrastructure.

- Self-driving vehicles need always-on, reliable communications and data from other transportation-related sensors to reach their full potential.

Connected Factory

- Industrial enterprises around the world are retooling their factories with advanced technologies and architectures to resolve these problems and boost manufacturing flexibility and speed.
- These improvements help them achieve new levels of overall equipment effectiveness, supply chain responsiveness, and customer satisfaction.
- A convergence of factory-based operational technologies and architectures with global IT networks is starting to occur, and this is referred to as the connected factory.

Smart Connected Buildings

- Sensors are often used to control the heating, ventilation, and air-conditioning (HVAC) system.
- Temperature sensors are spread throughout the building and are used to influence the building management system's (BMS's) control of air flow into a room**.**

Smart Creatures

- Sensors can be placed on animals and even insects just as easily as on machines.
- Living "things" can also be connected to the Internet and this connection can provide important results

9.Discuss IOT challenges. +1 (5 MARKS) (8 MARKS)

Challenge	**Description**
Scale	• While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger. • For example, one large electrical utility in Asia recently began deploying IPv6-based smart meters on its electrical grid. • While this utility company has tens of thousands of employees (which can be considered IP nodes in the network), the number of meters in the service area is tens of millions. • This means the scale of the network the utility is

	managing has increased by more than 1,000-fold!
Security	• Threat surface is now greatly expanded, and if a device gets hacked, its connectivity is a major concern. • A compromised device can serve as a launching point to attack other devices and systems. • IoT security is also pervasive across just about every facet of IoT.
Privacy	• As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. • This data can range from health information to shopping patterns and transactions at a retail establishment.
Big data and data analytics	• IoT and its large number of sensors is going to trigger a deluge of data that must be handled. • This data will provide critical information and insights if it can be processed in an efficient manner. • The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner.
Interoperability	• Various protocols and architectures are competing for market share and standardization within IoT. • Some of these protocols and architectures are based on proprietary elements, and others are open. • Recent IoT standards are helping minimize this problem, but there are often various protocols and implementations available for IoT networks.

10.With a neat diagram ,explain architecture of IOT. (4 MARKS)

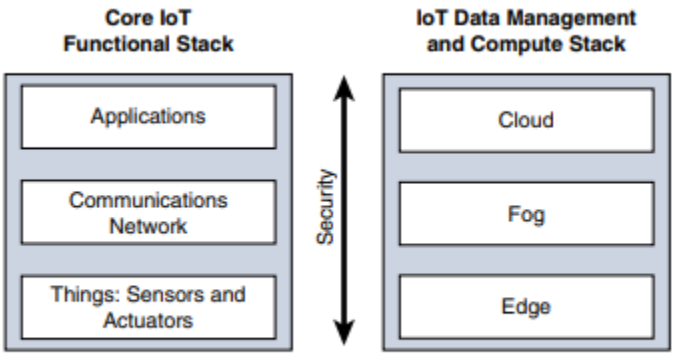
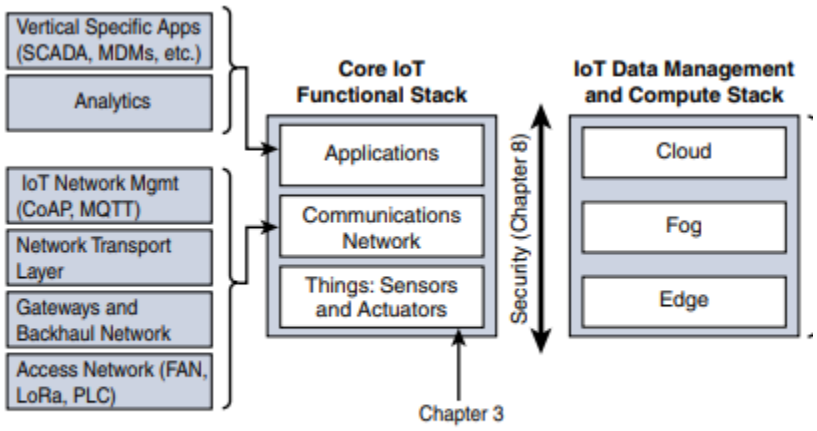


Figure 2-6 *Simplified IoT Architecture*



Expanded View of the Simplified IoT Architecture

- The network communications layer of the IoT stack itself involves a significant amount of detail and incorporates a vast array of technologies.
- The network communications layer needs to consolidate these together, offer gateway and backhaul technologies, and ultimately bring the data back to a central location for analysis and processing.
- Core IoT Functional Stack can be expanded into sublayers containing greater detail and specific network functions.
- For example, the communications layer is broken down into four separate sublayers: the access network, gateways and backhaul, IP transport, and operations and management sublayers.
- Applications layer typically has both analytics and industry-specific IoT control system components.
- Security is central to the entire architecture, both from network connectivity and data management perspectives.

11.Explain core IOT functional stack. (4 MARKS)

Components of core IOT functional stack”

■ **“Things” layer:** At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.

■ **Communications network layer:** When smart objects are not self-contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology.

This layer has four sublayers:

- ■ **Access network sublayer**
- ■ **Gateways and backhaul network sublayer**
- ■ **Network transport sublayer**
- ■ **IoT network management sublayer**

■ **Application and analytics layer:** At the upper layer, an application needs to process the collected data, not only to control the smart objects, when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the “things” or other systems to adapt to the analyzed conditions and change the behaviors or parameters.

12.Explain the concepts of Intersection Movement Assist with graphical representation. (5 MARKS)

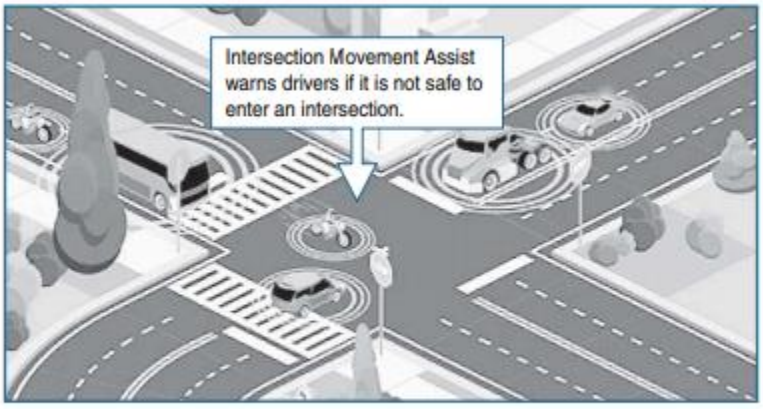


Figure 1-4 *Application of Intersection Movement Assist*

- This application warns a driver (or triggers the appropriate response in a self-driving car) when it is not safe to enter an intersection due to a high probability of a collision—perhaps because another car has run a stop sign or strayed into the wrong lane.

- Because of the communications system between the vehicles and the infrastructure, this sort of scenario can be handled quickly and safely
- IMA is one of many possible roadway solutions that emerge when we start to integrate IoT with both traditional and self-driving vehicles.

13.Explain IOT data management and compute stack. (8 MARKS)

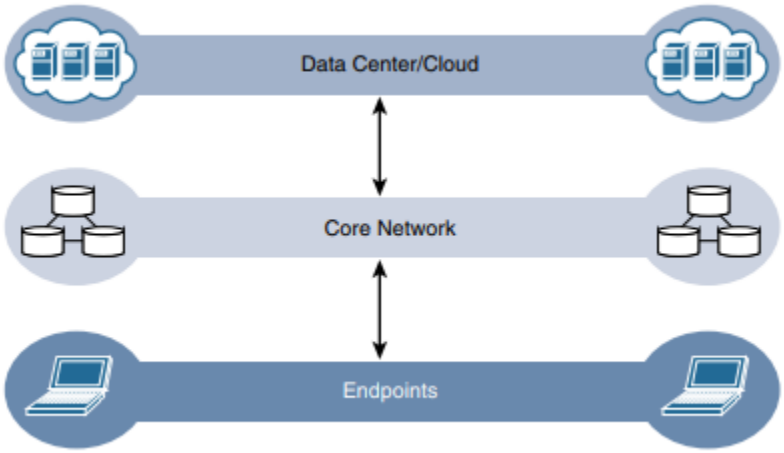


Figure 2-14 *The Traditional IT Cloud Computing Model*

- Data management in traditional IT systems is very simple. The endpoints (laptops, printers, IP phones, and so on) communicate over an IP core network to servers in the data center or cloud.
- Data is generally stored in the data center, and the physical links from access to core are typically high bandwidth, i.e., access to IT data is quick.
- The data generated by IoT sensors is one of the single biggest challenges in building an IoT system.
- As data volume increases, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system.

  These new requirements include the following:

  Minimizing latency:
- Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service.
- Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

  Conserving network bandwidth:

- Offshore oil rigs generate 500 GB of data weekly.
- Commercial jets generate 10 TB for every 30 minutes of flight.
- It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud and it is not necessary because many critical analyses do not require cloud-scale processing and storage.

Increasing local efficiency:

- Collecting and securing data across a wide geographic area with different environmental conditions may not be useful.
- The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away.
- Analyzing both areas in the same cloud system may not be necessary for immediate efficiency

MODULE-2

1.With a neat diagram, explain how actuator and sensors interact with physical world classify actuator based on energy type. (8 marks) +1

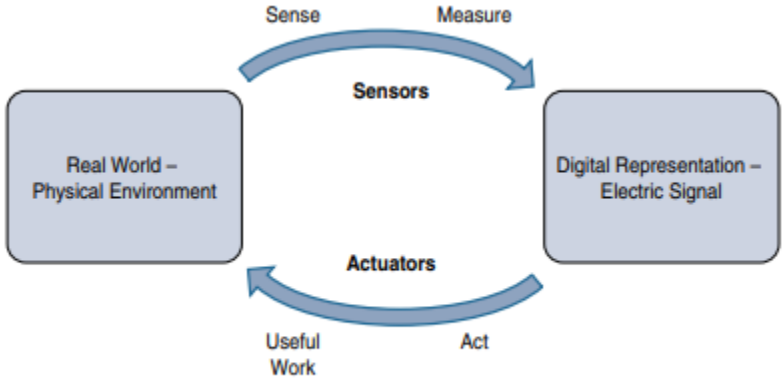


Figure 3-4 *How Sensors and Actuators Interact with the Physical World*

- Sensors are designed to sense and measure practically any measurable variable in the physical world.
- They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).
- Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.

- IoT sensors are devices that sense and measure the physical world and (typically) signal their measurements as electric signals sent to some type of microprocessor or microcontroller for additional processing.
- The human brain signals motor function and movement, and the nervous system carries that information to the appropriate part of the muscular system.
- Similarly, a processor can send an electric signal to an actuator that translates the signal into some type of movement (linear, rotational, and so on) or useful work that changes or has a measurable impact on the physical world.
- This interaction between sensors, actuators, and processors and the similar functionality in biological systems is the basis for various technical fields, including robotics and biometrics

Table 3-2 *Actuator Classification by Energy Type*

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor

Type	Examples
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

2. List out the limitations of the smart objects in WSN is and explain the data aggregation in WSN with a neat diagram. (8 marks) +1

The following are some of the most significant limitations of the smart objects in WSNs:

- Limited processing power
- Limited memory
- Lossy communication
- Limited transmission speeds
- Limited power

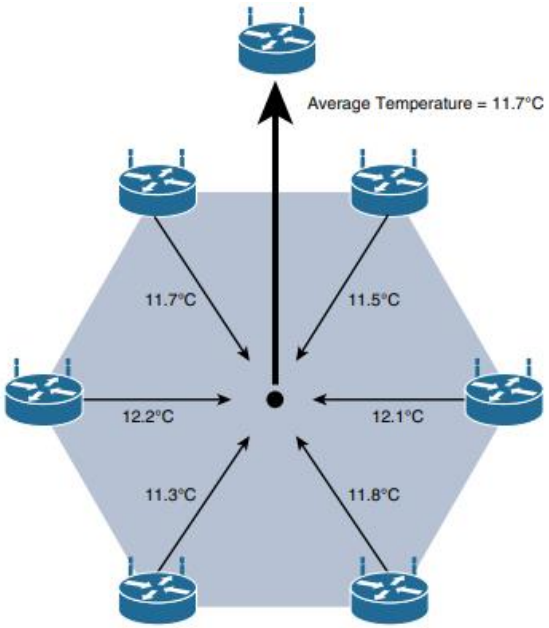


Figure 3-9 *Data Aggregation in Wireless Sensor Networks*

- The figure shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.
- These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSNs with very large numbers of deployed smart objects.
- While there are certain instances in which sensors continuously stream their measurement data, this is typically not the case.
- Wirelessly connected smart objects generally have one of the following two communication patterns:

  ■ Event-driven: Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.

  ■ Periodic: Transmission of sensory information occurs only at periodic intervals.
- The decision of which of these communication schemes is used depends greatly on the specific application.

3. What is Zigbee? Explain 802.15.4 physical layer, MAC layer, and security. (8 marks) +1

- ZigBee is one of the most well-known protocols built on an IEEE 802.15.4 foundation.
- On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles.

802.15.4 physical layer

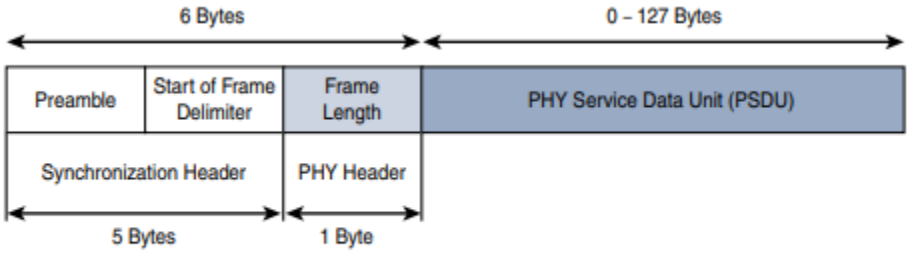


Figure 4-5 *IEEE 802.15.4 PHY Format*

- The synchronization header for this frame is composed of the Preamble and the Start of Frame Delimiter fields.
- The Preamble field is a 32-bit 4-byte (for parallel construction) pattern that identifies the start of the frame and is used to synchronize the data transmission.
- The Start of Frame Delimiter field informs the receiver that frame contents start immediately after this byte.
- The PHY Header portion of the PHY frame is a frame length value.
- It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY.

MAC layer

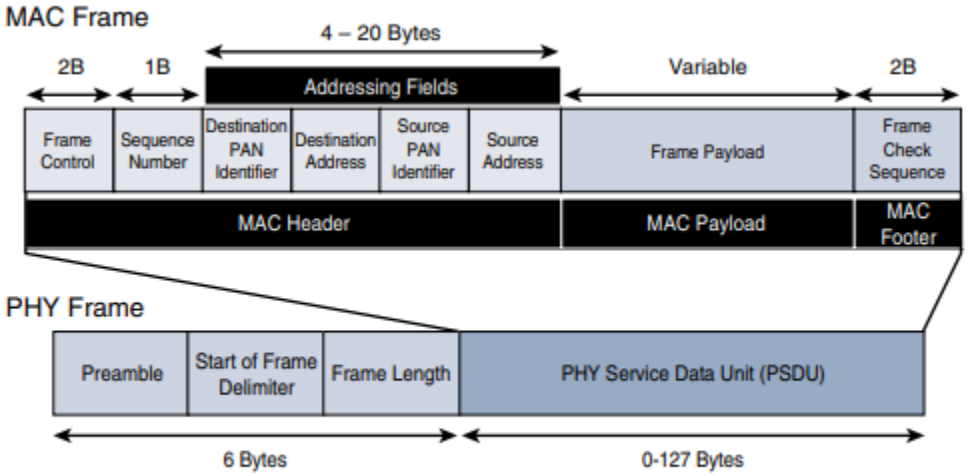


Figure 4-6 *IEEE 802.15.4 MAC Format*

- The 802.15.4 MAC layer performs the following tasks:

  ■ Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)

  ■ PAN association and disassociation by a device

  ■ Device security

  ■ Reliable link communications between two peer MAC entities

Security

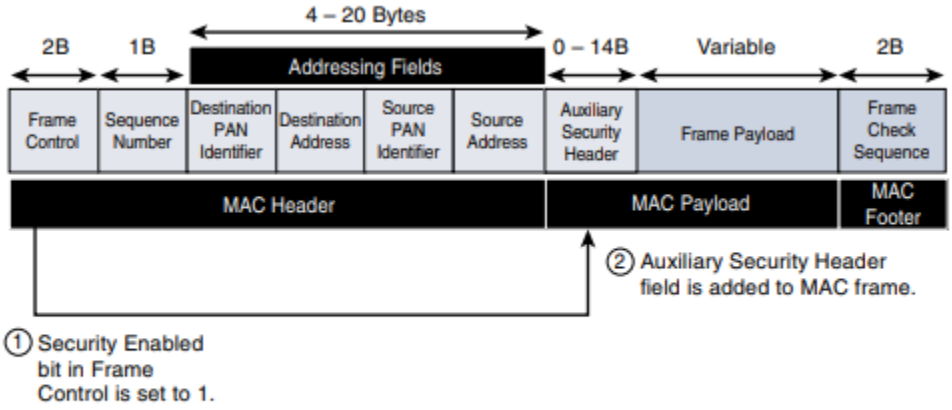


Figure 4-8 *Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions*

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data.
- AES is a block cipher - means it operates on fixed-size blocks of data.
- In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent.
- This is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption

4. Explain LoRa WAN standard and alliance MAC layer and security. (8 marks)

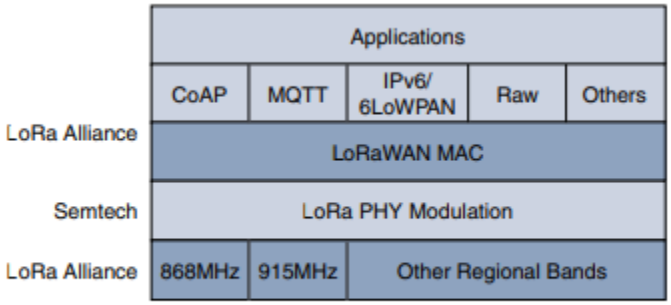


Figure 4-15 *LoRaWAN Layers*

- LPWA technologies open new business opportunities to both services providers and enterprises considering IoT solutions.
- An unlicensed-band LPWA technology, is known as LoRaWAN.
- Initially, LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named Cycleo. Later, Cycleo was acquired by Semtech.
- Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors.

- To differentiate from the physical layer modulation known as LoRa, the LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols

MAC Layer

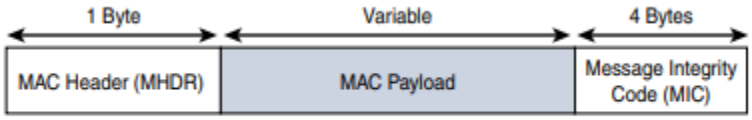


Figure 4-16 *High-Level LoRaWAN MAC Frame Format*

- The LoRaWAN specification documents three classes of LoRaWAN devices:

  ■ Class A:

- This class is the default implementation.
- Since it is Optimized for battery-powered nodes, it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting.
- Two receive windows are available after each transmission.

  ■ Class B:

- This class was designated “experimental” in LoRaWAN 1.0.1 until it can be better defined.
- A Class B node or endpoint should get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process.

  ■ Class C:

- This class is particularly adapted for powered nodes.
- This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.

Security

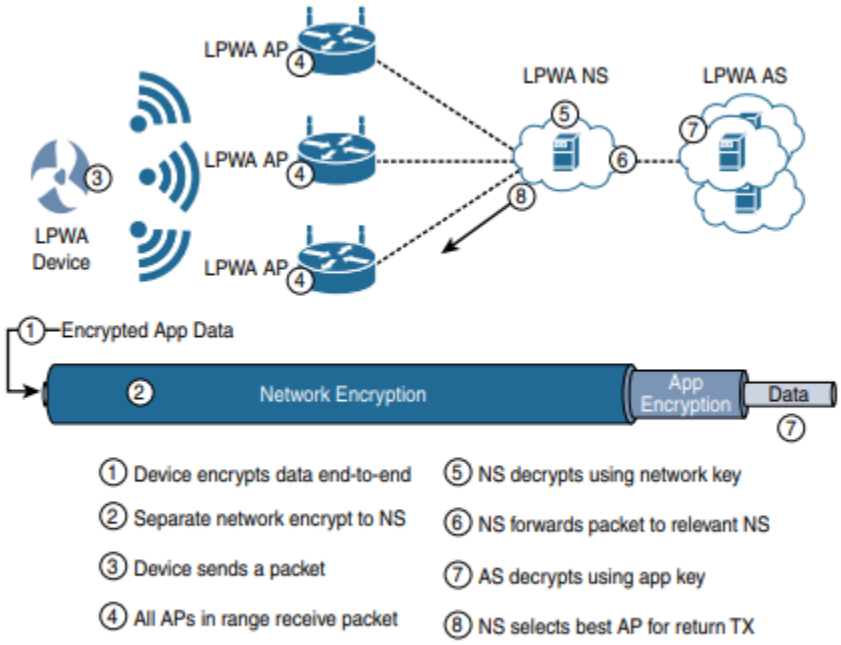


Figure 4-18 *LoRaWAN Security*

- Security in a LoRaWAN deployment applies to different components of the architecture.
- LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.
- The first layer, called "**network security**" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server.
- Also, it protects LoRaWAN packets by performing encryption based on AES.

- The second layer is an **application session key** (AppSKey), which performs encryption and decryption functions between the endpoint and its application server.
- Further, it computes and checks the application-level MIC, if included.
- This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access

5. List and explain different types of sensors . (8 marks)

Table 3-1 *Sensor Types*

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Sensor Types	Description	Examples
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

6.Elaborate on small physical objects and small virtual objects. (4 marks)

- A smart object is an object that enhances the interaction with other smart objects as well as with people also.
- Smart objects are utilized widely to transform the physical environment to a digital world using the Internet of things (IoT) technologies.
- A smart object carries blocks of application logic that make sense for their local situation and interact with human users.
- A smart object sense, log, and interpret the occurrence within themselves and the environment, and intercommunicate with each other and exchange information with people.
- The work of smart object has focused on technical aspects (such as software infrastructure, hardware platforms, etc.) and application scenarios. Application areas

range from supply-chain management and enterprise applications (home and hospital) to healthcare and industrial workplace support. As for human interface aspects of smart-object technologies are just beginning to receive attention from the environment.

7.Explain "IOT access technologies". (4 marks)

(brief points in question 3)

8. What is SANET? Explain some advantages and disadvantages that a wireless based solution offers . (8 marks)

- A sensor/actuator network (SANET), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment.
- The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner.
- SANETs offer highly coordinated sensing and actuation capabilities.
- Smart homes are a type of SANET that display this coordination between distributed sensors and actuators.
- For example, smart homes can have temperature sensors that are strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators.
- When a sensor detects a specified temperature, this can trigger an actuator to take action and heat or cool the home as needed.

Advantages:

- Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
- Simpler scaling to a large number of nodes
- Lower implementation costs
- Easier long-term maintenance
- Effortless introduction of new sensor/actuator nodes
- Better equipped to handle dynamic/rapid topology changes

Disadvantages:

- Potentially less secure (for example, hijacked access points)
- Typically, lower transmission speeds
- Greater level of impact/influence by environment

9. Define smart objects. Explain it characteristics (5 marks)

Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way.

A smart object has the following four defining characteristics

- **Processing Unit**: A smart object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensor(s), coordinating control signals to any actuators, and controlling a variety of functions on the smart object, including the communication and power systems.
- **Sensor(s) and /or actuator(s):** A smart object is capable of interacting with the physical world through sensors and actuators. A smart object does not need to contain both sensors and actuators. In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.
- **Communication Device:** The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network).
  Communication devices for smart objects can be either wired or wireless.
- **Power Source:** Smart objects have components that need to be powered. Interestingly, the most significant power consumption usually comes from the communication unit of a smart object.

10. What are constrained Devices and constrained node networks ? Classify them. (6 marks)

Class	Definition
Class 0	• This class of nodes is severely constrained with < 10KB of memory and < 100KB of flash processing • These nodes are battery powered. • They do not have resources to directly implement IP stack and associated security mechanisms
Class 1	• The processing and code space characteristics of class 1 are lower than expected for a complete IP stack implementation • They cannot easily communicate with nodes employing a full IP stack. • These nodes can implement optimized stack specifically designed for constrained nodes such as CoAP (constrained Application protocol
Class 2	• They are characterized by running full implementation of an IP stack on

	embedded devices. • They contain more than 50KB of memory and 250KB of Flash, so they can be fully integrated in IP networks.

MODULE -3

1.With a neat diagram, explain 6LOWPAN protocol header compression and fragmentation. (8 marks) +1

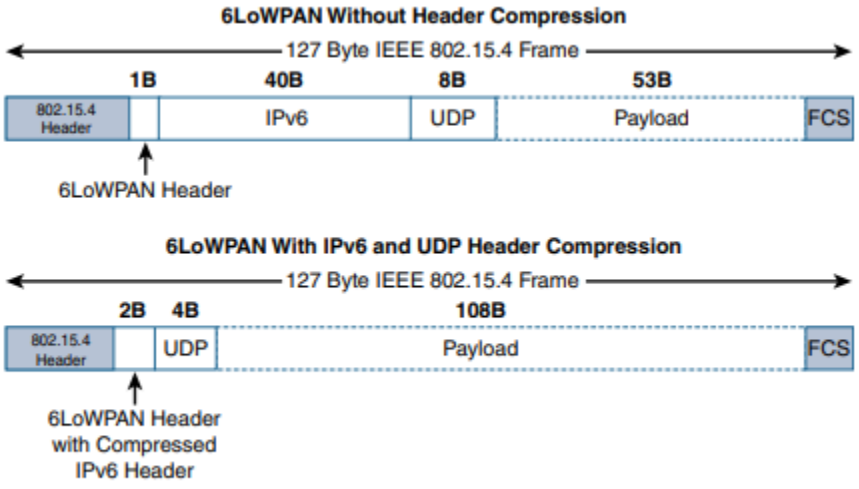


Figure 5-4 *6LoWPAN Header Compression*

- 6LoWPAN header compression is stateless, and conceptually it is not too complicated.
- However, a number of factors affect the amount of compression, such as implementation of RFC 4944 versus RFC 6922, whether UDP is included, and various IPv6 addressing scenarios.
- At a high level, 6LoWPAN works by taking advantage of shared information known by all nodes from their participation in the local network.
- **6LoWPAN frame without any header compression enabled**: The full 40-byte IPv6 header and 8-byte UDP header are visible. The 6LoWPAN header is only a single byte in this case. Notice that uncompressed IPv6 and UDP headers leave only 53 bytes of data payload out of the 127-byte maximum frame size in the case of IEEE 802.15.4.
- **The 6LoWPAN header** increases to 2 bytes to accommodate the compressed IPv6 header, and UDP has been reduced in half, to 4 bytes from 8. Most importantly, the header compression has allowed the payload to more than double, from 53 bytes to 108 bytes, which is obviously much more efficient.
- **Fragmentation**

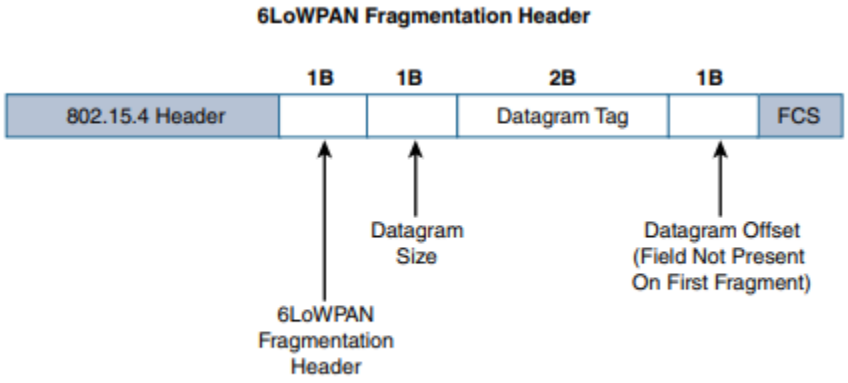


Figure 5-5 *6LoWPAN Fragmentation Header*

- The fragment header utilized by 6LoWPAN is composed of three primary fields: Datagram Size, Datagram Tag, and Datagram Offset.
- The 1-byte Datagram Size field specifies the total size of the unfragmented payload.
- Datagram Tag identifies the set of fragments for a payload.
- The Datagram Offset field delineates how far into a payload a particular fragment occurs.
- 6LoWPAN fragmentation header field itself uses a unique bit value to identify that the subsequent fields behind it are fragment fields as opposed to another capability, such as header compression

2.List and explain the key advantages of internet protocol. (4 marks)

- **Open and standards-based:** The Internet of Things creates a new paradigm in which devices, applications, and users can leverage a large set of devices and functionalities while guaranteeing interchangeability and interoperability, security, and management.
- **Versatile**: A large spectrum of access technologies is available to offer connectivity of "things" in the last mile.
- **Scalable**: As the common protocol of the Internet, IP has been massively deployed and tested for robust scalability.
- **Manageable and highly secure:** One of the benefits is a well-understood network management and security protocols, mechanisms, and toolsets that are widely available.
- **Stable and resilient:** IP has been around for 30 years, and it is clear that IP is a workable solution.
- **The innovation factor:** The past two decades has largely established the adoption of IP as a factor for increased innovation.

- **Ubiquitous**: IP is the most universal protocol when you look at what is supported across the various IoT solutions and industry verticals.
- **Consumers' market adoption:** The common protocol that links IoT in the consumer space to these devices is IP.

3.Explain RPL encryption and authentication on constraint nodes. (4 marks)

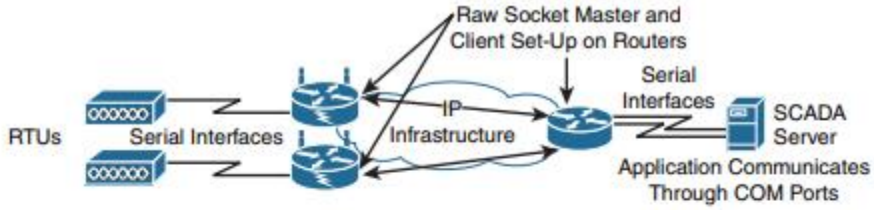
ACE

- The Authentication and Authorization for Constrained Environments (ACE) working group is tasked with evaluating the applicability of existing authentication and authorization protocols and documenting their suitability for certain constrained-environment use cases.
- Once the candidate solutions are validated, the ACE working group will focus its work on CoAP with the Datagram Transport Layer Security (DTLS) protocol.
- The ACE working group may investigate other security protocols later, with a particular focus on adapting whatever solution is chosen to HTTP and TLS.

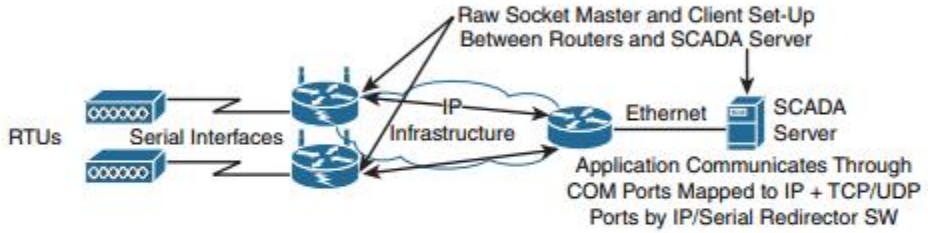
DICE

- New generations of constrained nodes implementing an IP stack over constrained access networks are expected to run an optimized IP protocol stack.
- In constrained environments secured by DTLS, CoAP can be used to control resources on a device.
- The DTLS in Constrained Environments (DICE) working group focuses on implementing the DTLS transport layer security protocol in these environments.
- The first task of the DICE working group is to define an optimized DTLS profile for constrained nodes.
- DICE working group is considering the applicability of the DTLS record layer to secure multicast messages and investigating how the DTLS handshake in constrained environments can get optimized.

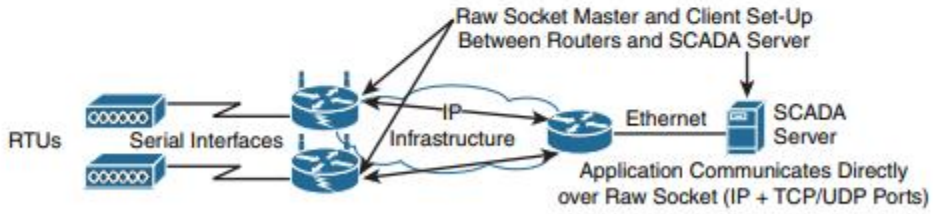
4.Explain tunneling legacy SCADA over IP networks and SCADA protocol translation with a neat diagram (8 marks)



Scenario A: Raw Socket between Routers – no change on SCADA server



Scenario B: Raw Socket between Router and SCADA Server – no SCADA application change on server but IP/Serial Redirector software and Ethernet interface to be added



Scenario C: Raw Socket between Router and SCADA Server – SCADA application knows how to directly communicate over a Raw Socket and Ethernet interface

Figure 6-3 *Raw Socket TCP or UDP Scenarios for Legacy Industrial Serial Protocols*

- Deployments of legacy industrial protocols, such as DNP3 and other SCADA protocols, in modern IP networks need flexibility when integrating several generations of devices or operations
- Native support for IP can vary and may require different solutions.
- Ideally, end-to-end native IP support is preferred, using a solution like IEEE 1815-2012 in the case of DNP3.
- Transport of the original serial protocol over IP can be achieved either by tunneling using raw sockets over TCP or UDP or by installing an intermediate device that performs protocol translation between the serial protocol version and its IP implementation.
- A raw socket connection simply denotes that the serial data is being packaged directly into a TCP or UDP transport.
- A socket in this instance is a standard application programming interface (API) composed of an IP address and a TCP or UDP port

- It is used to access network devices over an IP network.
- More modern industrial application servers may support this capability
- Older versions typically require another device or piece of software to handle the transition from pure serial data to serial over IP using a raw socket.

5.Describe MQIT frameworks and message format in detail. (8 marks)

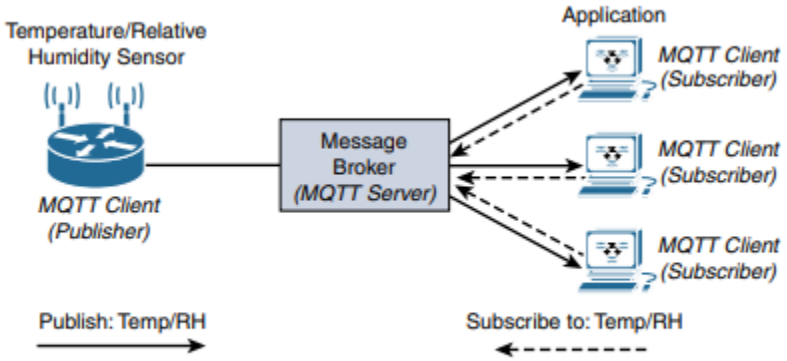


Figure 6-10 *MQTT Publish/Subscribe Framework*

- Message Queuing Telemetry Transport (MQTT) protocol is now standardized by the organization for the Advancement of Structured Information Standards (OASIS).
- An MQTT client can act as a publisher to send data (or resource information) to an MQTT server acting as an MQTT message broker.
- The MQTT client on the left side of figure is a temperature (Temp) and relative humidity (RH) sensor that publishes its Temp/RH data.
- The MQTT server (or message broker) accepts the network connection along with application messages, such as Temp/RH data, from the publishers.
- It also handles the subscription and un subscription process and pushes the application data to MQTT clients acting as subscribers.
- The application on the right side of Figure is an MQTT client that is a subscriber to the Temp/RH data being generated by the publisher or sensor on the left.
- This model, where subscribers express a desire to receive information from publishers, is well known.
- A great example is the collaboration and social networking application Twitter

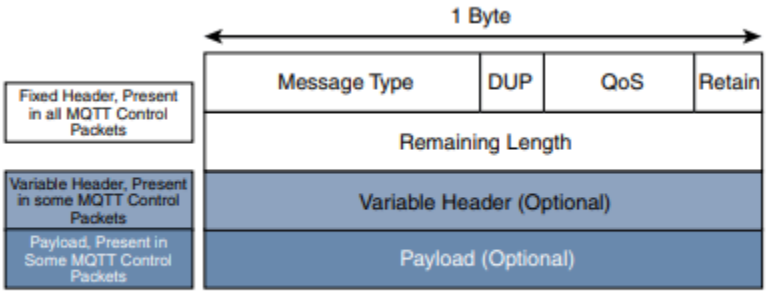


Figure 6-11 *MQTT Message Format*

- MQTT is a lightweight protocol because each control packet consists of a 2-byte fixed header with optional variable header fields and optional payload.
- Compared to the CoAP message format, MQTT contains a smaller header of 2 bytes compared to 4 bytes for CoAP.
- The first MQTT field in the header is Message Type, which identifies the kind of MQTT packet within a message.
- Fourteen different types of control packets are specified in MQTT version 3.1.1.
- Each of them has a unique value that is coded into the Message Type field.
- Values 0 and 15 are reserved.

(Extra)

Table 6-2 *MQTT Message Types*

Message Type	Value	Flow	Description
CONNECT	1	Client to server	Request to connect
CONNACK	2	Server to client	Connect acknowledgement
PUBLISH	3	Client to server Server to client	Publish message
PUBACK	4	Client to server Server to client	Publish acknowledgement
PUBREC	5	Client to server Server to client	Publish received
PUBREL	6	Client to server Server to client	Publish release
PUBCOMP	7	Client to server Server to client	Publish complete
SUBSCRIBE	8	Client to server	Subscribe request
SUBACK	9	Server to client	Subscribe acknowledgement
UNSUBSCRIBE	10	Client to server	Unsubscribe request

Message Type	Value	Flow	Description
UNSUBACK	11	Server to client	Unsubscribe acknowledgement
PINGREQ	12	Client to server	Ping request
PINGRESP	13	Server to client	Ping response
DISCONNECT	14	Client to server	Client disconnecting

6.Explain working of IP as the IOT network layer. (8 MARKS)

(combine points from Question 2 and 7)

7.Write a note on Business case for IP. (4 MARKS)

- Data flowing from or to "things" is consumed, controlled, or monitored by data center servers either in the cloud or in locations that may be distributed or centralized.
- Dedicated applications are then run over virtualized or traditional operating systems or on network edge platforms (for example, fog computing).
- These lightweight applications communicate with the data center servers.
- Therefore, the system solutions combining various physical and data link layers call for an architectural approach with a common layer(s) independent from the lower (connectivity) and/or upper (application) layers.
- This is how and why the Internet Protocol (IP) suite started playing a key architectural role in the early 1990s.
- IP was not only preferred in the IT markets but also for the OT environment.

8.Discuss need for optimization. (4 MARKS)

- In addition to coping with the integration of non-IP devices, you may need to deal with the limits at the device and network levels that IoT often imposes.
- Therefore, optimizations are needed at various layers of the IP stack to handle the restrictions that are present in IoT networks.

Constrained nodes

- Depending on its functions in a network, an architecture may or may not offer similar characteristics compared to a generic PC or server in an IT environment. IoT constrained nodes can be classified as follows:

  Devices that are very constrained in resources, may communicate infrequently to transmit a few bytes, and may have limited security and management capabilities:
- This drives the need for the IP adaptation model, where nodes communicate through gateways and proxies.

Devices with enough power and capacities to implement a stripped-down IP stack or non-IP stack:

- In this case, you may implement either an optimized IP stack and directly communicate with application servers (adoption model) or go for an IP or non-IP stack and communicate through gateways and proxies (adaptation model).

Devices that are similar to generic PCs in terms of computing and power resources but have constrained networking capacities, such as bandwidth:

- These nodes usually implement a full IP stack (adoption model), but network design and application behaviors must cope with the bandwidth constraints
- **Constrained Networks**
- Constrained networks have unique characteristics and requirements. In contrast with typical IP networks, where highly stable and fast links are available, constrained networks are limited by low-power, low-bandwidth links.
- They operate between a few kbps and a few hundred kbps and may utilize a star, mesh, or combined network topology, ensuring proper operations.
- With a constrained network, in addition to limited bandwidth, it is not unusual for the packet delivery rate (PDR) to oscillate between low and high percentages.

9.Describe application protocol for IOT. (8 MARKS)

The Transport Layer

With the TCP/IP protocol, two main protocols are specified for the transport layer:

■ **Transmission Control Protocol (TCP):** This connection-oriented protocol requires a session to get established between the source and destination before exchanging data. You can view it as an equivalent to a traditional telephone conversation, in which two phones must be connected and the communication link established before the parties can talk.

■ **User Datagram Protocol (UDP):** With this connectionless protocol, data can be quickly sent between source and destination—but with no guarantee of delivery. This is analogous to the traditional mail delivery system, in which a letter is mailed to a destination. Confirmation of the reception of this letter does not happen until another letter is sent in response

Transport methods

- Because of the diverse types of IoT application protocols, there are various means for transporting these protocols across a network.
- The following are the categories of IoT application protocols:

- **Application layer protocol not present:** In this case, the data payload is directly transported on top of the lower layers.
  No application layer protocol is used.
- **Supervisory control and data acquisition (SCADA):** SCADA is one of the most common industrial protocols in the world, but it was developed long before the days of IP, and it has been adapted for IP networks.
- **Generic web-based protocols:** Generic protocols, such as Ethernet, Wi-Fi, and 4G/LTE, are found on many consumer- and enterprise-class IoT devices that communicate over non-constrained networks.
- **IoT application layer protocols:** IoT application layer protocols are devised to run on constrained nodes with a small compute footprint and are well adapted to the network bandwidth constraints on cellular or satellite links or constrained 6LoWPAN networks. Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), covered later in this chapter, are two well-known examples of IoT application layer protocols

10.Discuss the various methods used in iot application transport. (8 marks)

(in Question 9)

11.Explain the different schedule management and packet forwarding model of 6TiSCH.

(6 MARKS)

The 6TiSCH architecture defines four schedule management mechanisms:

■ **Static scheduling:**

- All nodes in the constrained network share a fixed schedule.
- Cells are shared, and nodes contend for slot access in a slotted aloha manner.
- Slotted aloha is a basic protocol for sending data using time slot boundaries when communicating over a shared medium.
- Static scheduling is a simple scheduling mechanism that can be used upon initial implementation or as a fallback in the case of network malfunction.
- The drawback with static scheduling is that nodes may expect a packet at any cell in the schedule. Therefore, energy is wasted idly listening across all cells.

■ **Neighbor-to-neighbor scheduling:**

- A schedule is established that correlates with the observed number of transmissions between nodes.

- Cells in this schedule can be added or deleted as traffic requirements and bandwidth needs change.

■ **Remote monitoring and scheduling management:**

- Time slots and other resource allocation are handled by a management entity that can be multiple hops away.
- The scheduling mechanism leverages 6top and even CoAP in some scenarios.
- This scheduling mechanism provides quite a bit of flexibility and control in allocating cells for communication between nodes.

■ **Hop-by-hop scheduling:**

- A node reserves a path to a destination node multiple hops away by requesting the allocation of cells in a schedule at each intermediate node hop in the path.

There are three 6TiSCH forwarding models:

■ **Track Forwarding (TF):**

- This is the simplest and fastest forwarding model.
- A “track” in this model is a unidirectional path between a source and a destination.
- This track is constructed by pairing bundles of receive cells in a schedule with a bundle of receive cells set to transmit.
- A frame received within a particular cell or cell bundle is switched to another cell or cell bundle.
- This forwarding occurs regardless of the network layer protocol.

■ **Fragment forwarding (FF):**

- This model takes advantage of 6LoWPAN fragmentation to build a Layer 2 forwarding table.
- IPv6 packets can get fragmented at the 6LoWPAN sublayer to handle the differences between IEEE 802.15.4 payload size and IPv6 MTU.
- Additional headers for RPL source route information can further contribute to the need for fragmentation.

■ **IPv6 Forwarding (6F):**

- This model forwards traffic based on its IPv6 routing table.
- Flows of packets should be prioritized by traditional QoS (quality of service) and RED (random early detection) operations.

- QoS is a classification scheme for flows based on their priority, and RED is a common congestion avoidance mechanism.

12.Explain the raw socket tunneling of SCADA using different scenarios. (6 MARKS)

(same as question 4)

13. What is COAP? Draw COAP Message format. Explain its fields. (6 MARKS)

Constrained Application Protocol (CoAP) resulted from the IETF Constrained RESTful Environments (CoRE) working group's efforts to develop a generic framework for resource-oriented applications targeting constrained nodes and networks.

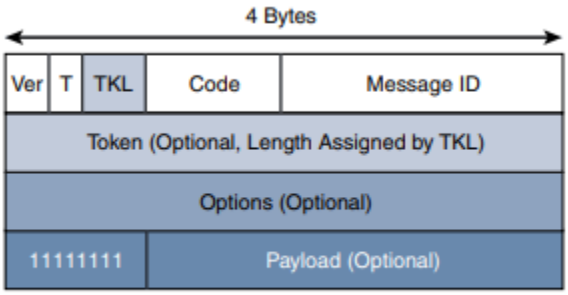


Figure 6-7 *CoAP Message Format*

Table 6-1 *CoAP Message Fields*

CoAP Message Field	Description
Ver (Version)	Identifies the CoAP version.
T (Type)	Defines one of the following four message types: Confirmable (CON), Non-confirmable (NON), Acknowledgement (ACK), or Reset (RST). CON and ACK are highlighted in more detail in Figure 6-9.
TKL (Token Length)	Specifies the size (0–8 Bytes) of the Token field.
Code	Indicates the request method for a request message and a response code for a response message. For example, in Figure 6-9, GET is the request method, and 2.05 is the response code. For a complete list of values for this field, refer to RFC 7252.
Message ID	Detects message duplication and used to match ACK and RST message types to Con and NON message types.
Token	With a length specified by TKL, correlates requests and responses.
Options	Specifies option number, length, and option value. Capabilities provided by the Options field include specifying the target resource of a request and proxy functions.
Payload	Carries the CoAP application data. This field is optional, but when it is present, a single byte of all 1s (0xFF) precedes the payload. The purpose of this byte is to delineate the end of the Options field and the beginning of Payload.

14.Compare between COAP and MQTT. (4 MARKS)

Table 6-3 *Comparison Between CoAP and MQTT*

Factor	CoAP	MQTT
Main transport protocol	UDP	TCP
Typical messaging	Request/response	Publish/subscribe
Effectiveness in LLNs	Excellent	Low/fair (Implementations pairing UDP with MQTT are better for LLNs.)
Security	DTLS	SSL/TLS
Communication model	One-to-one	many-to-many
Strengths	Lightweight and fast, with low overhead, and suitable for constrained networks; uses a RESTful model that is easy to code to; easy to parse and process for constrained devices; support for multicasting; asynchronous and synchronous messages	TCP and multiple QoS options provide robust communications; simple management and scalability using a broker architecture
Weaknesses	Not as reliable as TCP-based MQTT, so the application must ensure reliability.	Higher overhead for constrained devices and networks; TCP connections can drain low-power devices; no multicasting support

MODULE-4

1.Explain the elements of Hadoop with a neat diagram. (7 MARKS)

- Hadoop was originally developed as a result of projects at Google and Yahoo!, and the original intent for Hadoop was to index millions of websites and quickly return search results for open-source search engines.

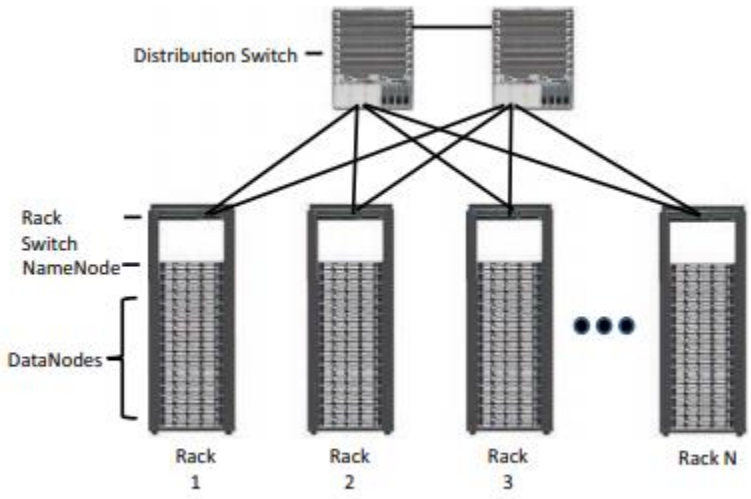


Figure 7-8 *Distributed Hadoop Cluster*

There are two key elements

■ Hadoop Distributed File System (HDFS): A system for storing data across multiple nodes. HDFS has specialized nodes in the cluster

- NameNodes:
  - These are a critical piece in data adds, moves, deletes, and reads on HDFS.
  - They coordinate where the data is stored, and maintain a map of where each block of data is stored and where it is replicated.
  - All interaction with HDFS is coordinated through the primary (active) NameNode, with a secondary (standby) NameNode notified of the changes in the event of a failure of the primary.
  - The NameNode takes write requests from clients and distributes those files across the available nodes in configurable block sizes, usually 64 MB or 128 MB blocks.
  - The NameNode is also responsible for instructing the DataNodes where replication should occur.
- DataNodes:
  - These are the servers where the data is stored at the direction of the NameNode.
  - It is common to have many DataNodes in a Hadoop cluster to store the data.
  - Data blocks are distributed across several nodes and often are replicated three, four, or more times across nodes for redundancy.
  - Once data is written to one of the DataNodes, the DataNode selects two (or more) additional nodes, based on replication policies, to ensure data redundancy across the cluster.
  - Disk redundancy techniques such as Redundant Array of Independent Disks (RAID) are generally not used for HDFS because the NameNodes and DataNodes coordinate block-level redundancy with this replication technique.

■ MapReduce: A distributed processing engine that splits a large task into smaller ones that can be run in parallel

Both MapReduce and HDFS take advantage of this distributed architecture to store and process massive amounts of data and are thus able to leverage resources from all nodes in the cluster.

2.Explain neural network in machine learning with a detailed example. (5 MARKS)

- Neural networks are ML methods that mimic the way the human brain works.
- When you look at a human figure, multiple zones of your brain are activated to recognize colors, movements, facial expressions, and so on. Your brain combines these elements to conclude that the shape you are seeing is human.
- Neural networks mimic the same logic as a human brain.
- The information goes through different algorithms (called units), each of which is in charge of processing an aspect of the information.
- The resulting value of one unit computation can be used directly or fed into another unit for further processing to occur.
- For example, a neural network processing human image recognition may have two units in a first layer that determines whether the image has straight lines and sharp angles—because vehicles commonly have straight lines and sharp angles, and human figures do not.
- If the image passes the first layer successfully (because there are no or only a small percentage of sharp angles and straight lines), a second layer may look for different features (presence of face, arms, and so on), and then a third layer might compare the image to images of various animals and conclude that the shape is a human (or not).
- The great efficiency of neural networks is that each unit processes a simple test, and therefore computation is quite fast.

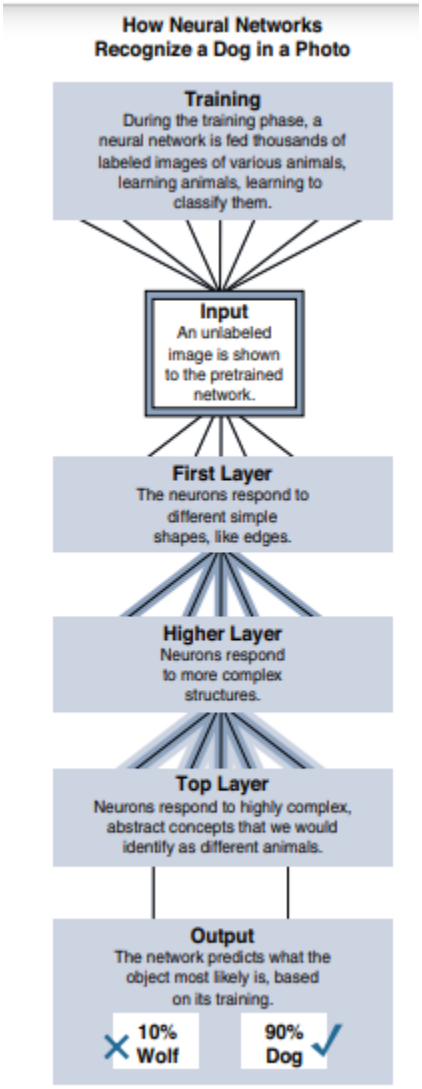


Figure 7-6 *Neural Network Example*

3.Describe the components of FNF. (4 MARKS) +1 (8 MARKS)

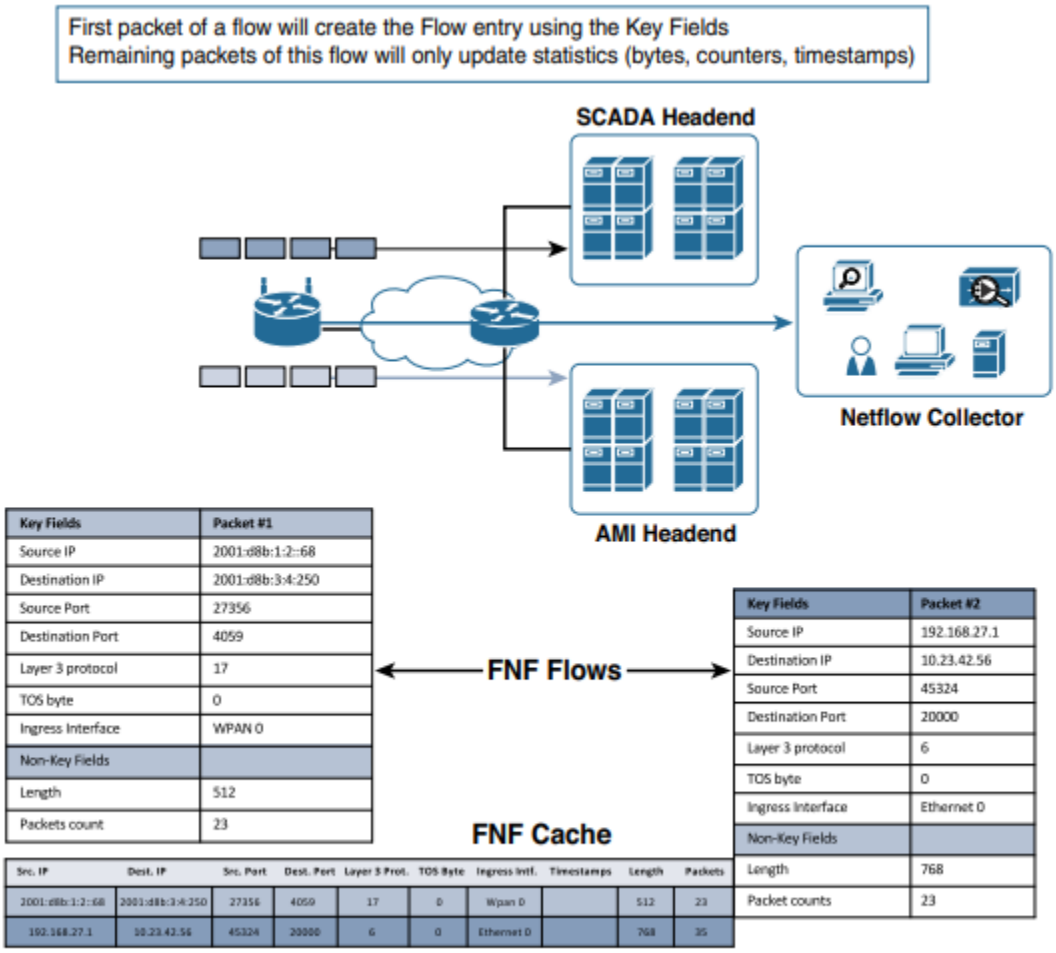


Figure 7-17 *Flexible NetFlow overview*

FNF has the following main components

■ FNF Flow Monitor (NetFlow cache):

- The FNF Flow Monitor describes the NetFlow cache or information stored in the cache. The Flow Monitor contains the flow record definitions with key fields and non-key fields within the cache.
- Part of the Flow Monitor is the Flow Exporter, which contains information about the export of NetFlow information, including the destination address of the NetFlow collector.
- The Flow Monitor includes various cache characteristics, including timers for exporting, the size of the cache, and, if required, the packet sampling rate.

■ FNF flow record:

- A flow record is a set of key and non-key NetFlow field values used to characterize flows in the NetFlow cache.
- Flow records may be predefined for ease of use or customized and user defined.

- A typical predefined record aggregates flow data and allows users to target common applications for NetFlow.
- User-defined records allow selections of specific key or non-key fields in the flow record.
- The user-defined field is the key to Flexible NetFlow, allowing a wide range of information to be characterized and exported by NetFlow.
- It is expected that different network management applications will support specific ser-defined and predefined flow records based on what they are monitoring.

■ FNF Exporter:

- There are two primary methods for accessing NetFlow data:
    - Using the show commands at the command-line interface (CLI)
    - Using an application reporting tool.
- NetFlow Export, unlike SNMP polling, pushes information periodically to the NetFlow reporting collector.
- The Flexible NetFlow Exporter allows the user to define where the export can be sent, the type of transport for the export, and properties for the export.
- Multiple exporters can be configured per Flow Monitor

■ Flow export timers: Timers indicate how often flows should be exported to the collection and reporting server.

■ NetFlow export format: This simply indicates the type of flow reporting format.

■ NetFlow server for collection and reporting: This is the destination of the flow export. It is often done with an analytics tool that looks for anomalies in the traffic patterns.

4.Explain Formal Risk Analysis Structures. (8 MARKS)

There are two risk assessment frameworks:

■ OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) from the Software Engineering Institute at Carnegie Mellon University

■ FAIR (Factor Analysis of Information Risk) from The Open Group

OCTAVE

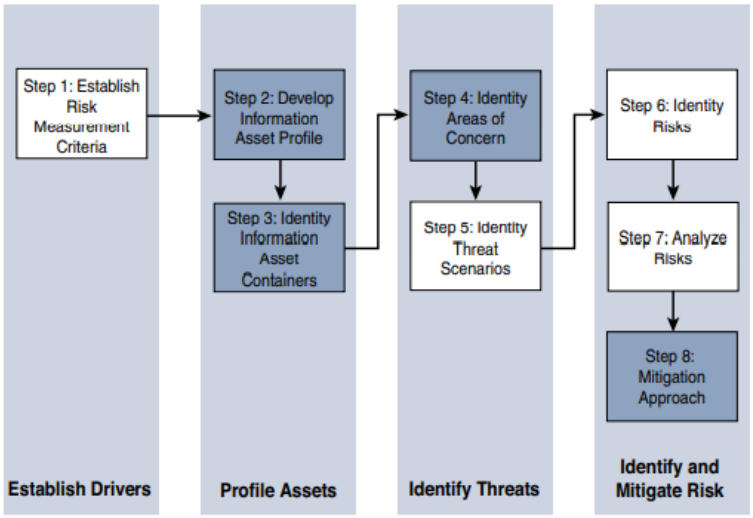


Figure 8-5 *OCTAVE Allegro Steps and Phases (see https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/).*

- The first step of the OCTAVE Allegro methodology is to establish a risk measurement criterion. OCTAVE provides a fairly simple means of doing this with an emphasis on impact, value, and measurement.
- The second step is to develop an information asset profile. This profile is populated with assets, a prioritization of assets, attributes associated with each asset, including owners, custodians, people, explicit security requirements, and technology assets.
- The third step is to identify information asset containers. This is the range of transports and possible locations where the information might reside.
- The fourth step is to identify areas of concern. At this stage, the analyst looks to risk profiles and delves into the previously mentioned risk analysis. It is no longer just facts, but there is also an element of creativity that can factor into the evaluation.
- The fifth step is where threat scenarios are identified. Threats are broadly identified as potential undesirable events. This definition means that results from both malicious and accidental causes are viable threats. In the context of operational focus, this is a valuable consideration. It is at this point that an explicit identification of actors, motives, and outcomes occurs
- At the sixth step risks are identified. Within OCTAVE, risk is the possibility of an undesired outcome. This is extended to focus on how the organization is impacted.
- The seventh step is risk analysis, with the effort placed on qualitative evaluation of the impacts of the risk. Here the risk measurement criteria defined in the first step are explicitly brought into the process.

- Finally, mitigation is applied at the eighth step. There are three outputs or decisions to be taken at this stage. One may be to accept a risk and do nothing, other than document the situation, potential outcomes, and reasons for accepting the risk. The second is to mitigate the risk with whatever control effort is required. The final possible action is to defer a decision, meaning risk is neither accepted nor mitigated. This may imply further research or activity, but it is not required by the process

FAIR

- FAIR (Factor Analysis of Information Risk) is a technical standard for risk definition from The Open Group.
- FAIR has clear applications within operational technology.
- FAIR places emphasis on both unambiguous definitions and the idea that risk and associated attributes are measurable.
- It allows for non-malicious actors as a potential cause for harm, but it goes to greater lengths to emphasize the point.
- FAIR defines six forms of loss, four of them externally focused and two internally focused

5.Explain the Purdue model for control hierarchy and OT network characteristics.

(8 MARKS)

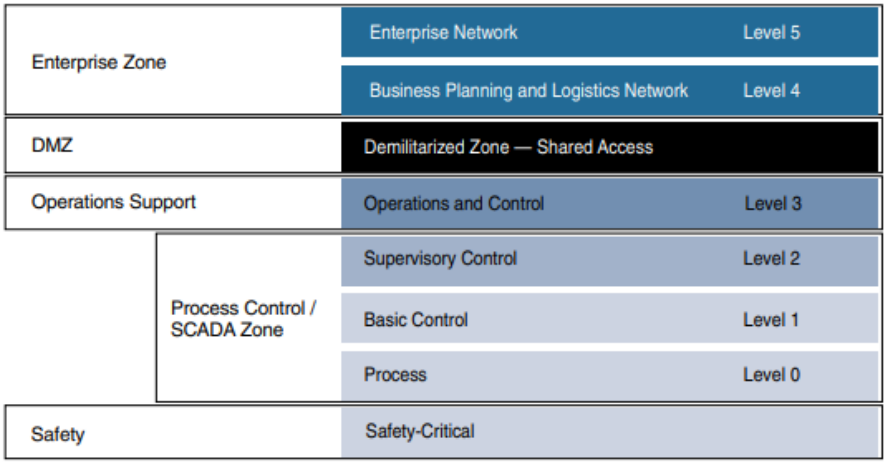


Figure 8-3 *The Logical Framework Based on the Purdue Model for Control Hierarchy*

This model identifies levels of operations and defines each level. The enterprise and operational domains are separated into different zones.

■ Enterprise zone

■ Level 5: Enterprise network:

■ Level 4: Business planning and logistics network:

■ Industrial demilitarized zone

■ DMZ: The DMZ provides a buffer zone where services and data can be shared between the operational and enterprise zones.

■ Operational zone

■ Level 3: Operations and control:

■ Level 2: Supervisory control:

■ Level 1: Basic control:

■ Level 0: Process:

■ Safety zone

■ Safety-critical: This level includes devices, sensors, and other equipment used to manage the safety functions of the control system

OT network characteristics

- In an OT environment (Levels 0–3), there are typically two types of operational traffic.
- The first is local traffic that may be contained within a specific package or area to provide local monitoring and closed-loop control.
- This is the traffic that is used for real-time (or near-real-time) processes and does not need to leave the process control levels.
- The second type of traffic is used for monitoring and control of areas or zones or the overall system.
- SCADA traffic is a good example of this, where information about remote devices or summary information from a function is shared at a system level so that operators can understand how the overall system, or parts of it, are operating.
- They can then implement appropriate control commands based on this information

6.What do you mean by data analytics for IOT? Explain. (8 MARKS)

- In the world of IoT, the creation of massive amounts of data from sensors is common and one of the biggest challenges—not only from a transport perspective but also from a data management standpoint.
- A great example of the surge of data that can be generated by IoT is found in the commercial aviation industry and the sensors that are deployed throughout an aircraft.
- Modern jet engines are fitted with thousands of sensors that generate a 10GB of data per second.

- Modern jet engine can be equipped with around 5000 sensors. Therefore, a twin engine commercial aircraft with these engines operating on average 8 hours a day will generate over 500 TB of data daily, and this is just the data from the engines.
- A single wing of a modern jumbo jet is equipped with 10,000 sensors.
- Across the world, there are approximately 100,000 commercial flights per day. The amount of IoT data coming just from the commercial airline business is overwhelming.
- Analyzing this amount of data in the most efficient manner possible falls under the umbrella of data analytics.
- Data analytics must be able to offer actionable insights and knowledge from data, no matter the amount or style, in a timely manner, or the full benefits of IoT cannot be realized.

7.Discuss Bigdata analytics tools and technology. (4 MARKS)

Big data analytics can consist of many different software pieces that together collect, store, manipulate, and analyze all different data types. Generally, the industry looks to the "Three Vs" to categorize big data:

■ Velocity:

- Velocity refers to how quickly data is being collected and analyzed.
- Hadoop Distributed File System is designed to ingest and process data very quickly.
- Smart objects can generate machine and sensor data at a very fast rate and require database or file systems capable of equally fast ingest functions.

■ Variety:

- Variety refers to different types of data.
- Often data is categorized as structured, semi-structured, or unstructured.
- Different database technologies may only be capable of accepting one of these types.
- Hadoop is able to collect and store all three types.
- This can be beneficial when combining machine data from IoT devices that is very structured in nature with data from other sources, such as social media or multimedia, that is unstructured.

■ Volume:

- Volume refers to the scale of the data.
- This is measured from gigabytes on the very low end to petabytes or even exabytes of data on the other extreme.

- Generally, big data implementations scale beyond what is available on locally attached storage disks on a single node.
- It is common to see clusters of servers that consist of dozens, hundreds, or even thousands of nodes for some large deployments.

8.With a case study relate the concept of securing IOT (8 MARKS)

A Fortune-100 enterprise needed a highly secure solution for its multi-million dollar video surveillance system.

- This enterprise initiated a multi-year, multi-million-dollar video surveillance system upgrade.
- The end result was significantly better for surveillance capturing and management functionality, but a compromised network security.
- The enterprise found itself under attack by an organized Far East adversary.
- It exploited firmware vulnerabilities in these camera systems and rapidly compromised nearly every camera on the network.
- Without firmware updates being extracted from the different camera manufacturers and then carefully applied to every installed camera, the enterprise had to consider a complete hardware and installation re-deployment with updated acceptable cameras.
- The new secure cameras had much higher price, so overall installation cost would be significantly higher.
- The enterprise can lessen the threats to its video infrastructure by implementing an agile, simple and highly secure solution: GoSilent.
- This device has been widely recognized as the most portable and easiest to configure hardware VPN solution for securing network communications to and from remote locations, no matter what IP device is connecting to it.

9.Explain in detail how IT and OT security practices and systems vary in real time. (8 MARKS)

(same as question 5)

10.Discuss OCTAVE and FAIR formal risk analysis. (8 MARK)

(Same as question 4)

11.Explain in details the core functions of edge analytics with necessary diagrams.

(8 MARKS)

There are three stages:

■ **Raw input data:** This is the raw data coming from the sensors into the analytics

processing unit.

■ **Analytics processing unit (APU):**

Figure 7-12 illustrates the stages of data processing in an edge APU.

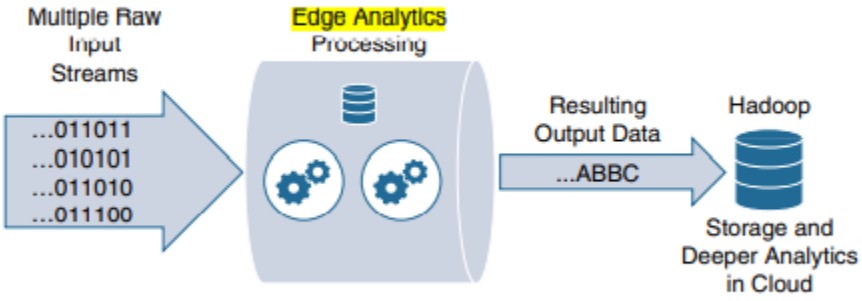


Figure 7-12 *Edge Analytics Processing Unit*

- The APU filters and combines data streams, organizes them by time windows, and performs various analytical functions.
- It is at this point that the results may be acted on by micro services running in the APU.
- In order to perform analysis in real-time, the APU needs to perform the following functions:

  ■ Filter: The streaming data generated by IoT endpoints is likely to be very large, and most of it is irrelevant.

  For example, a sensor may simply poll on a regular basis to confirm that it is still reachable. This information is not really relevant and can be mostly ignored.

  The filtering function identifies the information that is considered important.

  ■ Transform: In the data warehousing world, Extract, Transform, and Load (ETL) operations are used to manipulate the data structure into a form that can be used for other purposes.

  Analogous to data warehouse ETL operations, in streaming analytics, once the data is filtered, it needs to be formatted for processing.

  ■ Time: As the real-time streaming data flows, a timing context needs to be established. This could be to correlated average temperature readings from sensors on a minute-by-minute basis.

■ Output streams: The data that is output is organized into insightful streams and is used to influence the behavior of smart objects, and passed on for storage and further processing in the cloud. Communication with the cloud often happens through a standard publisher/subscriber messaging protocol, such as MQTT

12.Explain the different steps and phases of OCTAVE Allegro methodology (8 MARKS)

(same as question 4)

13.Explain secured network infrastructure by using process control hierarchy model

(8 MARKS)

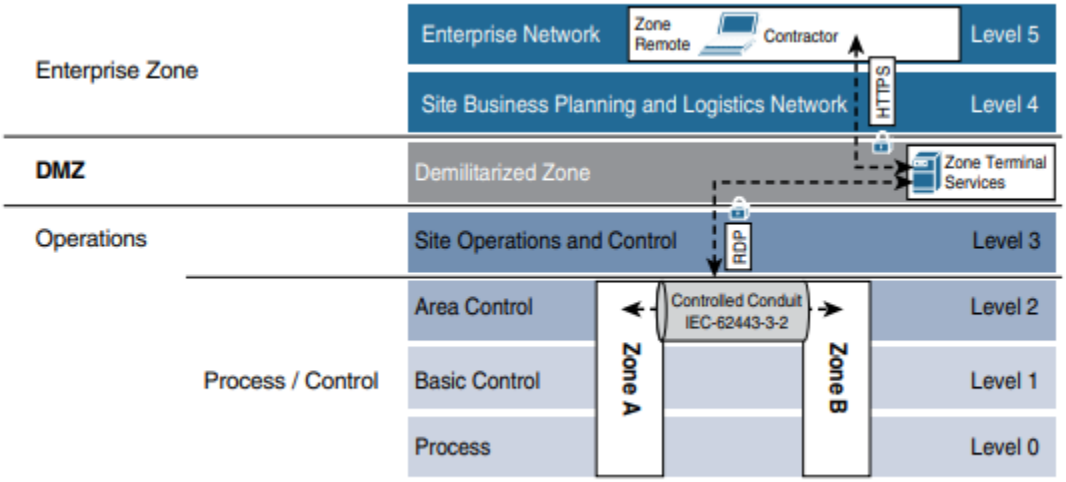


Figure 8-6 *Security Between Levels and Zones in the Process Control Hierarchy Model*

- First analyze and secure the basic network design.
- It is a basic rule of ISA99 and IEC 62443 that functions should be segmented into zones (cells) and that communication crossing the boundaries of those zones should be secured and controlled through the concept of conduits.
- After the network is physically mapped, the next step is to perform a connectivity analysis through the switch and router ARP tables and DHCP requests within the network infrastructure.
- Firewall and network infrastructure data contribute to understanding what devices are talking to other devices and the traffic paths over which this is done.
- At upstream levels, consider traffic controls such as denial of service (DoS) protection, traffic normalization activities, and quality of service (QoS) controls (such as marking and black-holing or rate-limiting scavenger-class traffic).
- Network infrastructure should also provide the ability to secure communications between zones via secured conduits.
- The primary method is encrypted communications in the form of virtual private networks (VPNs).

- VPNs can come in multiple forms, such as site-to-site, which would be appropriate between a utility substation and a control center, or perhaps in cell-to-cell communications.
- The next discovery phase should align with the software and configurations of the assets on the network. The network infrastructure and its status are within the network admin's view, but the individual assets likely are not. At this point, organizational cooperation is required for success. At the operations level, similar cooperation is required with those responsible for the maintenance of the OT assets.

MODULE-5

1.Explain the following with respect to Arduino programing. (8 MARKS)

1. **Structure:**
2. **Functions**
3. **Variables**
4. **Flow control statements**
5. **Data type**
6. **Constants.**

Structure: Arduino programs can be divided in three main parts: Structure, values and functions.

Software structure consists of two main functions – Setup () function and Loop () function.

```
void setup()            //Preparation function used to declare variables
{                       //First function that runs only one in the program
    Statement(s);       //used to set pins for serial communication
}
void loop()             //Execution block where instructions are executed repeatedly
{                       //this is the core of the Arduino programming
    Statements();       //Functionalities involve reading inputs, triggering outputs etc.
}
```

Functions: A function is a piece of code that has a name and set of statements executed when function is called. Functions are declared by its type followed with name of a function

Syntax : type functionName(parameters)

Variables: Local variables are those which are declared inside the function or block.

It can be used only inside that function or block.

They cannot function outside the block.

Example:

```
Void setup () {

}

Void loop () {
        int x,y;
        int z; Local variable declaration
        x=0;
        y=0; actual initialization
        z=0;
}
```

Flow control statements

Flow control Statements	

if	if(some_variable == value)
	{
	Statement(s); //Evaluated only if comparison results in a true value
	}

if...else	if(input==HIGH)
	{
	Statement(s); //Evaluated only if comparison results in a true value
	}
	else
	{
	Statement(s); //Evaluated only if comparison results in a false value
	}

for	for(initialization;condition;expression)
	{
	Dosomething; //Evaluated till condition becomes false
	}
	for(int p=0;p<5;p++) //declares p, tests if less than 5, increments by 1

	{
	digitalWrite(13,HIGH); //sets pin 13 ON
	delay(250); // pauses for ¼ second
	digitalWrite(13,LOW); //sets pin 13 OFF
	delay(250); //pause for ¼ second
	}

while	While loop executes until the expression inside parenthesis becomes false.
	while(some_variable ?? value)
	{
	Statement(s); //Evaluated till comparison results in a false value
	}

do...while	Bottom evaluated loop, works same way as while loop but condition is tested at the end of loop. do { Dosomething; }while(somevalue);

Data types

- It refers to a system for declaring variables and functions of different types.
- Space occupied in storage and how bit pattern is interpreted depends on type of variable.

Void	Boolean	char	Unsigned char	byte	int	Unsigned int	Word
long	Unsigned long	short	float	double	array	String-char array	String-object

Constants

Constants	Constants	Usage

	TRUE/FALSE	Boolean constants true=2 and false=0 defined in logic levels.
		if(b==TRUE)
		{
		//do something
		}

	INPUT/OUTPUT	Used with pinMode () function to define levels. pinMode (13,OUTPUT):
	HIGH/LOW	Used to define pin levels HIGH–1,ON,5 volts LOW –0,OFF, 0 volts Digital Write (13,HIGH);

2.Explain Raspberry Pi learning board (8 MARKS)

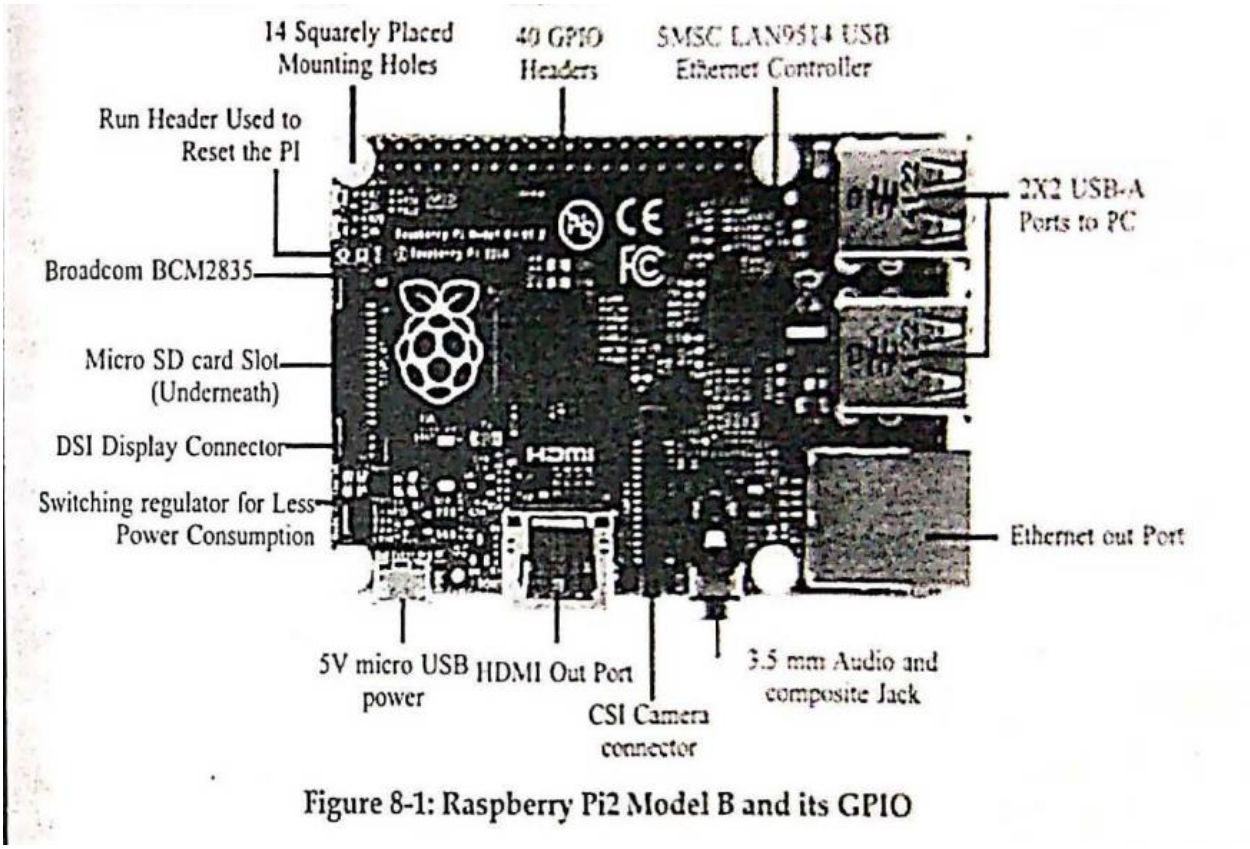


Figure 8-1: Raspberry Pi2 Model B and its GPIO

Processor:

- Broadcom BCM2835 SoC is used in Raspberry Pi 2 Board.
- It includes 900 MHz 32-bit quad-core ARM cortex A7 processor with 256 KB shared L2 cache.

- Raspberry Pi 3 board will have 1.2GHz 64-bit quad core ARM Cortex A53 processor with 512KB shared L2 Cache.

Power Source:

- It has a Micro USB port on the side for power.
- Input voltage is 5V, Input current is 2A.
- The latest Raspberry boards use a low voltage indicator to notify the user for any problems with user

SD Card:

- Raspberry Pi board does not have locally available storage.
- The working framework is stacked on a SD card which is embedded on the SD card space.

GPIO (General Purpose Input Output):

- It is a non-specific pin on a coordinated circuit to know if input/output pin can be controlled by the client at run time.
- GPIO pins can go unused after a time because they have no exceptional reason characterized.
- They can be designed to be an input/output
- It can be empowered/crippled.

DSI Display X:

- Raspberry Pi Connector S2 is the display serial interface (DSI)
- It is for connecting an LCD panel using a 15-pin ribbon cable.
- Graphic data is fed using mobile industry processor interface (MIPI) inside the Broadcom BCM2835 IC

Audio Jack:

- A standard 3.5 MM TRS connector is used for stereo sound yield.
- USB mics or USB sound cards are used for taking sound information

Status LEDs:

- There are 5 status LEDs
    - **OK - SDCard Access (by means of GPIOl6)** - named as "OK" on Model B Rev1.0 sheets and "ACT" on Model B Rev2.0 and Model A sheets
    - **POWER - 3.3 V Power** - named as "PWR" on all the boards
    - **FDX - Full Duplex (LAN) (Model B)** - marked as "FOX" on all the boards

- **LNK - Link/Activity (LAN) (Model B)** - marked as "LNK" on all the boards
- **IOM/100 - 10/I0OMbit (LAN) (Model B)**- named as "10M" on Model B Rev1.0 boards and "100" on Model B Rev2.0 and Model A boards USB Ports.

Ethernet port:

- Ethernet port is accessible on Model B and B+.
- It is associated with a system or web utilizing a standard LAN link on the Ethernet port.
- The Ethernet ports are controlled by Microchip LAN9512 LAN controller chip.

CSI connector (CSI):

- It is a serial interface.
- It is outlined by MIPI (Mobile Industry Processor Interface) organization.

JTAG headers:

- JTAG – Joint Test Action Group
- It is an association to address test point get to issues on PCB with surface mount gadgets**.**
- It founded a technique called TAP (Test Access Port) to access gadget pins by using serial port.
- In 1990, this changed to universal standard – IEEE Std 1149.2

HDMI: High Definition Multimedia Interface to give both video and sound yield.

3.Write a python program on Raspberry Pi to blink LED. (6 MARKS)

File: blink.py

```
#Access the python working environment
# !/usrtbin/python
#import the time module so as to switch LEDs on/off with the time elapsed
#import the RPI.GPIO library
import RPi.GPIO as GPIO
#use one of the two numbering system either BOARD numbers/BCM
# Refer to the channel numbers on the Broadcom SOC.
GPI0.setmode(GPIO.BCM)
#Configure Pin 17 as an OUTPUT
GPIO.setup( 17,GPIO.0UT)
#Configure Pin 27 as an OUTPUT
GPIO.setup(27,GPIO.OUT)
```

```
#Tum up LEDs on pin 17
GPIO.output(l 7,GPIO.HIGH)
#Turn up LEDs on pin 27
GPIO.output(27,GPIO.HIGH)'
#wait for I second
time.sleep(!)
#Turn up LEDs off on pin 17
GPIO.output( 17,GPIO.LO\V)
#Turn up LEDs off on pin 27
GPIO.output(27,GPJ0.LOW)
#wait for I second
time.sleep( I)
File:blink_cvcr.py
#Access the python working environment
#!/usrtbin/python
#import the time module so aJ to switch LEDs on/off with the time elapsed
import time
#import the RPI.GPIO library
import Hi.Cif'I0 a, (,PIO
1/u~c one of the t·.vo numberinf ~y;tcrn either B0 :\RD n:mi!-/:t";/H( :'> I
II Hcfcr to th~ chJnr.d nurnb,:r-, or, rhc Bmmkom SOC.
Gl'I0.sctrncrdc(GPIO.BO!>
//Configure pin 17 ;md 27 to be an OUTPUT pin,
GPIO.sctup( 17,Gl'l0.0 UT)
GPIO.sctup(27,GPI0.Ol1T)
#Use while: construe! which rJm infi:ii!c number ot' time·; there by bli:ikin;;
whilc I:
LEDs forever
#Turn up LEDs on
GPI0.output(l7,GPI0.HIGH)
GPIO.output(27,GPIO.HIGH>
time.sleep( I)
```

#Tum up LEDs off

GPI0.output(l7,GPIO.LOWi

GPI0.output(27,GPIO.LOW)

time.sleep(!)

4.Explain smart city security architecture. (6 MARKS)

- A serious concern of most smart cities and their citizens is data security.
- Vast quantities of sensitive information are being shared at all times in a layered, real time architecture, and cities have a duty to protect their citizens' data from unauthorized access, collection, and tampering.
- In general, citizens feel better about data security when the city itself, and not a private entity, owns public or city-relevant data.
- It is up to the city and the officials who run it to determine how to utilize this data A security architecture for smart cities must utilize security protocols to fortify each layer of the architecture and protect city data.
- Security protocols should authenticate the various components and protect data transport throughout.
- Starting from the street level, sensors should have their own security protocols.
- There are three common elements for security on the network layer:
- Firewall: It is located at the edge and it should be IPsec- and VPN-ready and include user and role-based access.
- VLAN: It provides end-to-end segmentation of data transmission further protecting data from rogue intervention.
- Encryption: Encryption starts at the sensor level. In some cases, sensor-to-gateway link uses one type of encryption and gateway-to-application connection uses another encryption

5.Write a short note on: (4 MARKS)

1. **IOT challenges**

   For the IoT industry to thrive there are three categories of challenges to overcome

   - Technology:
     - IoT Systems are poorly designed and implemented, using diverse protocols and technologies that create complex configurations.

    - Lack of mature IoT technologies and business processes.
    - Limited guidance for life cycle maintenance and management of IoT devices.
    - Limited best practices available for IoT developers.
    - There is a lack of standards for authentication and authorization of IoT edge devices.
- Business
    - Customer demands and requirements change constantly.
    - New uses for devices—as well as new devices—sprout and grows at breakneck speeds.
    - Inventing and reintegrating must-have features and capabilities are expensive and take time and resources.
    - The uses for Internet of Things technology are expanding and changing—often in uncharted waters.
- Society
    - Voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party
    - Many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries

2. Backhaul Technologies.

- A common communication system organizes multiple smart objects in a given area around a common gateway.
- The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a long-range medium which is called the backhaul, to a headend central station where the information is processed.
- This information exchange is a Layer 7 (application) function, which is the reason this object is called a gateway.

- On IP networks, this gateway also forwards packets from one IP network to another, and it therefore acts as a router.
- Backhaul technologies include: Free-space optical (FSO) Point-to-point microwave radio relay transmission (terrestrial or, in some cases, by satellite) Point-to-multipoint microwave-access technologies, such as LMDS, Wi-Fi, WiMAX, etc., can also function for backhauling purposes.

6.Give a brief note on Ardino UNO. (4 MARKS) +1

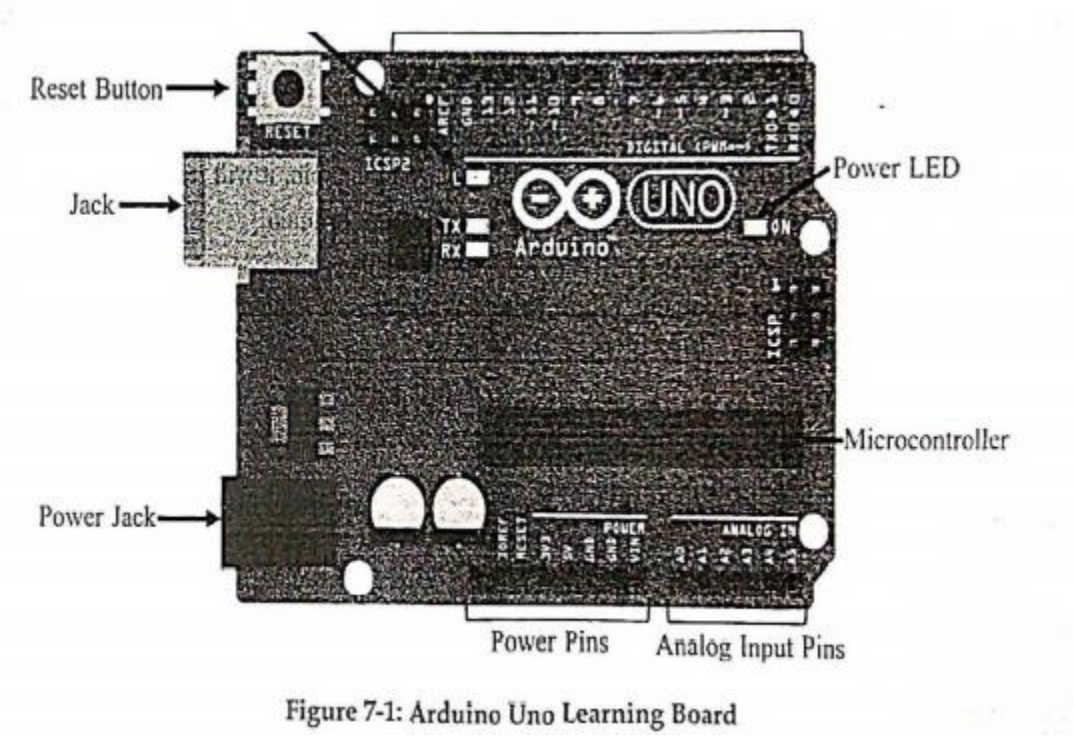


Figure 7-1: Arduino Uno Learning Board

The parts are:

- **Microcontroller:** the ATmega328p is the Arduino brain. Everything on the Arduino board is meant to support this microcontroller
- **Digital pins:** Arduino has 14 digital pins, labeled from 0 to 13 that can act as inputs or outputs.
- **PWM pins:** These arc digital pins marked with a - (pins 11, 10, 9, 6, 5 and 3). PWM ~lands for "pulse width modulation" and allows to make digital pins output "fake" varying amounts of voltage. You'll learn more about PWM later.
- **TX and RX pins:** digital pins 0 1. T stands for "transmit" and the R for "receive". Arduino uses these pins to communicate with the computer.
- **LED attached to digital pin 13:** This is useful for an easy debugging of the Arduino sketches.

- **TX and RX pins:** these pins blink when there are information being sent between the computer and the Arduino.
- **Analog pins:** the analog pins are labeled from A0 to A5 and are most often used to read analog sensors. They can read different amounts of voltage between 0 and 5V.
- **Power pins:** The Arduino has 3.3V or 5V supply, which is really useful since most components require 3.3V or 5V. The pins labelled as "GND" are the ground pins.
- **Reset button:** when you press that button, the program that is currently being run in your Arduino will start from the beginning. You also have a Reset pin next to the power pins that acts as reset button. When you apply a small voltage to that pin, it will reset the Arduino.
- **Power ON LED:** will be on since power is applied to the Arduino.
- **USB jack:** Connecting a male USB A to male USB B cable is how you upload programs from your computer to your Arduino board. This also powers Arduino.
- **Power jack:** The power jack is where you connect a component to power up your Arduino (recommended voltage is 5V). There are several ways to power up Arduino: rechargeable batteries, disposable batteries, wall-warts and solar panel.

7.With a neat diagram explain Raspberry Pi board. (4 MARKS)

(same as question 2)

8.With a neat diagram explain wireless temperature monitoring system using Raspberry Pi (8 MARKS)

Components required are Raspberry Pi+ SD card, Monitor+ HOM! Cable, Keyboard & Mouse and Power supply, I Red LED and Blue LED, 2 I K resistors, push button and jumper wires, Breadboard, buzzer. I LM35 temperature sensor.

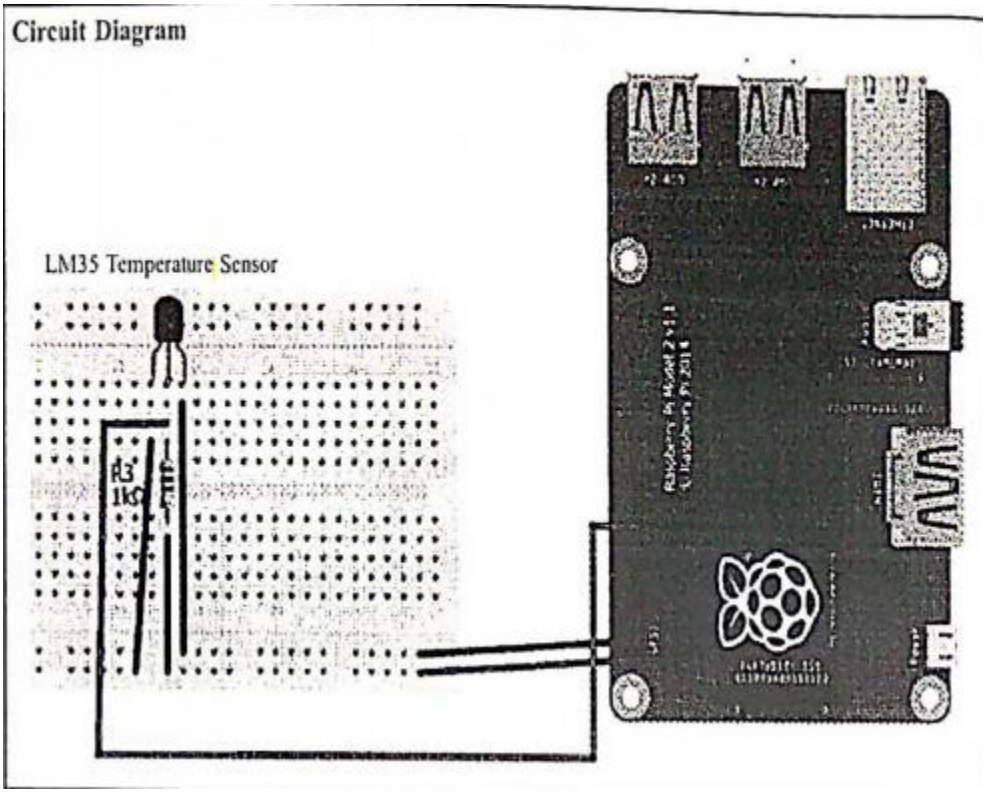


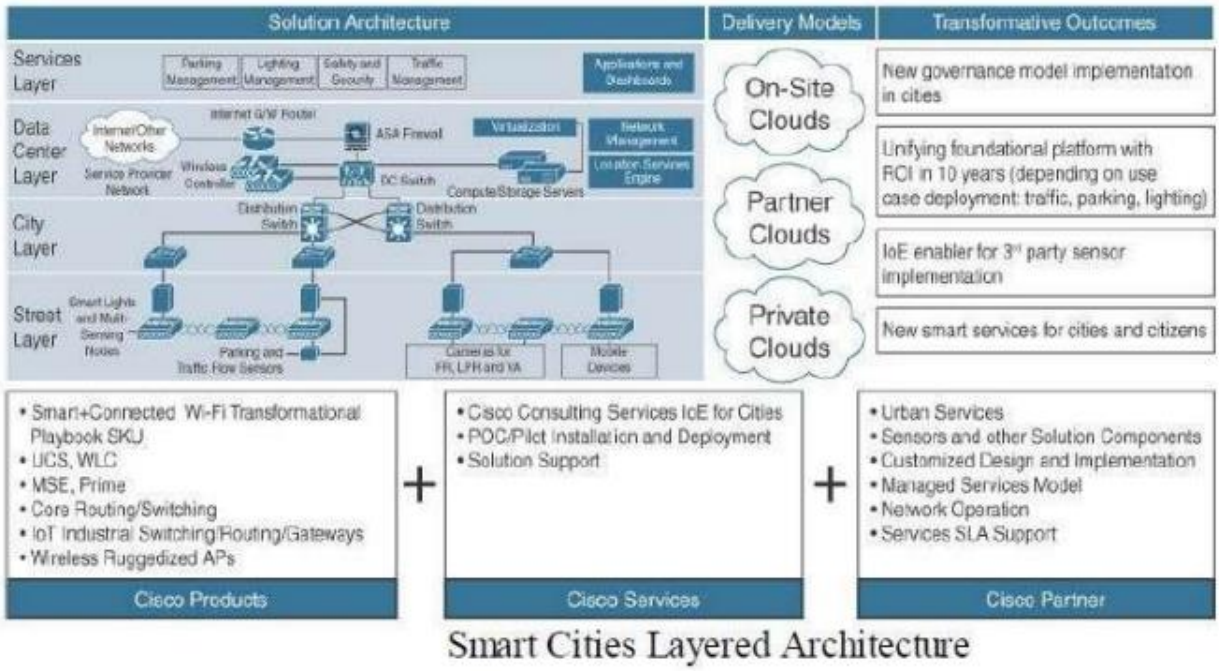
Figure shows the schematic diagram of connecting an OS I 8822 temperature sensors to Raspberry Pi board.

This example shows how to get an analog input from GPIO pins and process the input.

An infinite loop runs over the sensor which records a temperature every second.

9.Explain in detail smart city IOT architecture. +1 (8 MARKS)

- Data flows from devices at the street layer to the city network layer and connect to the data center layer, where the data is aggregated, normalized, and virtualized.
- The data center layer provides information to the services layer, which consists of the applications that provide services to the city.
- In smart cities, multiple services may use IoT solutions for many different purposes. These services may use different IoT solutions, with different protocols and different application language



Smart Cities Layered Architecture

A smart city IoT infrastructure is a four-layered architecture, as shown in Figure

Street Layer:

- The street layer is composed of devices and sensors that collect data and take action based on instructions from the overall solution, as well as the networking components needed to aggregate and collect data.
- A sensor is a data source that generates data required to understand the physical world.
- Sensor devices are able to detect and measure events in the physical world.

City Layer:

- At the city layer, which is above the street layer, network routers and switches must be deployed to match the size of city data that needs to be transported.
- This layer aggregates all data collected by sensors and the end-node network into a single transport network.
- The city layer may appear to be a simple transport layer between the edge devices and the data center or the Internet.

Data Center Layer:

- Ultimately, data collected from the sensors is sent to a data center, where it can be processed and correlated.
- Based on this processing of data, meaningful information and trends can be derived, and information can be provided back.

Service Layer:

- The true value of ICT connectivity comes from the services that the measured data can provide to different users operating within a city.
- Smart city applications can provide value to and visibility for a variety of user types, including city operators, citizens, and law enforcement.
- The collected data should be visualized according to the specific needs of each consumer of that data and the particular user experience requirements and individual use cases

10.With the case study explain smart and connected cities using Raspberry Pi (8 MARKS)

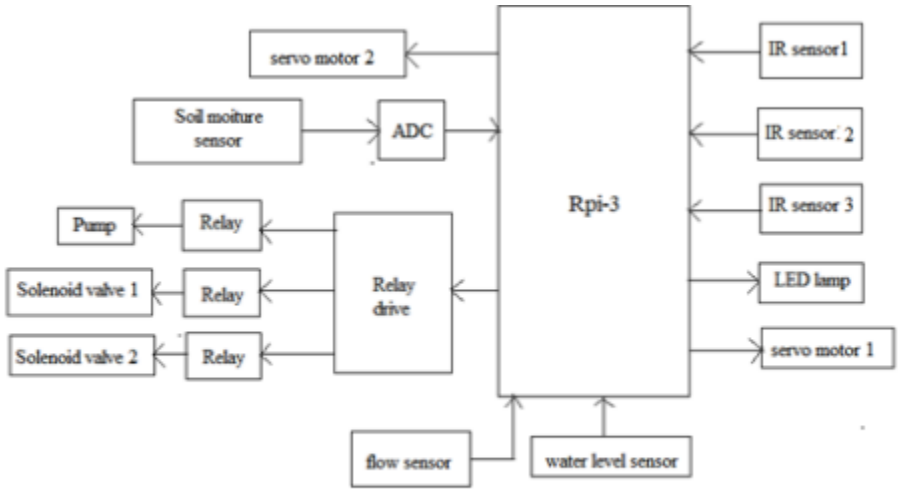


fig.(a) Block diagram

Smart and Connected cities using Raspberry Pi can be designed following three parameters.

Smart parking system:

- First, driver should check availability of parking from web using UI of mobile phones.
- If slot is available user can enter details such as name, mobile no etc.
- At night, the lamps will turn on
- IR sensors are used to detect if the slots are available or not and it will upload to the web server using Raspberry Pi controller
- Hence, such systems can be used in a smart city which becomes convenient for residents and tourists.

Smart water management:

- The central tank will be connected with solenoid valves.
- Tank will have water level indicator which shows the amount of water
- Automatic turning on of valves by using time can be done. Otherwise, user can also turn on water flow from the web.

- Water flow sensor is connected to tank to measure the flow of water distributed to each solenoid valve. This will show the user of how many liters are consumed in an area.
- Information of water consumption is updated on the Web through Raspberry Pi controller.
- If a person requires more water then they can turn on the solenoid valve through the web

Smart public garden:

- In the management of public garden solid moisture sensor can be place in the soil.
- It detects the moisture and turns on/off the water flow.
- Gate is automatically open/close through servo motors on given time or by user through the web.
- Turn on/off of light lamps can also be done by the user through a web page.

11.Write a program to record the current room temperature using Raspberry Pi. (8 MARKS)

```
import os
import glob
import time
#initialize the device
os.system('modprobe w 1-gpio')
os.system('modprobe w I-therm')
base_ dir = '/sys/bus/w I/devices/'
device_folder = glob.glob(basc_dir + '2S*')[O)
device_file = device_foldcr + '/wI _slave'
def read _temp _rnw():
        f= open(devicc_filc, 'r')
        lines = f.rcadlincs(}
        f.close()
        return lines
def read _temp():
        lines= read_temp_raw()
        while lines[O].strip(}[-3:) != 'YES':
                time.slccp(0.2)
```

```
        lines= read_temp_raw()
    equals_pos = lines[I].find('t=')
    if equals_pos != -I:
        temp_slring = lines[I][cquals_pos+2:]
        temp_c = float(temp_string) / 1000.0
        temp_f= temp_c * 9.0 / _5.0 + 32.0
    return temp_c, lemp_f
while True:
print(rcad _temp())
time.sleep( I)
```

12.Explain smart parking architecture with advantages and disadvantages (8 MARKS)

Smart parking system is a system that collects and disseminates real-time parking space availability data.

(include points from question 10)

Advantages

- Optimized parking
- Reduced traffic
- Enhanced User Experience
- Integrated Payments and POS
- Increased Safety
- Real-Time Data and Trend Insight
- Decreased Management Costs

Disadvantages

- The high cost of installation.
- Regular maintenance
- High maintenance costs and issues related to regular maintenance
- Problems of Operation or Breakdown may occur