K – 513042

Register No.

MCA Degree Examination May 2023

Second Semester

## 22MCC21 – INTERNET OF THINGS

(Regulations 2022)

Time: Three hours — Maximum: 100 marks

Answer all Questions

### Part – A (10 × 2 = 20 marks)

1. Write the role of microcontrollers and internet connectivity in IoT. [CO1,K2]
2. What are the key elements to be considered in selecting an IoT framework? [CO1,K1]
3. Define the term design patterns. [CO2,K1]
4. Interpret the difference between sensors and actuators. [CO2,K2]
5. Compare Data at Rest, Data in Use and Data in Flight. [CO3,K2]
6. How to perform functional testing on home automation system? [CO3,K2]
7. Mention any two examples of IIoT. [CO4,K1]
8. What is classification and how it works? [CO4,K2]
9. Interpret the challenges and requirements of the oil and gas industry. [CO5,K2]
10. Mention any three performance characteristics of media redundancy protocol. [CO5,K2]

### Part – B (5 × 16 = 80 marks)

11. a. i) Describe any two use-cases of IoT across industries. (10) [CO1,K2]

ii) Write short note on IoT implementation challenges. (6) [CO1,K1]

(OR)

b. i) With suitable diagram describe the major components of IoT ecosystems. (10) [CO1,K2]

ii) Compare and contrast Cisco IoT and Azure IoT. (6) [CO1,K1]

12. a. Explore design patterns for node connections, deployment strategies and infrastructure. (16) [CO2,K2]

(OR)

b. Compare four layers with seven layer IoT architecture and explain various component of seven layer architecture. (16) [CO2,K2]

13. a. Identify various challenges in IoT implementation and provide essential technology and communication infrastructure for an IoT implementation. (16) [CO3,K3]

(OR)

b. List all types of testing for Internet of Things and create a comparison chart to show which one to use and when. (16) [CO3,K3]

14. a. i) What is industry 4.0? State the benefits that artificial intelligence provides for the successful implementation of IoT. (10) [CO4,K2]

ii) Describe the use of machine learning in IoT. (6) [CO4,K2]

(OR)

b. How various security attacks take place? Explain man-in-the-middle attack and IP spoofing with suitable example. (16) [CO4,K2]

15. a. Identify various levels in industrial automation and control system model and describe the role of each layer in the model. (16) [CO5,K3]

(OR)

b. "Internet of Things improves public safety". Justify the above statement with any two relevant use case, also identify various challenges in implementation. (16) [CO5,K3]

| Bloom's Taxonomy Level | Remembering (K1) | Understanding (K2) | Applying (K3) | Analysing (K4) | Evaluating (K5) | Creating (K6) |
|---|---|---|---|---|---|---|
| Percentage | 10 | 54 | 36 | – | – | – |

# MCA Degree Examination May 2023

## Second Semester

## 22MCC21 – INTERNET OF THINGS

## Regulation 2022

## Part –A

1. Very Small computer with CPU helps device storage and process of preprocessing before sending it to cloud, local storage of data, data processing and internet connectivity. If we want to send the gathered data to the cloud database, the IoT needs internet connectivity.

2. Security , Data Sensitivity, Scalability, AI, Interoperability

3. Helps the developer to write code faster by providing a clearer picture of how you are implementing the design. An effective way of solving common repetitive problems in various domains. Help in building end-to-end solutions, which can be used to architect the desired system. Consider a design pattern as a template to build a concrete solution for your specific purpose

4.

| Sensor | Actuators |
|---|---|
| It converts physical characteristics into electrical signals. | It converts electrical signals into physical characteristics. |
| It takes input from environment. | It takes input from output conditioning unit of system. |
| It gives output to input conditioning unit of system. | It gives output to environment. |
| Sensor generated electrical signals. | Actuator generates heat or motion. |
| It is placed at input port of the system. | It is placed at output port of the system. |
| It is used to measure the physical quantity. | It is used to measure the continuous and discrete process parameters. |
| It gives information to the system about environment. | It accepts command to perform a function. |
| Example: Photo-voltaic cell which converts light energy into electrical energy. | Example: Stepper motor where electrical energy drives the motor. |

(Any Two points)

**5.**

**Data at Rest**

Data is Stored in app /database on-premises/Cloud Architecture
Antivirus / Firewalls to Safe guard the data using Encryption for S/W and H/W

**Data in use**

Data is used by gateway / application uses for access in use data.
use authentication for device & users for access of data.

**Data in Fight**

Data which is moved from devices to cloud use Cryptography Algorithm
TLS Transport layer Security HTTPS, DNS security, SFTP - Secure file transfer protocol
Combination of private and public infrastructure (prevents breaches)

**6.** A Home automation system can monitor and/or manage home attributes adore lighting, climate, enjoyment systems, and appliances. Functional testing can be carried out by the following ways

- Portable Keypad by pressing buttons to perform functions for home appliances
- Login /Reliability, performance, reliability, maintainability.
- Temperature detection, receive message/Reliability, performance, availability, maintainability.
- Smoke detection, receive message/Reliability, performance, availability, maintainability.
- Gate , receive message/Reliability, performance, availability, maintaibility.
- By enabling security make the sensors to detect intruders.
- Check the alarm should be buzz or have some sound if the any intruder.
- By disabling security makes the sensors not to detect.
  (any four)

**7.** IIOT Examples

- ✓ Smart cities
- ✓ Smart retail
- ✓ Smart home
- ✓ Enterprise and Industrial
- ✓ Social media and human resources

(any four)

- ✓ Autonomous delivery robots
- ✓ Healthcare
- ✓ Robots in manufacturing
- ✓ Self-driving car
- ✓ Retail analytics

**8.** Classification and how it works

The classification algorithms predict the categories present in the dataset
The machine learning program must draw a conclusion from observed values and determine to what category new observations belong.
(1 mark)
To identify the category of a given dataset and these algorithms are mainly used to predict the output for the categorical data.
(1 mark)

**9.** People effective Collaboration, Process Optimization, Asset Management and Maintenance, Secure Operation, Network Reliability, Asset safety and security, People safety and security and Business Continuity

(any four)

**10.** Latency – average amount of time a message takes to transfer from source to destination

Jitter – amt of variance in the latency

Packet Loss – no of consecutive packet intervals lost before applications generates errors or fails into a safe state

## Part – B

**11) a) i)Two Use-cases of IoT across Industries** (10 marks)

Industrial IoT (IIoT) brings machines, cloud computing, analytics, and people together to improve the performance and productivity of industrial processes.
With IIoT, industrial companies can digitize processes, transform business models, and improve performance and productivity, while decreasing waste.

- ❖ Automated and remote equipment management and monitoring.
- ❖ Predictive maintenance.
- ❖ Faster implementation of improvements. (any two)
- ❖ Pinpoint inventories. (2*4=8 marks)
- ❖ Quality control. (listing 2 marks)
- ❖ Supply chain optimization.
- ❖ Plant safety improvement.

**11) a) ii) IoT Implementation Challenges: Security** (6 marks)

- **Lack of visibility**
  Users often deploy IoT devices without the knowledge of IT departments, which makes it impossible to have an accurate inventory of what needs to be protected and monitored.
- **Limited security integration**
  Because of the variety and scale of IoT devices, integrating them into security systems ranges from challenging to impossible.
- **Open-source code vulnerabilities**
  Firmware developed for IoT devices often includes open-source software, which is prone to bugs and vulnerabilities.
- **Overwhelming data volume**
  The amount of data generated by IoT devices make data oversight, management, and protection difficult. (any three 3*2=6 marks)
- **Poor testing**
  Because most IoT developers do not prioritize security, they fail to perform effective vulnerability testing to identify weaknesses in IoT systems.

- **Vulnerable APIs**
  APIs are often used as entry points to command-and-control centers from which attacks are launched, such as SQL injection, distributed denial of service (DDoS), man-in-the-middle (MITM), and breaching networks
- **Weak passwords**
  IoT devices are commonly shipped with default passwords that many users fail to change, giving cyber criminals easy access. In other cases, users create weak passwords that can be guessed.

**IoT Implementation Challenges: Regulatory and Legal Issues**

The Internet of Things (IOT) raises legal and regulatory challenges, mainly in the area of privacy and security.

- Who owns the data
- anytime you connect something to the Internet, you open it up to an attack
- Are there privacy policies for IOT? What privacy protections exist? What can the devices learn about you that you want to keep private?

**Big market players** in IOT will include:

- Self-driving cars (reduce accidents)
- Smart meters on household devices
- Surveillance
- Stores
- Home health care and hospital care

**IoT Implementation Challenges: Network Latency**

- **Latency** is affected by several factors: distance, propagation delay, internet connection type, website content, Wi-Fi, and your router.
- The longer the device is asleep, the less power it consumes. This also means that there are fewer opportunities for information to be exchanged. This impacts the performance of the device, causing it to run slower (known as latency)
- The amount of time between when data is sent from a connected device to when it returns to the same device – which in turn limits IoT solutions' effectiveness

**IoT Implementation Challenges: Unavailability of standardized platform and common Architecture**

- One of the many significant issues is the multitude of languages, protocols and standards, as well as the lack of agreement on which it works best for individual layers of the IoT.
- It does not have a single platform of standardization; it is changed due to the heterogeneity of connected things.

**IoT Implementation Challenges: Scalability**

- The capability of a system to manage an increasing quantity of work by adding extra resources
- if not handled early enough, such vulnerabilities might evolve into problems that risk higher maintenance hours and latency issues.

**IoT Implementation Challenges: Sensors**

- Related to the reduction of their cost, size, and energy consumption.
- Moreover, additional efforts in design and development of nanoscale sensing materials have to be made to achieve improved device performance.

**IoT Implementation Challenges: Power supply**

- IoT devices are often powered by a battery because they do not have direct access to a power supply.
- This is often caused by being located in places where access to the electric network is simply not possible.

**11) b) i) IoT Ecosystem** (10 marks)

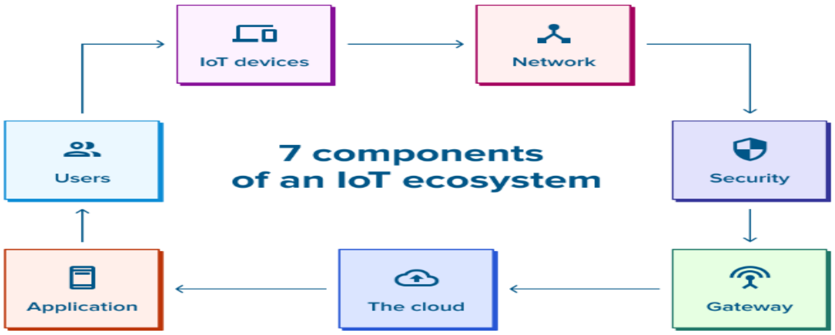


diagram (4 marks)

**Device & Sensors** **any two points** (1 mark)

The smarter devices send and receive data from the devices themselves in the environment that are integrated over network and Cloud Computing.

The layer of sensors, actuators, and smart objects that gather information about the environment and measure physical parameters.

An actuator is **a machine component or system that moves or controls the mechanism or the system**.

To get information from the environment and transform it into data.

Different types of applications require different types of sensors to collect data from the environment.
sensors and actuators are at the centre of the entire IoT network.
Sensors are connected to assets in the form of a physical micro appliance, embedded into an IoT device.
Sensors or device remain connected via wireless networks such as bluetooth, Z-wave, and WiFi
Temperature sensor, Proximity sensors, Water quality Sensor, Chemical Sensors, Humidity, Motion sensors, Pressure, Smoke, Image, Accelerometers, IR

**Gateway** **any two points** (1 mark)

- Acts as a medium to open up connection between cloud and controller(sensors / devices) in Internet of Things (IoT).
- An IoT gateway is an intelligent central hub for IoT devices.
- By the help of gateways it is possible to establish device to device or device to cloud communication.
- A gateway can be a typical hardware device or software program.
- Performs protocol translation, aggregating all data, local processing and filtering of data before sending it to cloud, locally storing data and autonomously controlling devices based on some inputted data, providing additional device security.

- Connectivity types include LPWAN, Wi-Fi, Bluetooth, and Zigbee, among many others.
- Gateways can communicate with sensors/devices over varying connectivity types
- Translate that data into a standard protocol such as MQTT to be sent to the cloud
- Designed to simplify and streamline IoT device communications and management.
-

**IoT Ecosystem : Data capture done through IoT gateway** **(any two points** (1 mark))

❖ The first requirement of an IoT Gateway is to discover and connect devices and collect data from those devices.

❖ Data provided by devices are generally continuous and has a tendency to occupy large communication bandwidth.
Gateway provides bandwidth flexibility and data management that is necessary for evaluation of system performance and device control & management.

❖ Standards and protocols establish a bidirectional connection between devices and IoT gateway. Gateway provides an end to end communication between edge and cloud.

❖ Gateway analyses data according to set parameters and accordingly conveys the message to the messaging interface for further control actions.

**Cloud** **any two points** (1 mark)

- One component that improves the success of the Internet of Things is Cloud Computing.
- Activities like storage and data processing take place in the cloud rather than on the device itself,
- Cloud computing enables users to perform computing tasks using services provided over the Internet.
- Sensor data can be uploaded and saved using cloud computing for later use as intelligent monitoring and activation using other devices.
- Using the cloud also allows for high scalability.
- When you have hundreds, thousands, or even millions of sensors, putting large amounts of computational power on each sensor would be extremely expensive and energy-intensive.
- Data can be passed to the cloud from all these sensors and processed there in aggregate.

**Analytics** **any two points** (1 mark)

- IoT Analytics is used to make sense of the vast amounts of analog data.
- Analytics requires storage power and intelligent computation to be able to make sense of any data
- Software systems that analyze the data generated by IoT devices.
- IoT analytics assesses vast quantities of data and produces useful information from it.
- Analysis can be used for a variety of use-cases, most common would be predictive maintenance.
- Enables organisations to generate real-time insights that benefit them in the present, but also helps them to foresee future business trends in advance.
- Predictive analytics(future), real-time analytics and descriptive analytics(Past data)

**User interface** **any two points** (1 mark)

- The user interface is the visible component that is easily accessible and in control of the IoT user.
- This is where a user can control the system and set their preferences.
- A user may interact with the system via the device itself, or this interaction can be conducted remotely via smartphones, tablets, and laptops.
- Smart home systems such as Amazon Alexa or Google Home etc. also allow users to communicate with their “things”.

**11 ) b) ii) Ciso IoT and Azure IoT** (6 marks)

**Cisco IoT** **any three points** (3marks)

Helps enterprises connect and monitor devices, secure and automate operations, and compute and manage data.

Provides methods for management and storage of data centers and cloud platform

Components - Virtualized data center, Intelligent network and Connected devices

Services

Network Connectivity - built routing, switching, and wireless products, Fog Computing - distributed computing, Security - cyber and physical security , Data Analytics, Management & Automation and Application Enablement Platform - Offers a set of APIs

LoRaWAN

Low-power, wide area networking protocol built on top of the LoRa radio modulation technique.

It wirelessly connects devices to the internet and manages communication between end-node devices and network gateways.

Cat-M1

LTE Cat-M, is a low-cost LPWAN technology developed by 3GPP as part of the 13th edition of LTE standard.

NarrowBand-Internet of Things (NB-IoT)

Standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services.

**Advanced Metering Infrastructure (AMI)**

Utilities to achieve business goals by saving truck rolls, enabling demand response, fast outage notification, and preventing power theft.

Cisco's AMI Validated Design is based on Wi-Sun mesh which provides standard based scalable, resilient, OpEx effective, and secure smart meter networking.

**Cisco Network Services Orchestrator**

NSO provides a robust bridge linking network automation and orchestration tools with the underlying physical and virtual infrastructure.

orchestration platform for hybrid networks. It provides comprehensive lifecycle service automation to enable you to design and deliver high-quality services faster and more easily

**PDI**

Planning and design and implementation

Build the network hierarchy and image repository, and configure network settings.

Streamline IT operations with custom network and IT service management (ITSM) solution integration.

**Azure IoT** **any three points** (3 marks)

A managed service hosted in the cloud that acts as a central message hub for communication between an IoT application and its attached devices.

The users can connect millions of devices and their backend solutions reliably and securely.

It also includes security and operating systems for devices and equipment, along with data and analytics that help businesses to build, deploy and manage IoT applications.

- Connect, monitor and manage billions of IoT assets
- Authenticate every device for enhanced security
- Automate device provisioning to accelerate IoT deployment
- Extend the power of the cloud to your edge devices
- Security-enhanced communication channel for sending and receiving data from IoT devices

Table (or)

| | **Ciso** | **Azure** | |
|---|---|---|---|
| **Communications Protocols** | MQTT | MQTT,HTTP,<br>AMQP Over Socket | |
| **Main Functions** | **Cisco IoT Control Center**<br>Mobile Connectivity<br>Machine Learning for data analysis<br>improve security | **Azure IoT Hub**<br>Connectivity<br>Authentication<br>Device Monitoring<br>Device Management<br>IoT Edge | **(2 marks)** |
| **2Edge Computing** | Cisco iOX<br>Edge Computing Platform<br>Cisco Edge Intelligence | IoT Edge as an Integral part of Hub | (2 marks) |
| **Use Cases** | Connected Vehicles<br>Manufacturing<br>Smart City | Healthcare, Retail and Manufacturing | (2 marks) |

**12) a) Design Patterns for Node Connections, Deployment Strategies and Infrastructures - (16 marks)**

***Node Connections*** ***( 5 marks)***

**1. Design Patterns for Node Connections: Connected Sensor**

**Problem** **listing (1 mark) any two 2*2 =( 4 marks)**

Even a not in use sensor node stays active which consumes power and bandwidth.

It's a huge problem in a large and complex IoT deployment, as the scalability suffers a lot due to the loss of valuable resources like power and bandwidth.

**Solution**

Make these nodes connected with the host and stay in sleep mode.
These nodes can send its state to the host as and when they feel like doing so.
On the other hand, if needed, the host can ping the node and make it change its state from sleep to active.
This pattern greatly improves the resource consumption and improves the possibility of scalability

2. **Design Patterns for Node Connections: Remote Read**

**Problem**

Many times host needs to just check the state of a node

host needs to get data from it without affecting the node's current task.

For example, in a hospital environment, a node may be collecting data about patient's vitals like blood pressure, and temperature,

Host may need to access the previous data or just check the state while the node is busy in performing the task.

**Solution**

Allow the host to connect with the required node and

permit it to read its data remotely without affecting its state or current task in hand.

This pattern is useful as it silently allows the host to perform its operation without affecting the nodes

3. **Design Patterns for Node Connections: Remote Control (5 marks)**

**Problem**

Sometimes it is essential to interact with the nodes in a physical capacity to perform service related tasks.

In many cases, these tasks are programmatic tasks rather than physical movement or placement of nodes.

For all these cases, it brings a lot of overhead cost in terms of money, resources, and time by having a service engineer visit the nodes personally.

Also, it is a time-consuming process, which may bring a panic situation in highly critical areas like hospitals, and airports.

**Solution**

Assign the host proper administrator rights on the nodes allow this host to send commands to control and configure the connected network nodes remotely.

This way, the host can connect to these nodes anytime and perform the necessary service tasks.

Host can also perform various critical tasks on the nodes like configure, reconfigure, install updates, read data, change state, etc.

However, in order to achieve reliability in a critical environment,

these nodes must stay in awake or waiting state.

This adds a little overhead, as the resource consumption will be a little higher.

***Design Patterns for Deployment Strategies*** ***(5 marks)***

1. **Design Patterns for Deployment Strategies : Single Environment** **( listing (1 mark))**

All IoT deployment requirements are not the same. **any two 2*2 =( 4 marks)**
They differ by many variables and there is no single best solution available.

**Problem**

For small IoT projects, it is important to have less complexity in the deployed environment so speed, security and reliability won't get affected.

Sometimes, speed and reliability are more important than scalability as the scope of the project is very limited to one particular area.

In this case complex deployment will not work

**Solution**

For such problems, single environment deployment pattern is more useful as all the nodes are located in close proximity of each other.

This ensures the speed of communication and reliability as single and data loss possibility is reduced down to none.

Single environment also brings a lot of benefits as the tasks such as installation, configuration, and addition of a new node are very easy to manage with fewer resources in hand

2. **Design Patterns for Deployment Strategies Heterogeneous**

**Problem**

For larger IoT deployment, single environment deployment does not work as it brings a lot of problems like limited computing resources,

inadequate networking capability,

and shortage of storage.

Also, these types of IoT deployments have limited geographical reach and availability.

**Solution**

Using multiple distinct infrastructure environments or regions called Heterogeneous deployments can easily solve this problem.

Heterogeneous deployments are also known as "hybrid", "multi-cloud", or "public-private".

These environments span regions in the local and public cloud, or various public clouds or a single cloud

3. **Design Patterns for Deployment Strategies Distributed System**

**Problem**

For some organizations such as banks and government secret agencies, even for a large scale IoT deployment,

it is important to keep data in a private environment with full control on storage and management of the physical servers.

For such purposes, neither single nor Heterogeneous Deployment is suitable

**Solution**

Using a distributed model where computing operations are spread across different environments can solve this problem.

This gives benefits of heterogeneous deployment such as scalability, more computing resources, on-demand resource enhancement, and more bandwidth.

Also, benefits of single environment deployment such as resource control, on-demand accessibility, and closed environment setup

Provides solutions for connectivity for low power devices with wireless sensor networks

use less electric power than usual

***Design Patterns for Infrastructure***

**Design Patterns for Infrastructure : WSN Access Point**
**Problem** **listing (1 mark) any two 2*2 =( 4 marks)**

In order for IoT devices to communicate with each other, they need to connect with each other via a network.
This network requires access points through which these devices can connect.
*An access point is a device that creates a wireless local area network*

**Solution**

WSN stands for Wireless Sensor Network that allows various low power sensor nodes to connect with each other.
These sensors measure environmental conditions such as temperature, sound, pollution levels, humidity, and wind.
These WSN provide access points for these sensor nodes to share data with each other.

1. **Design Patterns for Infrastructure : 6LoWPAN Edge Router**

**Problem**

Many IoT deployments contain low power devices which are needed to communicate with wireless infrastructure.
This is problematic due to the power needed for devices to route IPV6 packets.
Primarily divided on the basis of routing decision taken on adaptation or network layer

**Solution**

Low power devices need a different solution to communicate with each other.
6LoWPAN stands for IPv6 over Low-Power Wireless Personal Area Networks.
It routes IPv6 packages to lower power networks by compressing a header
A Mesh IoT network is a local network topology where devices are connected directly in a non-hierarchical way to route data across the network.

The devices in a mesh network communicate according to a predefined protocol that allows each device to participate in the data transmission on the network

2. **Design Patterns for Infrastructure : Mesh Routing**

**Problem**

Reliable communication among nodes and with the access point is essential for a successful IoT deployment.

If structured in a serial manner, upon failure of one of the nodes, the entire communication may fail.

Also, in another case, if structured in some other manner which requires a particular node to connect with a particular node

Then again failing on the dependent node may cause in reliable communication.

**Solution**

This problem can be solved by creating a mesh structure so nodes are not dependent on a particular node in the chain.

Mesh structure provides connectivity in a direct, dynamic and non-hierarchical manner.
This type of structure offers reliability in data sharing as even if one particular node fails, the communication can get diverted to other node in the mesh.
This removes the dependency on one particular node and allows every node to participate in relaying information.
As you can see this type of network is self-organized and self-configured, which greatly reduces the maintenance and management tasks.

3. **Design Patterns for Infrastructure: Behind NAT Connectivity**

**Problem**

Every sensor node will require having a public IP address in order to get connected to the inter-net.
However, having this will increase the cost significantly as well as create a lot of security risk by exposing these devices to the public network.
In order to secure this device, we must monitor and control traffic which is a daunting task.

**Solution**

We can avoid having a public IP address for every sensor.
All these sensors can work behind a network

4. **Design Patterns for Infrastructure : Application Gateway**

**Problem**

Security is an important aspect when setting up the wireless sensor network.

Any third party can target this network to get access to the nodes and control them.

There is a need to make sure the nodes are communicating in a safe manner

**Solution**

A firewall proxy can provide the desired security, which can filter network application data.

These network applications can be Telnet, FTP (File Transfer Protocol), RTSP (Real Time Streaming Protocol), and BitTorrent.

This firewall proxy is known as Application Gateway, which provides this required security at the highest level.

This security can be achieved by diverting the traffic like a web page request or a file request through a proxy server that can be diverted further to the main server.

This proxy server has a public IP address which hides the details of the main server as the outside world does not have access to it.

The only access is established by a proxy server

5. **Design Patterns for Infrastructure : M2M WAN**

**Problem**

In IoT world, sensors must communicate with each other to perform required tasks.

This must happen without any human intervention.

There should be a mechanism to make these devices communicate

**Solution**

Wireless communication has opened up a door of possibilities for these sensors to communicate with each other.

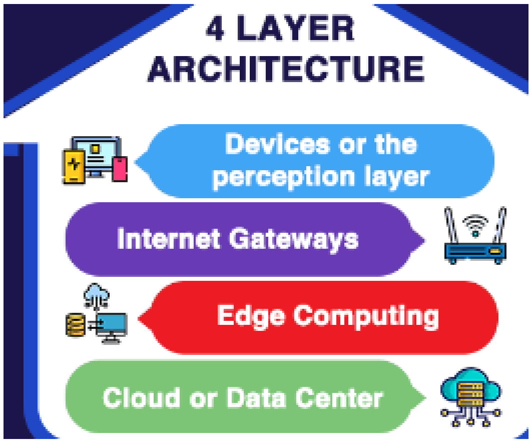
This node-to-node communication is achievable by M2M WAN (Machine-to-machine Wireless Access Network)

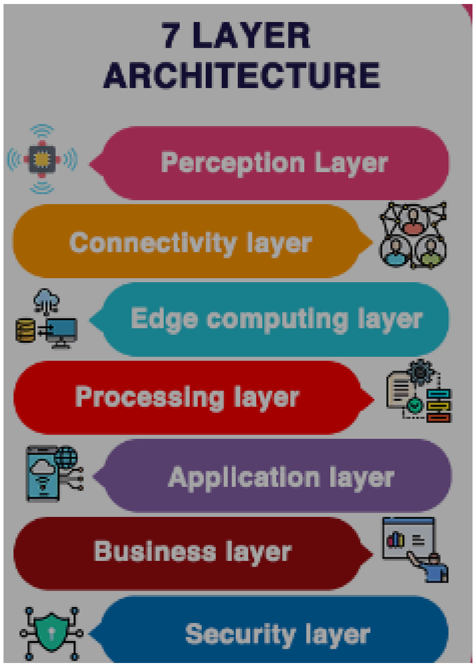
to exchange data and communicate without human intervention.

Some examples of this type of communication are sending an alert to all the doctors in case a patient’s vitals are falling down to some threshold

**12) b) Four Layers with Seven Layers Architecture and Various component of seven layer architecture**

**Compare (4 marks)**





**Four Layer Architecture (4 marks)**

***First Layer : Sensors & Actuators*** (1 mark)

Sensors, actuators, devices are present in this Sensing layer.

These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.

Actuators

components of IoT devices which can modify an object’s physical state.

For example, they can switch off the light and adjust the temperature in a room.

***Second Layer : Internet Gateway*** (1 mark)

Internet/Network gateways, Data Acquisition System (DAS) are present in this layer.

- DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc).
- Advanced gateways which mainly opens up connection between Sensor networks
- Internet also performs many basic gateway functionalities like malware protection.
- Filtering also some times decision making based on inputted data and data management services, etc.

***Third Layer : Edge IoT (1 mark)***

Data processing Layer

This is processing unit of IoT ecosystem.

Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored and managed

further actions are also prepared. So here Edge IT or edge analytics comes into picture.

edge IT systems perform enhanced analytics and pre-processing here.

For example, it refers to machine learning and visualization technologies.

At the same time, some additional processing may happen here, prior to the stage of entering the data center.

***Fourth Layer : The Data Center and the Cloud (1 mark)***

Application Layer

This is last layer of 4 stages of IoT architecture.

Data centers or cloud is management stage of data where data is managed

Used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

***Seven Layer Architecture (6 marks)***

**1. Physical Devices (1 mark)**

Physical equipment like controllers falls into the first layer of the seven layer architecture.

The “things” in “internet of things” is referred to these physical devices as they are responsible for sending and receiving data.

For example, the sensor data or the device status description is associated with this type of data.

A local controller can compute this data and use NFC for transmission.

**2. Connectivity (1 mark)**

The relay of data which is communicated between devices via multiple different networks.

- It is used to set up a connection with the first layer devices
- It is used for trustable delivery throughout the network.
- It is used to implement different device compatible protocols.
- It is used for routing and switching.
- It is used to translate for protocols.
- It serves as an added protection measure for the network.
- It is used for networking analytics.

**3. Edge Computing (1 mark)**

The edge computing layer is responsible for data formatting

- It can filter data
- It can clean up data.
- It can aggregate data
- It can provide evaluation for validation so data can be processed by the fourth layer.
- It is used to reformat data so it can help in more complex and higher-level computations.
- It is used for expanding and decoding.
- It is used to compress data so its impact on data and traffic is reduced for the network.
- It is used to generate events for any alerts

**4. Data Accumulation (1 mark)**

- The data from the sensor is constantly changing.
- Therefore, the fourth layer is tasked to convert it.
- This layer maintains the data in a format that is extremely accessible.
- After data is filtered through this layer, a lot of data is decreased
- The layer ensures that data is maintained in such a state that other components and module of IoT can easily access it.

**5. Data Abstraction (1 mark)**

- The relevant data is processed for holding to specific properties related to the stored data. Afterward, data is provided to the application layer for further processing.
- The primary purpose of the data abstraction layer is data rendering keeping in mind its storage and using an approach through which IoT developers are easily able to code applications.

**6. Application (1 mark)**

- responsible to process data in order to ensure that it is accessible for everyone.
- all the IoT modules can access data.
- It is associated with both the physical and software layer.
- It is used for data interpretation to create reports.
- Business intelligence tools are also used in this layer

**7. Collaboration and Processes (1 mark)**

- Response or actions are offered to provide assistance for the given data.
- For instance, an action may be the actuator of an electromechanical device following a controller’s trigger.

***13) a) Various Challenges in IoT Implementation and Technology and communication infrastructure (listing 2 marks)***

Cost, security, Infrastructure for Technology, Infrastructure for Communication, IoT Standards and Procurement

**1. COST ( 1 mark)**

Migration from one end to other end to handle cost - bite speed (reasonably affordable with fixed milestone Instantly S/W On -Premise Documentation of business Cases)

**2. SECURITY ( 1 mark)**

Uploading /Moving data on Internet

**Data at Rest**

Data is Stored in app /database on-premises/Cloud Architecture

Antivirus / Firewalls to Safe guard the data using Encryption for S/W and H/W

**Data in use**

Data is used by gateway / application uses for access in use data.

use authentication for device & users for access of data.

**Data in Fight**

Data which is moved from devices to cloud use Cryptography Algorithm

TLS Transport layer Security HTTPS, DNS security, SFTP - Secure file transfer protocol

combination of private and public infrastructure (prevents breaches)

**Validation of data access**

APM - Asset performance management

SCADA ( Supervisory control and data acquisition)

EAM - Enterprise asset management

**3 Infrastructure For Technology (5 marks)**

No power monitoring equipment is used

Network of SCADA - offer - required infrastructure to establish a connection

SCADA - Manage control signals for equipment

Data transmission for APM

There are two strategies

1. Establish connection with SCADA historical and APM

Historian (used to store database record of all control actions for equipments

2. Use of an Independent Infrastructure of cellular service connect 5 device - one cellular gateway device

**4. Infrastructure For Communication ( 5 marks)**

Use of cellular gateway - for establishing connection with IoT instruments

LTE - NB cellular towers

LTE - M cellular towers

4G - LTE data hoot signal for voice calling

**5. IoT Standards** (1 mark)

Open Interconnect consortium, Open Connectivity foundation and IEEE - IoT Architecture Standard

**6. Procurement ( 1 mark)**

Procurement of Services and device , Communications N/W, Instrumentation

Data management consultants. Storage , Stakeholders

**13) b) Types of Testing for IoT (listing 2 marks)**

***Usability Testing***

Focused on the end-user, on how easily user was able to use the interface if the design of the interface was friendly enough.

3 Aspects

1.What is the purpose of an IoT Device?

2.Who is going to use the IoT Device?

3.How is the IoT Device going to used?

**Target Audience of the IoT device (explain any 2 testing 2*5=10 marks)**

Customer Requirements - users Expectations

Gain Productivity in their lives

**1. The user**

End User - another aspects

1. Standard Average User
2. Individual - Enthusiastic to test the device
3. Students from college ,schools ,universities
4. Government department
5. Workers with commercial ,retail, Industries Sectors
6. Patients - Medical IoT - MIot

**2) User Behavior**

1.What are features which are over invoked by the consumer?

2.Which features interest them?

3.How is the IoT device being used?

**Unexpected stumbling blocks**

An obstacle to progress - **stumbling blocks**

1.how may user experiencing unique Issues which are not being experience by other?

2.What is the reasons behind their issues ?

3.Issues related to size the device ,orientation & finger size

**3) Selection of Testers**

1.Who are responsible for the IoT Device testing?

2.Age and generation of user.

3. valuable feedback

***Functional Testing***

Type of testing in which all the functions of the IoT infrastructure are working according to the requirements.

Testing of IoT is very similar to testing other software products.

**Unit testing**

It tests each module or component of an application. The IoT development team usually performs this task.

**Integration testing**

When all modules are integrated, it is essential to see how they work together.

**End-to-end testing**

This type involves running tests for the entire software product.

**Smoke testing**

This type of testing helps determine if the software is stable enough.

**Regression testing**

Each added module leads to changes in the program.

- If it takes any updates to the firmware of the IoT device, they can also lead to changes in the system.
- It is crucial to ensure that all components are still working correctly after each update.

**Interface testing**

Testers verify the GUI meets the specified requirements and specifications.

***Scalability Testing***

To asses the capability of a process, system, network in the IoT device infrastructure while modify the volume or the size of its data.

To manage the user traffic, frequency of transactions counts and data volume.

To test the DB, system and the process of IoT Infrastructure.

1. Scalability after the added load.
2. Evaluate the end user experiences
3. Evaluate the degradation and robustness at the server side
4. Evaluates the limit for consumers of an IoT Applications

**Metrics**

1. Screen transition - Time (Session time, reboot time, printing time, transaction time, task execution time)
2. Time taken for task execution
3. Throughput
4. Hits per second, transaction per seconds and request per seconds
5. Memory,CPU, and network usage
6. Performance of multiple users
7. Heavy workload
8. Webserver handling of response and request per seconds

***Compatibility Testing***

An assessment used to ensure a software application is properly working across different browsers, databases, operating systems (OS), mobile devices, networks and hardware.

IoT and Firmware running with various Appli, OS,Systems,H/W, IoT devices and network environments

Non-functional Testing

**1.S/W -** Asses the designed S/W and ensure it works well with other S/W

**2.Os**- S/W works with OS

**3.H/W**- Asses the compatibility of S/W with various Config of H/W

**4.N/W-** System performance with N/W like capacity, Os, and bandwidth

**5.Browers**- Website compatibility like browers like Chrome,Firefox,IE Etc

**6.Devices**- S/w compatibility test for Diff Iot Devices

**7.Mobile**- Compatibility of mobile platforms like android, IoS

**8.Software Versions-** assess the compatibility of various versions and IoT Software Applications

***Performance Testing***

A non-functional software testing technique

Determines how the stability, speed, scalability, and responsiveness of an Appl holds up under a given workload.

Test the infrastructure perform correctly within the estimated workload

To measure system behavior and performance under load

**3 Aspects of IOT Software**

1.What is the speed of the IoT Appl

how fast it create a response

2. What is the extreme workload – Iot software can manage

3. How stable is the IoT Appl works when constantly changing user loads?

**Types**

1. **Stress Testing**

Find out the application breaking point

Maximum workloads in data processing And high traffic

2. **Load Testing**

Examines how the system behaves during normal and high loads and determines if a system, piece of software, or computing device can handle high loads given a high demand of end-users.

3. **Spike Testing**

Application receives a sudden and extreme increase or decrease in load. The goal of spike testing is to determine the behavior of a software application when it receives extreme variations in traffic.

4. **Endurance Testing**

Performed to check the performance of the system under constant use. In terms of detecting the issues such as memory leaks, the execution of endurance testing is essential. These issues can be the reason for system failure, causing the loss of crucial data.

5. ***Volume Testing***

It helps us to check the behavior of an application by inserting a massive volume of the load in terms of data concentrate on the number of data rates than the number of users - **Flood testing.**

**Comparison chart (4 marks)**

| | |
|---|---|
| Usability Testing | Examining how easily and effectively an IoT device can be used by different end users |
| Functional Testing | Testing of the scenarios, such as user actions on the applications, data and events |
| Scalability Testing | Load testing that measures the application's ability to scale up or down as a reaction to an increase in the number of users |
| Compatibility Testing | To ensure that an IoT device app is compatible with various devices, apps, and operating systems |
| Performance Testing | To simulate devices from different locations (to simulate latency) with required network technologies like 2G, 3G, 4G, Bluetooth, etc |

**14) a) i) Industry 4.0 and its benefits of AI with IoT (10 marks)**

***Industry 4.0 (2 marks)***

Manufacturers are integrating new technologies, including

Internet of Things (IoT), cloud computing and analytics, and AI and machine learning into their production facilities and throughout their operations.

smart factories are equipped with advanced sensors, embedded software and robotics that collect and analyze data and allow for better decision making

***Benefits of AI For IoT*** ***( listing 2 marks)***

**1.Reduction in Downtime** **(*2 marks)***

**Downtime-** to the period of time in which a company's factory is not producing product.

- Increase productivity, lower costs decrease accidents.
- Production - series of processes explain any 3 (3****2=6 marks)***
- One process is dependent on another process.

**Snowball effect**

If one process is down /delay serving other dependent processes so in a waiting stage.

- Factory- is not producing anything until that single process is fixed.
- Effect the markets where products are out of stock due to the failure
- Find ways to reduce this downtime.

**AI Works For**

- Trigger can be given by AI Self-diagnostic tests
- Sending emergency alerts to the Technicians
- Reassigning
- Resetting time line for other dependent processes

Alerting the entire supply chain about the process change

**2. Preventative measures to reduce downtime** **(*2 marks)***

With AI assist – prevent downtime

1. ML

Analyzing data generated by these machines and train them

Taking preventing actions given through triggers

2. Identify maintenance requirements

performance maintenance

3. Identify patterns – causes disruption and schedule predictive maintenance

Predictive Maintenance

Minimizing downtime in production

Uses data collected from all machinery

AI solutions analyze incoming data and monitors all machines in manufacturing

Causes of Downtime

- Inefficient processes
- Human error
- Supply chain disruptions
- Inaccurate maintenance

**3. Operational Efficiency** **(*2 marks)***

By reducing downtime and using preventative measures

-achieve operation efficiency

Predictive analysis on supply and demand side.

based on- AI Defect

- Historical data
- Current market conditions
- Political stability
- International market influence
- Catastrophic events occur in other parts of world

Catastrophic events -involving /causing sudden great damage/suffering Unfortunate events.

These predictions used

Schedule a production capacity
Purchase of raw material
Plan workforce
Arrange transport capacity etc.,

**4. Increased Risk Management** **(1 *mark)***

Organization struggling for not able to predict risks in future.

- Understanding of the data in hand
- Ability to decode various internal/external factors – May effect the organization

AI - trigger a rapid response
- prevent the large losses

**5.New product and services** **(*2 marks)***

Use of AI – open up new opportunities to launch new products and services

**14) a) ii) Use of Machine Learning in IOT** **(6 *marks)***

Deliver insights otherwise hidden in data for rapid, automated responses and improved decision making.

used to project future trends, detect anomalies, and augment intelligence by ingesting image, video and audio.

**Why use machine learning for IoT?**

ML can help demystify the hidden patterns in IoT data by analyzing massive volumes of data using sophisticated algorithms.

Supervised, unsupervised and deep learning Alg – process the data and generate conclusions

**With machine learning for IoT**

- Acquire and transform data into a consistent format
- Build a machine learning model **any 6 use (6*1=6 marks)**
- Deploy this machine learning model on cloud, edge and device

Example : using machine learning

- a company can automate quality inspection
- defect tracking on its assembly line
- track activity of assets in the field and
- Forecast consumption & demand patterns.

**14) b) Various Security Attacks and Man-in-the-Middle attack and IP Spoofing (16 *marks)***

***Various types of Attacks (4 marks)***

1. Attacks that target communications between IoT devices and servers to compromise or steal data.
2. Firmware vulnerability exploits that take advantage of weaknesses in an IoT device's operating system, commonly known vulnerabilities, some of which cannot be patched.
3. Credential-based attacks that use IoT devices' default administrator usernames and passwords to gain unauthorized access.
4. Man-in-the-middle (MITM) attacks where the attacker "sits" between two trusted entities (e.g., a sensor and the cloud where data is being sent) and intercepts unencrypted communications.
5. Physical hardware-based attacks that focus on the chip in the IoT system to take over the device to steal data, use it as a launchpad for other attacks, or gain access to the network.
6. **Denial-of-service (DoS) attacks**

   IoT devices have limited processing power, which makes them highly vulnerable to denial-of-service attacks.

   a device's ability to respond to legitimate requests is compromised due to a flood of fake traffic.
7. **Denial-of-sleep (DoSL) attacks**

   Sensors connected to a wireless network should continuously monitor the environment, Sleep and awake modes are controlled according to the communication needs of different protocols, such as medium access control (MAC). Attackers may exploit vulnerabilities of the MAC protocol to carry out a DoSL attack. This type of attack drains battery power and thus disables the sensor.
8. **Device spoofing**

   when a device has improperly implemented digital signatures and encryption.

   For instance, a poor public key infrastructure (PKI) may be exploited by hackers to "spoof" a network device and disrupt IoT deployments.
9. **Physical intrusion** **(any 4 attacks 4*1=4 *marks)***

   **P**hysical intrusion of a device is also possible if it's stolen. Attackers can tamper with device components to make them operate in an unintended way.
10. **Application-based attacks**

    **S**ecurity vulnerabilities in device firmware or software used on embedded systems or weaknesses in cloud servers or backend applications

***Man-in-the-middle-attack (6 marks)***

A man-in-the-middle (MitM) attack is a type of cyberattack in which communications between two parties is intercepted, often to steal login credentials or personal information, spy on victims, sabotage communications, or corrupt data.

Cybercriminal disguises itself as server deceives a client to make establishing a connection

Client initiates the connections sends a request to the real server

Hacker the able to access this response and passes it over to the client

Hackers ensure that client route into their server not with the actual server

Hackers can read and save information

All the HTTP/HTTPS communication and transaction

Modify the message between two users

Modify sensitive real-time data

**Examples**

DNS Traffic Manipulation

Hostname redirection

Operational configuration

Uses scripting features to infect, delete data in a connection

Find Protocol password

Gives fake SSL Certification to the affected users

Vulnerabilities through Bluetooth known as Blueborne

**IP Spoofing (6 marks)**

IP spoofing, or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system.

IP spoofing allows cybercriminals to carry out malicious actions, often without detection. This might include stealing your data, infecting your device with malware, or crashing your server.

Identity spoofing attacks are easy to launch in an IoT access network.

By using a faked identity such as the MAC (media access control) or IP (internet protocol) address of the legitimate user, an identity spoofing attacker can claim to be another legitimate IoT device.

The attacker can then gain illegal access to the IoT network and launch more advanced attacks, such as man-in-the-middle attacks and denial-of service attacks

**Examples**

1. PayPal phishing attacks (multiple incidents) – Over the years, scammers have consistently sent spoofed emails pretending to be PayPal, tricking users into providing their login credentials on fake websites.
2. GPS spoofing incident **-** In this event, the Iranian government allegedly captured an American stealth drone by spoofing its GPS coordinates, tricking it into landing in Iran instead of its home base

3. Operation Aurora (2009) – Chinese hackers used spoofed emails to trick employees of Google and other large corporations into downloading malicious software, leading to a significant data breach.
4. DNS spoofing attack on Brazilian banks (2017) – Cybercriminals rerouted all the online traffic of a major Brazilian bank to perfectly duplicated fake websites, leading to a massive data breach.
5. Voice phishing attack on a UK-based CEO (2019) – Hackers used AI to mimic the voice of a CEO and tricked the firm's employee into transferring $243,000 to a fraudulent account.

**15) a) Industrial Automation and control systems Model (16 marks)**

**Level 0 /process (*2 marks)***

It is the Process or equipment under control

Contains sensors and actuators involved in manufacturing

ex manufacturing robots, spraying ,driving a motor and welding.

**Level 1/Basic Control (*2 marks)***

controller

direct the manufacturing process live

interact with level 0 IOT devices

uses PLC - controller

distributed control systems(DCS)

It includes the Controllers / PLCs that provide basic control, safety and protection functions

**Level 2/ Area Supervisory Control (*1 mark)***

Functions within cell/area Zones

Runtime supervision and operation

include HMIs, alarm and control workstations

It includes supervisory control functions and includes devices such as HMI (Human Machine Interface) Operating workstations, Engineering Workstations, Historians, Application Servers, Engineering Databases, etc

**Level 3 / Site Level (*1 mark)***

Includes file server, control room workstations, scheduling systems and reporting systems

It includes the operations management functions such as domain controller, backup server, antivirus and patch management, etc.

**Level 4 (*1 mark)***

It refers to the Enterprise systems

**Safety Zone** ***(1 mark)***

Hard-wired and air-gapped from IACS N/w

Provide shutdown in case of emergency – equipment if a dangerous event occurs

**Manufacturing** ***(1 mark)***

Composed of several cell/area Zones (levels 0-2) and site level manufacturing (level 3) activities ***(1 mark)***

Application, devices – controlled and monitored

**Cell/area Zone** ***(1 mark)***

Machine area within a plant

Multiple Cell/area Zone within a single plant

**Demilitarized Zone (DMZ)** ***(1 mark)***

Demarcation between the plant operational network and traditional network

Protects the machines at lower level from malicious activity

**Enterprise Zone**

Enterprise networking functions, including like file services, Internet Connectivity and email systems

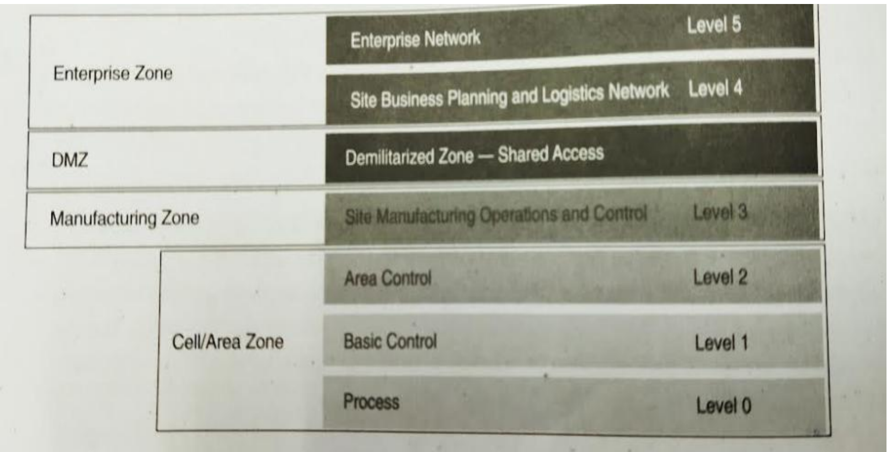


**Figure 9-3** *The ISA99 / IEC-62443 IACS Logical Framework, Based on the Purdue Model for Control Hierarchy*

**Diagram (*4 marks)***

**15)b) Public Safety uses cases and Challenges in implementation**

IoT technology is capable of increasing the efficacy of any public safety system, thanks to connecting smart devices, collecting, processing, and displaying data received from them. The received real-time data can be used for making timely decisions and reacting to any possible threat effectively ***(1 mark)***

***IoT public safety use cases (any 2 ) 2*4=8 marks)***

1. **Smart buildings**
   "Smart building" systems carry out functions such as tracking entries, recording videos that can help authorities investigate cases, as well as monitoring the building's interior environment. When an emergency is detected, such systems can send alerts to authorized employees and public safety officials.
2. **Smart traffic signals**
   These IoT devices are an important part of smart cities, aimed at enhancing urban mobility and optimizing traffic flow. These traffic signals are enriched with special sensors that allow them to monitor and analyze ongoing traffic conditions. Based on this IoT data, they can change the timing of lights to ease traffic flow. When a car accident or other emergency is detected, smart traffic signals can find an appropriate solution for regulating traffic under unusual conditions.
3. **Smart streetlights**
   These objects of urban infrastructure can include a microphone, IoT sensors, and cameras to gather information about possible accidents, criminal behavior, and general traffic. When a deviation from the norm is detected, smart streetlights can send alerts and call for help.
4. **Smart emergency vehicles**
   These vehicles, used in a similar way to smart streetlights, can capture video and audio that is forwarded to a relevant authority for use in addressing emergencies as well as to inform traffic planning and training.
5. **Smart intersections**
   These IoT public safety solutions are designed with a view to analyzing traffic patterns and defining possible risks and threats. Data can be processed with the help of artificial intelligence in an effort to reduce the number of accidents, injuries, and crashes.
6. **Environmental safety**
   IoT devices included in modern smart city systems can be used for tracking factors such as noise, air temperature, humidity, gas composition, object velocity, etc. All this data can be of great importance in analyzing the overall wellbeing of people living in a monitored area. For example, such systems can automatically send alerts when the risk of forest fire is detected.

***Challenges in implementation of Public Safety (6 marks) listing 2 marks***

1. ***Lack of unified standards***
   Developers around the world are working on enhancing IoT technologies and looking for new ways to apply IoT tools in everyday life. Nevertheless, it is difficult to create a single standard and use it all over the world.
2. ***Lack of regulation*** ***explain any 2 (2*2=4 marks)***
   IoT is considered a rather new sector, so there are still no well-developed rules and legislation.
3. ***Privacy issues***
   Though IoT systems gather data to improve public safety, they inevitably also collect a lot of private information, and the ethical questions this raises can't be ignored. Moreover, IoT networks can be quite vulnerable to breaches and hacker attacks, which may lead to sensitive data loss.