-----------------IOT IA test 2 HW QUESTIONS---------------------

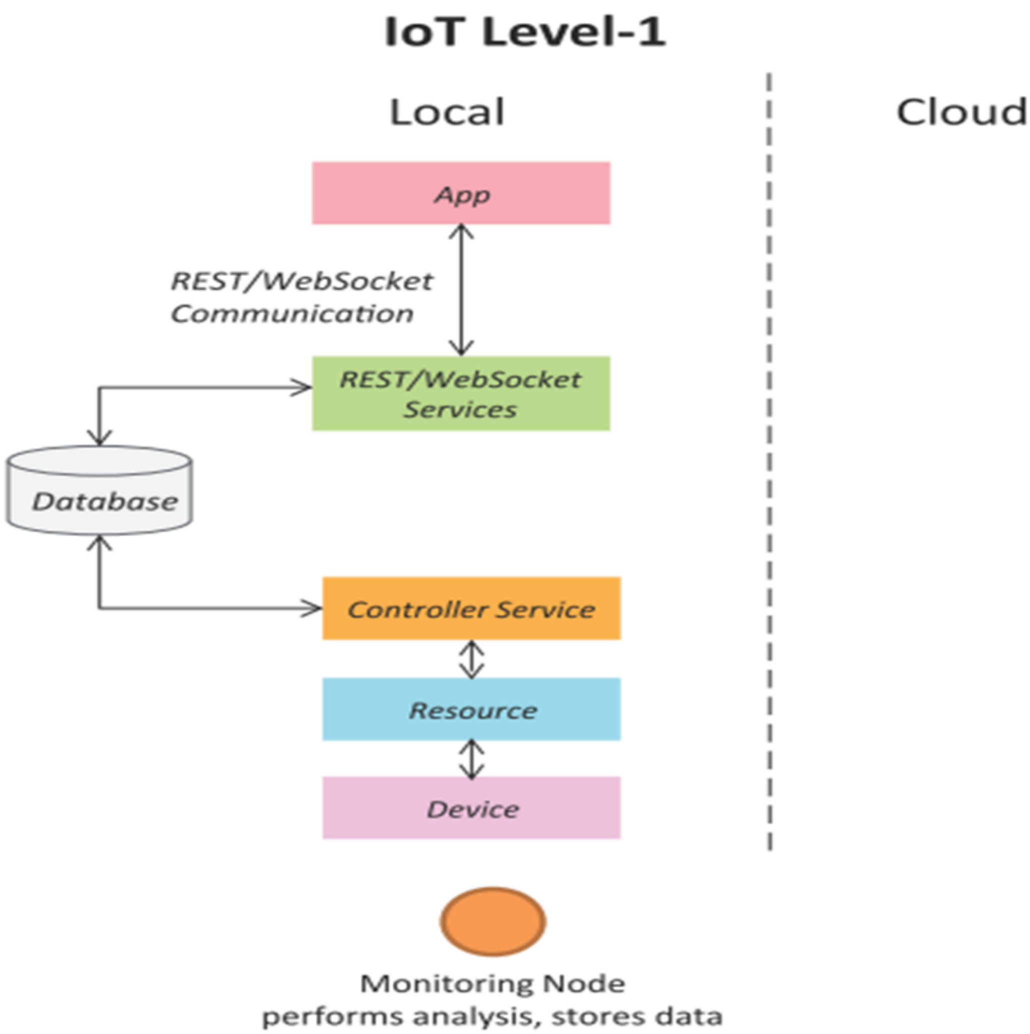
Q1 &2: EXPLAIN IOT LEVELS AND DEPLOYMENT TEMPLATES 1,2,3,4,5,6.

ANS : LEVEL-1

*A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application.

*Level-1 IoT systems are suitable for modelling low-cost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.

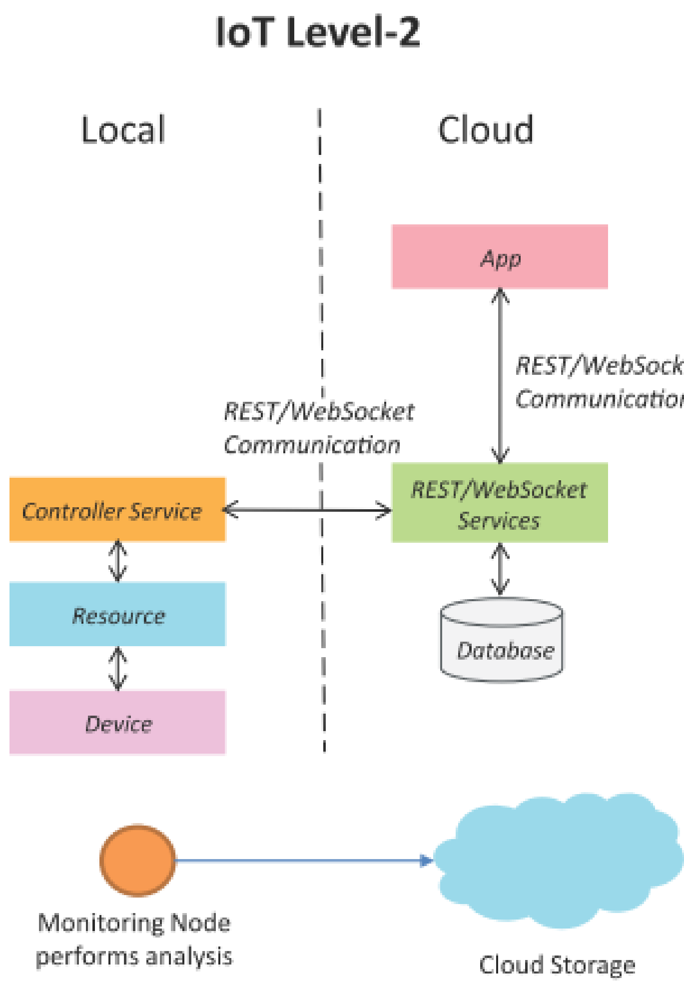
EXAMPLE: Home automation system.



LEVEL -2

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

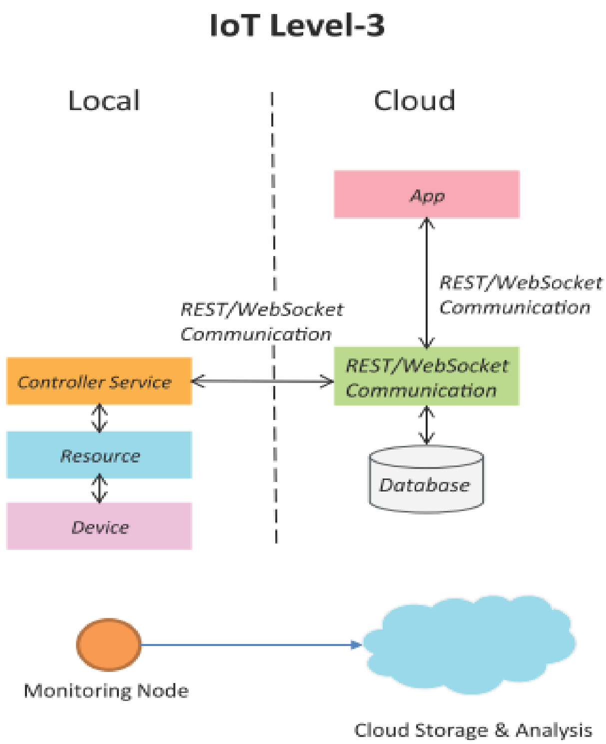
  Example: smart irrigation system



LEVEL 3

- A level-3 IoT system has a single node. Data is stored and analyzed in the cloud and the application is cloud-based.
- Level-3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.

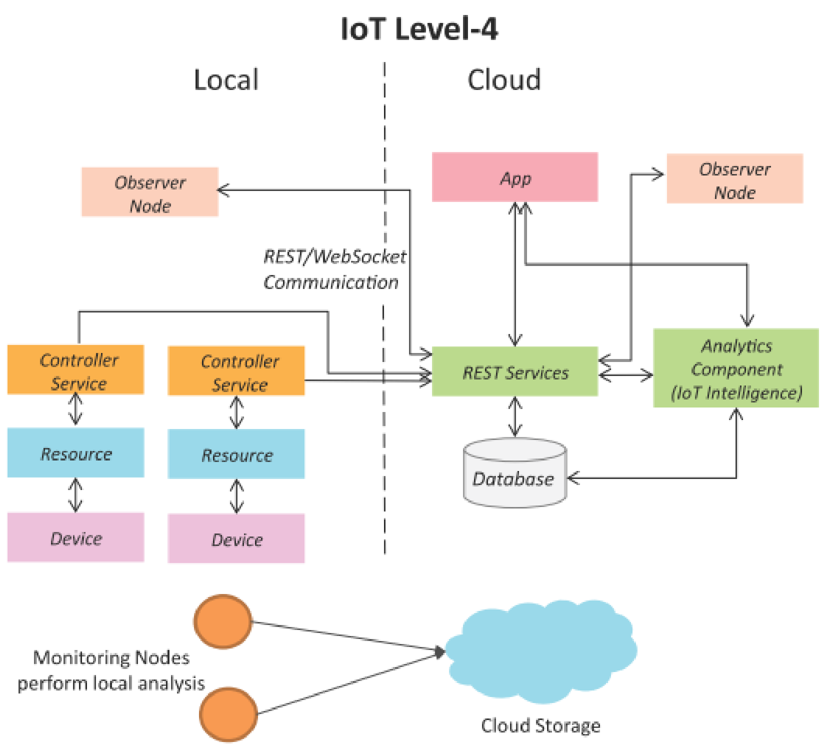
  EXAMPLE: Tracking Package Handling.



LEVEL-4:

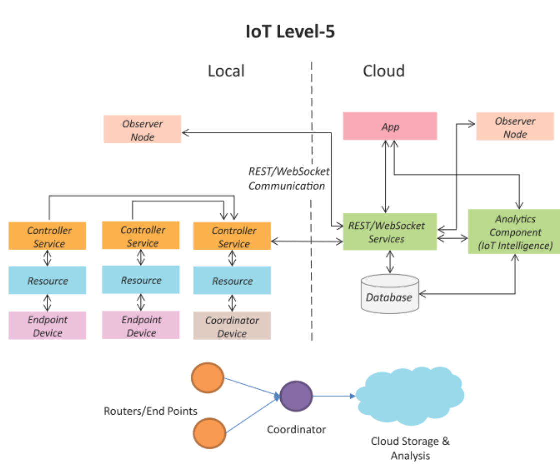
- A level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and the application is cloud-based.
- Level-4 contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- Level-4 IoT systems are suitable for solutions where multiple nodes are required, the data involved is big and the analysis requirements are computationally intensive.

EXAMPLE: SOUND SENSORS



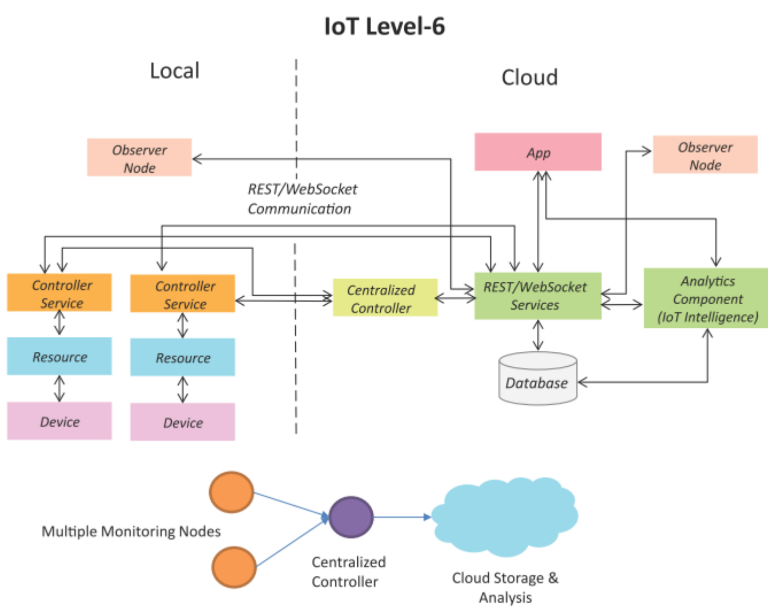
LEVEL-5:

- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes perform sensing and/or actuation.
- The coordinator node collects data from the end nodes and sends it to the cloud.
- Data is stored and analyzed in the cloud and the application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.



LEVEL-6:

- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and the application is cloud-based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.



Q3 :**EXPLAIN OVERVIEW OF MICROPROCESSOR AND MICROCONTROLLER**

ANS: Microprocessor:

Microprocessor is a type of computer processor in which both the data processing logic and control are included on a single integrated circuit or on small numbers of integrated circuits. These processors consist of logic, control and arithmetic circuits. Its integrated circuit is capable of interpreting and executing program instructions. These are multiple purpose, clockdriven and register based digital integrated circuits that accept input in binary data and processes it as per the instruction stored in its memory.

A microprocessor has the following components

• I/O Units

•Control units

•Arithmetic Logic Unit (ALU)

•Cache

•Registers

Types of Microprocessors:

1. CISC Microprocessor
2. DSP (Digital Signal Processor)
3. . RISC Microprocessor
4. Input/Output Processor (IOP)
5. Bit-Slice Microprocessors (BSM)
6. Graphics Processors
7. Coprocessor

Microcontroller:

A microcontroller is a small and low-cost microcomputer on a single VLSI integrated circuit (IC) chip. It is used for controlling portions of an electronic system through a microprocessor unit (MOU) and some peripherals. Microcontroller contains processor cores with additional peripherals such as serial interface, time, programmable I/O, and memory on the same chip. It interacts with other components due to its functionality that results from the combination of digital memory and digital processor with additional hardware. A microcontroller is also known as an Embedded controller, single-chip-computer, or a computer-on-a-chip.

Microcontrollers consist of the following mentioned components:

•Central Processing Unit (CPU) •Program Memory (ROM) •Data Memory (RAM) •Timers and Counters • I/O Ports (I/O – Input/Output) •Serial Communication Interface •Clock Circuit (Oscillator Circuit) • Interrupt Mechanism •CAN (Controlled Area Network) •SPI (Serial Peripheral Interface) • I2C (Inter Integrated Circuit) •DAC (Digital to Analog Converter) •ADC (Analog to Digital Converter) •USB (Universal Serial Bus)

Types of Microcontrollers:

1. Microcontrollers According to the size
   •8-bits Microcontroller
   •16-bits microcontroller:
   •32-bit microcontroller:

2. Microcontrollers According to Memory Device

   •**Embedded Memory Microcontroller:** Any embedded system with a microcontroller unit that consists of all functional blocks on a chip is known as an embedded microcontroller.

•**External Memory Microcontroller:** These microcontrollers do not have all functional blocks on a chip.

Q4: EXPLAIN IOT KEY FEATURES,ADVANTAGES AND DISADVANTAGES

ANS:

1. AI − IoT makes virtually anything “smart” , with the power of data collection, artificial intelligence algorithms, and networks. enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.

2. Connectivity − no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

3. Sensors − IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

4. Active Engagement − Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

5. Small Devices − Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

ADVANTAGES:

1. Improved Customer Engagement − Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

2. Technology Optimization − The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

3. Reduced Waste − IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real world information leading to more effective management of resources.

4. Enhanced Data Collection − Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

DISADVANTAGES:

Security − users exposed to various kinds of attackers. Privacy − personal data in extreme detail without the user's active participation.

Complexity − Complicated as use of multiple Flexibility integrate easily with another.

Compliance − in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging IO

Q5:EXPLAIN IOT HARDWARES AND SOFTWARES.

ANS: SOFTWARE-

Data Collection: manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks.

Device Integration :Software supporting integration binds (dependent relationships) all system devices to create the body of the IoT system.

Real-Time Analytics :take data or input from various devices and convert it into viable actions or clear patterns for human analysis.

Application and Process Extension :These applications extend the reach of existing systems and software to allow a wider, more effective system.

HARDWARE:

IoT − Sensors • Wearable Electronics • Standard Devices

IoT − Sensors :

Sensor is an input device which provides an output (signal) with respect to a specific physical quantity (input).

• It is a device that converts signals from one energy domain to electrical domain.

Classification of sensors

• Active: Sensors that require power supply are called as Active Sensors. ex: LiDAR (Light detection and ranging),

• Passive: Sensors that do not require power supply. ex: Radiometers, film photography

Analog Sensors: Analog Sensors produce an analog output i.e. a continuous output signal with respect to the quantity being measured.

Digital Sensors: produce an Digital output i.e. a discrete output signal with respect to the quantity being measured

Wearable Electronics

• Head − Helmets, glasses

• Neck − Jewelry, collars

• Arm − Watches, wristbands, rings

• Torso − Clothing, backpacks

• Feet – Socks, shoes

Standard Devices

• The desktop provides the user with the highest level of control over the system and its settings.

• The tablet provides access to the key features of the system in a way resembling the desktop, and also acts as a remote.

• The cellphone allows some essential settings modification and also provides remote functionality

routers and switches:

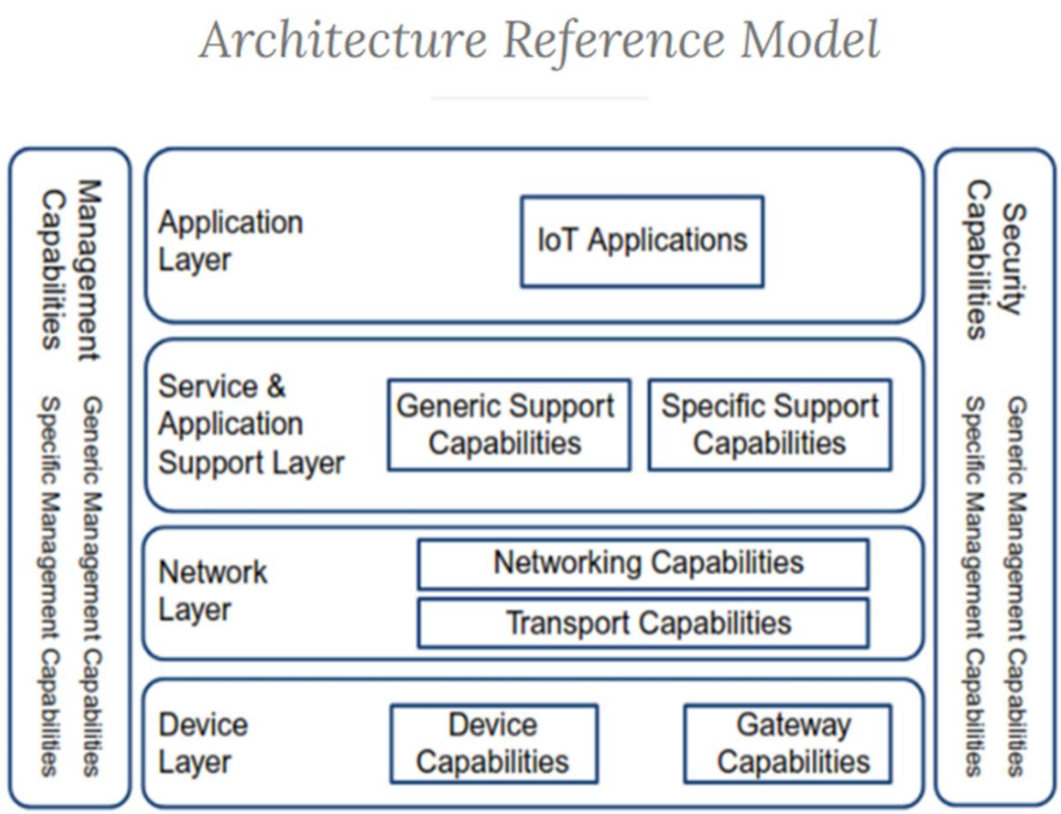
a switch is designed to connect computers within a network, while a router is designed to connect multiple networks together.

Q6 AND Q7 PDF

https://drive.google.com/drive/u/1/folders/1pTCXQqy2jS51xc-ahRjhkvX6auLS-HvX

->domain specific.pdf

Q8.EXPLAIN ARCHITECTURE REFERENCE MODEL



L

Application Layer: This layer includes the software applications that provide value to the end-users by leveraging the data and capabilities of the IoT system. Examples include smart home automation systems, industrial control systems, and wearable devices.

Service Layer: This layer includes the services that provide the logic and functionality of the IoT system, such as data storage, management, and processing. This layer may include cloud services, edge computing, and software as a service (SaaS) solutions.

Network Layer: This layer includes the communication protocols and network infrastructure that enable the devices and services in the IoT system to communicate with each other. Examples include wireless technologies such as Zigbee, Z-Wave, and Bluetooth, as well as cellular and internet protocols like HTTP, MQTT, and CoAP.

Device Layer: This layer includes the physical devices and sensors/actuators that collect data and perform actions in the physical world. Examples include temperature sensors, cameras, and actuators like lights and motors.

Management and Security: These are critical aspects of any IoT architecture, and include the systems and practices that ensure that devices, services, and data are secure, and can be managed, maintained, and updated over time. This layer includes security protocols, access controls, and device management.

Q9: EXPLAIN IOT FUNCTIONAL MODEL(Write in short and explain using keywords)

Functional model

The IoT Functional Model aims at describing mainly the Functional Groups (FG) and their interaction with the ARM, while the Functional View of a Reference Architecture describes the functional components of an FG, interfaces, and interactions between the components. The Functional View is typically derived from the Functional Model in conjunction with high-level requirements.

Device functional group

The Device FG contains all the possible functionality hosted by the physical Devices that are used for increment the Physical Entities. This Device functionality includes sensing, actuation, processing, storage, and identification components, the sophistication of which depends on the Device capabilities

Communication functional group

The Communication FG abstracts all the possible communication mechanisms used by the relevant Devices in an actual system in order to transfer information to the digital world components or other Devices.

IoT Service functional group

The IoT Service FG corresponds mainly to the Service class from the IoT Domain Model, and contains single IoT Services exposed by Resources hosted on Devices or in the Network (e.g. processing or storage Resources).

Virtual Entity functional group

The Virtual Entity FG corresponds to the Virtual Entity class in the IoT Domain Model, and contains the necessary functionality to manage associations between Virtual Entities with themselves as well as associations between Virtual Entities and related IoT Services, i.e. the Association objects for the IoT Information Model. Associations between Virtual Entities can be static or dynamic depending on the mobility of the Physical Entities related to the corresponding Virtual Entities.

IoT Service Organization functional group

The purpose of the IoT Service Organization FG is to host all functional components that support the composition and orchestration of IoT and Virtual Entity services. Moreover, this FG acts as a service hub between several other functional groups such as the IoT Process Management FG when, for example, service requests from Applications or the IoT Process Management are directed to the Resources implementing the necessary Services.

IoT Process Management functional group

The IoT Process Management FG is a collection of functionalities that allows smooth integration of IoT-related services (IoT Services, Virtual Entity Services, Composed Services) with the Enterprise (Business) Processes.

Management functional group

The Management FG includes the necessary functions for enabling fault and performance monitoring of the system, configuration for enabling the system to be flexible to changing User demands, and accounting for enabling subsequent billing for the usage of the system. Support functions such as management of ownership, administrative domain, rules and rights of functional components, and information stores are also included in the Management FG.

Security functional group

The Security FG contains the functional components that ensure the secure operation of the system as well as the management of privacy. The Security FG contains components for Authentication of Users (Applications, Humans), Authorization of access to Services by Users, secure communication (ensuring integrity and confidentiality of messages) between entities of the system such as Devices, Services, Applications, and last but not least, assurance of privacy of sensitive information relating to Human Users.

Q10: EXPLAIN IOT PROTOCOLS

1. 6LowPAN:
   IoT (Internet of Things) protocol 6LowPAN (IPv6 over Low power Wireless Personal Area Networks) is a networking protocol that allows for the communication of devices with limited processing power and memory. It is used to connect devices such as sensors, actuators, and other low-power devices to the internet using IPv6, the latest version of the internet protocol. 6LowPAN uses a header compression mechanism that allows for the efficient transmission of IPv6 packets over low-power wireless networks, such as Zigbee or Bluetooth Low Energy. This allows for the efficient use of limited resources while still providing the benefits of IPv6, such as large address space and end-to-end connectivity.

2. RPL:
   RPL (Routing Protocol for Low-Power and Lossy Networks) is a routing protocol designed for use in low-power, wireless sensor networks and other Internet of Things (IoT) devices. RPL uses a directed acyclic graph (DAG) structure to create a tree topology for the network, where each node has a single parent and zero or more children. The DAG is rooted at a special node called the "root" and each node in the network maintains a routing table that contains information about the best next hop to reach the root.

   RPL uses a number of metrics to determine the best path to the root, such as the number of hops, the link quality, and the energy consumption. This allows for the efficient use of network resources while ensuring that the network is robust and reliable.

3.CoAP:

CoAP (Constrained Application Protocol) is a lightweight application protocol designed for use in resource-constrained devices and networks, such as those found in the Internet of Things (IoT). It is based on the principles of HTTP (Hypertext Transfer Protocol) and is designed to be simple and efficient, while still providing the functionality of a full-featured application protocol.

CoAP uses a request/response model similar to HTTP, but with a more compact binary format for messages, which reduces the overhead and processing requirements for devices. The protocol also supports multicast communication, which allows for efficient communication between groups of devices.

3.MQTT:

MQTT (Message Queue Telemetry Transport) is a lightweight messaging protocol designed for use in resource-constrained devices and networks, such as those found in the Internet of Things (IoT). It is designed to be simple and efficient, while still providing the functionality of a full-featured messaging protocol. MQTT uses a publish/subscribe model, where devices can publish messages to a specific topic and other devices can subscribe to that topic to receive the messages. he protocol also supports Quality of Service (QoS) levels, which can be used to ensure that messages are delivered reliably.

MQTT is designed to be lightweight and efficient, which makes it well-suited for use in low-power devices and networks with limited bandwidth. The protocol also supports security mechanisms, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).