Dhruv Singhal || 500075346 || R177219074 || BATCH-5(AI&ML)

ASSIGNMENT - 2

1. Define Device Configuration and Management in detail.

Device configuration is the process of defining operation, flow, and controls of a network in the initial phase & maintaining the information collaborated with all the components in that network.

Device configuration & management is the process of checking the setup configurations of all the network devices & maintaining the software and firmware installed on them. This process focuses on the discovery of devices in a network & then monitoring of device configuration, checking the status, and the maintenance of inventory.
Using this process we can focus on -

- Incident management
- Problem management
- Change management
- Maintenance, Safety and Risk management

Industrial Examples of Device Configuration & Management -
Airlines
In tracking the parts and components in an aircraft for safety & maintenance.
Banking
In the banking sector, device configuration & management is used for service support, incident management and IT risk management.
Telecom
In the telecom sector, a configuration management database is maintained which includes relationships between components which can be used to determine the impact of failures.
Space
In complex space missions, keeping a track on detailed configuration of softwares & components is required. Change is carefully controlled and managed to mission objectives using the configuration information. When a mission launches, configuration management includes exact details of how it is configured. This information can be used to find workarounds. If a rover breaks down while exploring an alien planet, you want to know exactly how it is designed and configured. All these tasks can be maintained using the Device Configuration & management process.

2. Short Notes

a. IoT Verticals

Verticals are business functions where vendors generally
serve a specific type of customers and fulfil their set of needs. IoT verticals refer to all the technologies the IoT sector has to offer. Top IoT verticals include Agriculture & Farming,

Energy, Enterprise, Finance, Healthcare, Industrial, Retail and Transportation. Such verticals include a plethora of sensors providing information about device status, service configuration, and performance, etc

b. Wireless Network
A wireless network is a computer network that uses wireless data connections between network nodes. It is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.
Types of Wireless Networks in IoT:

I. **Cellula**r - Cellular networks use the same mobile networks as smartphones to allow IoT devices to communicate.

II. **Local and Personal Area Networks (LAN/PAN)** -
Wireless personal and local area network technologies that are commonly incorporated into IoT connectivity solutions are WIFI and Bluetooth.

III. **Low Power Wide Area Networks (LPWAN)** -
IoT devices that run on LPWANs send small packets of information infrequently and over long distances. LPWAN provides longer-range than WiFi and Bluetooth.

IV. **Mesh Networks** -
In mesh networks, all the sensor nodes cooperate to distribute data amongst each other to reach the gateway. **Zigbee** is one example of an IoT wireless network technology.

V. **RFID** - Radio Frequency Identification
It is used to automatically identify an object and capture data about that object that has been stored in a small microchip tag and attached to the object.

3. Discuss IoT requirements in detail.

The key requirements of IoT include -
a. **Security**:
Security is a very critical requirement in IoT solutions, and the oneM2M defines its security framework including identification, authorization and authentication. Our middleware platform can be registered to the oneM2M server (i.e., Mobius) as an application entity. It can attempt to access a list of authorized resources hosted by the server with its server-generated unique identifier and privileges, called access control policy. However, authentication and other security components such as certificates still remain incomplete.

b. **Privacy**:
A huge amount of data will be stored in IoT platforms, having great potential in providing people with valuable services across different application domains. At the same time,

however, it leads to obvious privacy issues, for example, normal users obviously need to decide the level of disclosure for the collected personal data to protect privacy.

c. **Scalability**:
An IoT platform needs to support rapidly growing numbers of IoT devices and keep a certain level of QoS support. Although the scalability of an IoT platform is crucial, it highly depends on implementation and performance in IoT servers rather than connected devices.

d. **Resource management**:
The resources include battery-time, memory usage, and other data related to application performance to make quality of service (QoS) reliable.

e. **Ease of deployment, maintenance, and use**:
The platform-installed devices need to be easily maintained through existing device management technologies.

4. Discuss Cellular Machine-to-Machine (M2M) application networks.

Cellular M2M is a mode of communication, within which data is transmitted over an extended network. Cellular networks permit machines to exchange data with other machines, services, and applications running within the cloud software. M2M or machine-to-machine are often found over WAN and might be employed in cellular networks. There are 3 main components in M2M, they're sensors, a wireless network, and internet-connected servers. Some samples of M2M are serial connection, wireless communication in IoT and PLC.

Advantages of M2M
There are various advantages of M2M like low power consumption, packet-switched service, functionality to detect events, time tolerance, etc.

Applications

- Machine-to-machine communication is often used for remote monitoring.
- In product restocking, tracking and monitoring.
- In telemedicine the patient’s condition can be monitored in real time.
- In smart homes, appliances have real time control of operations and remote communication is also possible.
- It is also useful in remote-control software, robotics, traffic control, and security.