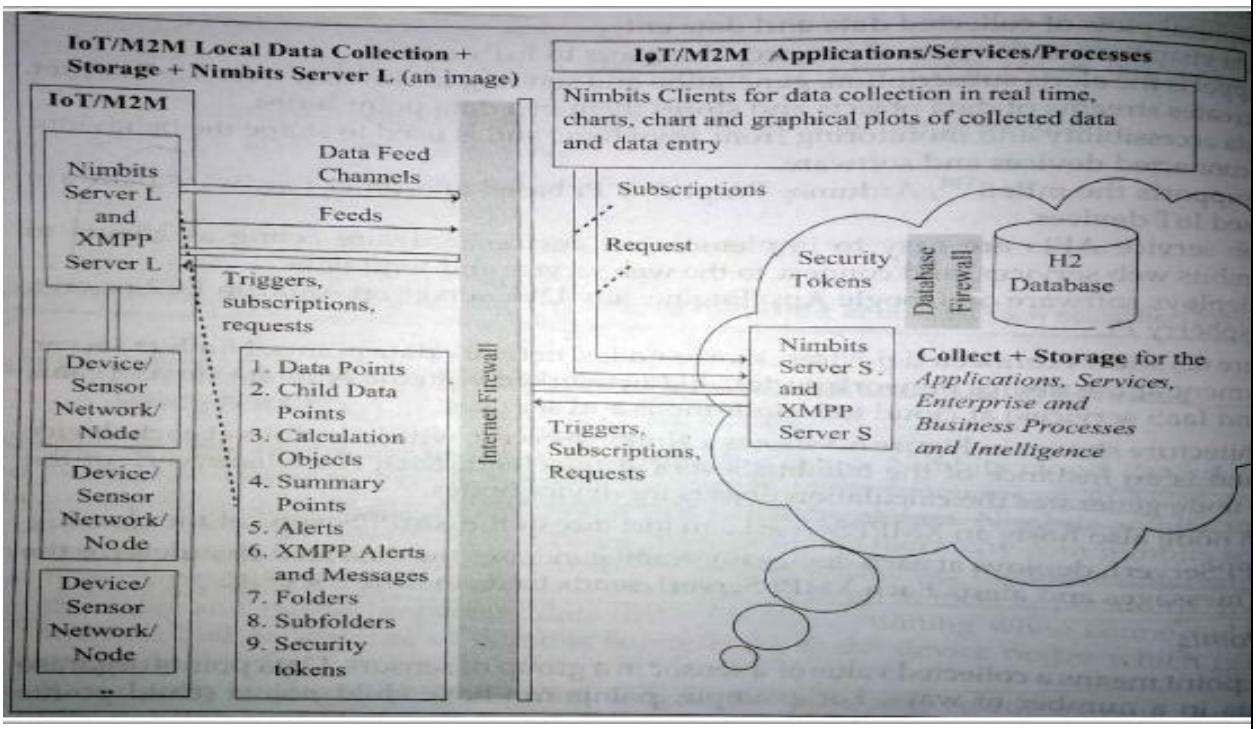
Sub:	IoT&WSN					Sub Code:18EC741
Date:	8/02/2021	Duration:	90 Minutes	Max Marks:	50	Sem / Sec:

Scheme and Solution

1 Explain IoT cloud based data collection, storage and computing services using Nimbits. [10]

- Nimbits is a platform as a service (PaaS) used to develop software and hardware solutions that seamlessly connect to the cloud and each other.
- Nimbits server runs on powerful cloud platforms like Google App Engine to the smallest Raspberry Pi device.
- Nimbits server is a web portal and API designed to
- Provides time-stamping or geo-stamping on incoming data.
- Store and process that time and location stamped data over cloud (pushing the data over cloud and store them in a data point)
- Provide filtering to incoming data from noise, add important changes to it and then generate trigger events and alerts based on rules and then sending them in real time over internet.
- It provides rule engine for connecting sensors, persons and software to cloud.
- Nimbits clients can plot charts and graphs of real time collected data over the internet.
- It supports many format like text, JSON or XML values into the cloud.
- It provides edge computing locally on devices and nodes**.**
- It supports multiprogramming languages, M2M communication and hardware platform of IoT devices like mbed, Arduino, raspberry Pi based etc.
- Nimbits data points can relay data between the software systems or hardware devices like Arduino, using cloud as backend.
- It provides data logging services, access and data monitoring from anywhere.



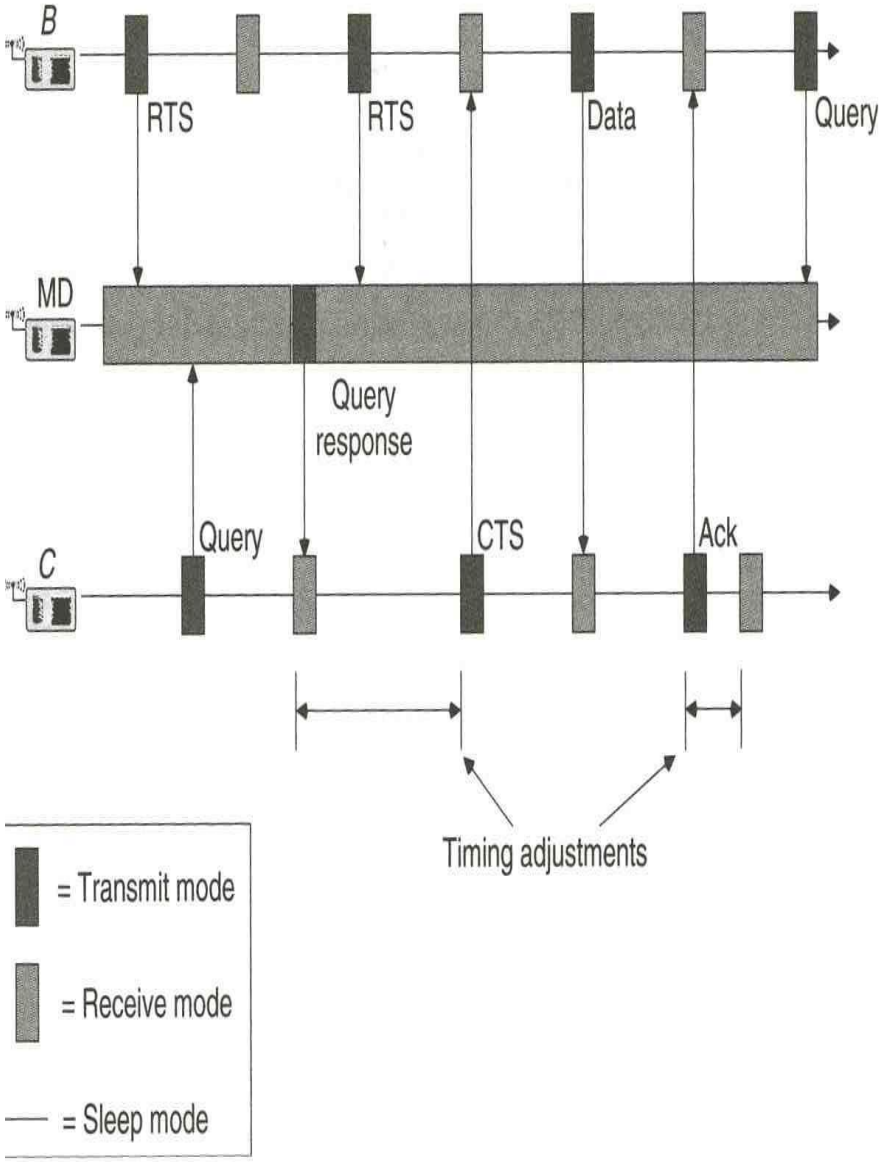
2 Explain Mediation Device Protocol with advantages and disadvantages.. [10]

- Basically a lot of time and energy is wasted in waiting for query beacon
- **Hence mediation device (MD) is used which is available all the time.**

- **It is a dynamic synchronization approach where tranmitter does not need to wake up permanentlly to detect the query beacons.**
- **It acts as a mediator for query and query response.**

Working:

- First Sender **B** sends **RTS** to **MD**
- **MD** stores this information
- Receiver **C** sends **query** to **MD**
- **MD** sends **Query response** which contain B's Address and timing information.
- **MD** tells reciever **C** when to wake up and transmit.
- **C** sends **CTS** to **B (now in sync)**
- **B sends data**
- **C** sends **ACK to B**
- **C returns to old timing**



Main advantage:

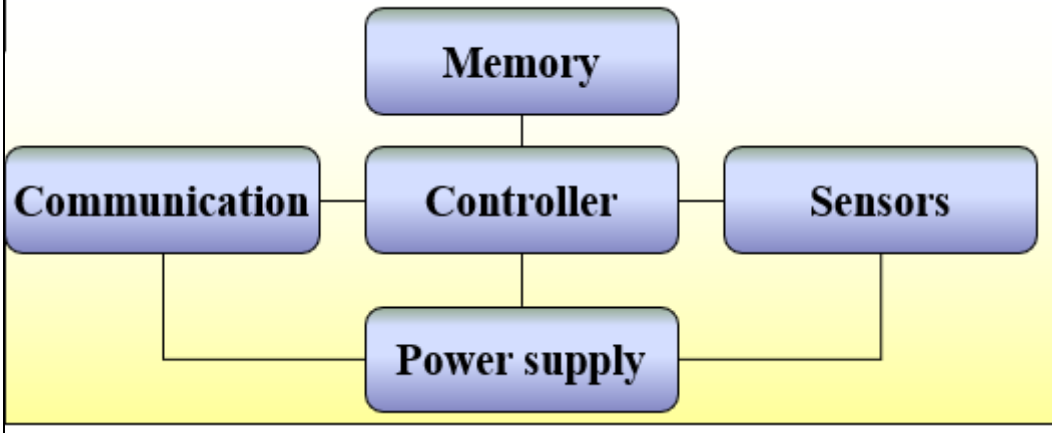
- **It does not require time synchronization between the nodes,** only mediation device needs to learn the period.
- It **save energy** also as most of energy burdon has shifted to mediation device.

Disadvantage:

- **Nodes transmit their query beacon withour checking for ongoing transmissions and leads to collisions**.
- Mediation device also require the energy.

There is no guarantees the mediation devices will cover all the sufficient nodes

3 Explain the single node architecture with necessary hardware components. [10]



Controller functionality

- **It is core of a wireless sensor network.**
- **It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes and decides on actuator's behavior.**
- **It is CPU of sensor node as it executes various programs ranging from time critical signal processing and communication protocols to application protocols.**

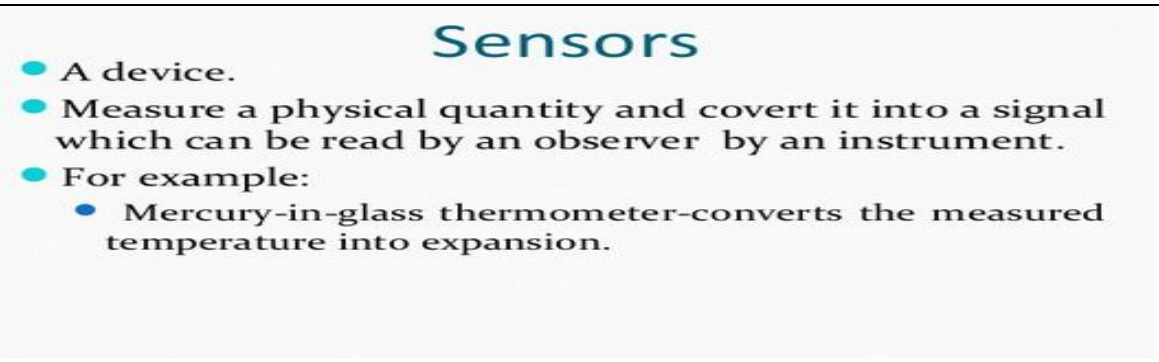
Communication Module

- **The communication module of a sensor node is called "Radio Transceiver".**
- **The essentially tasks of transceiver is to "transmit" and "receive" data between a pair of nodes.**
- **Depends upon the a) Choice of transmission medium b) Transceivers**
- **Both wired and wireless communication can be used.**
- **Wired communication:**

It can be carried out by using field buses like LON, CAN etc.

- **Wireless communication**

✓ **It can be radio frequencies, light, ultrasound etc**
✓ **It provides relatively high data rate and does not require the**
✓ **line of sight between sender and receiver.**
✓ **It uses communication frequency between 433 MHz to 2.4**
✓ **GHz.**



Power supply can be through

a) **Through batteries**
b) **Energy scavenging**

- **Memory:**
- ✓ **Memory is required to store programs and intermediate data; usually, different types of memory are used in WSN for programs and data.**
- ✓ **Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on.**
- ✓ **RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted.**
- ✓ **Read-Only Memory (ROM) Program code can be stored in Read-Only Memory (ROM) or in Electrically Erasable Programmable Read-Only Memory (EEPROM) or flash memory.**
- ✓ **Flash memory is similar to EEPROM but data can be erased or written in blocks instead of only a byte at a time. It can also serve as intermediate storage of data in case RAM is insufficient or the power supply of RAM should be shut down.**

4 . Explain the CSMA protocol with proper flow diagram. [10]

- CSMA protocols are contention-based, where neighbors try their luck to transmit their packet.
- The node sense the channel before transmitting.
- If the channel is busy then the node selects other random channel, repeats the carrier sensing and after a number of unsuccessful trials it just backsoff.
- And if the channel is idle then it start transmitting.

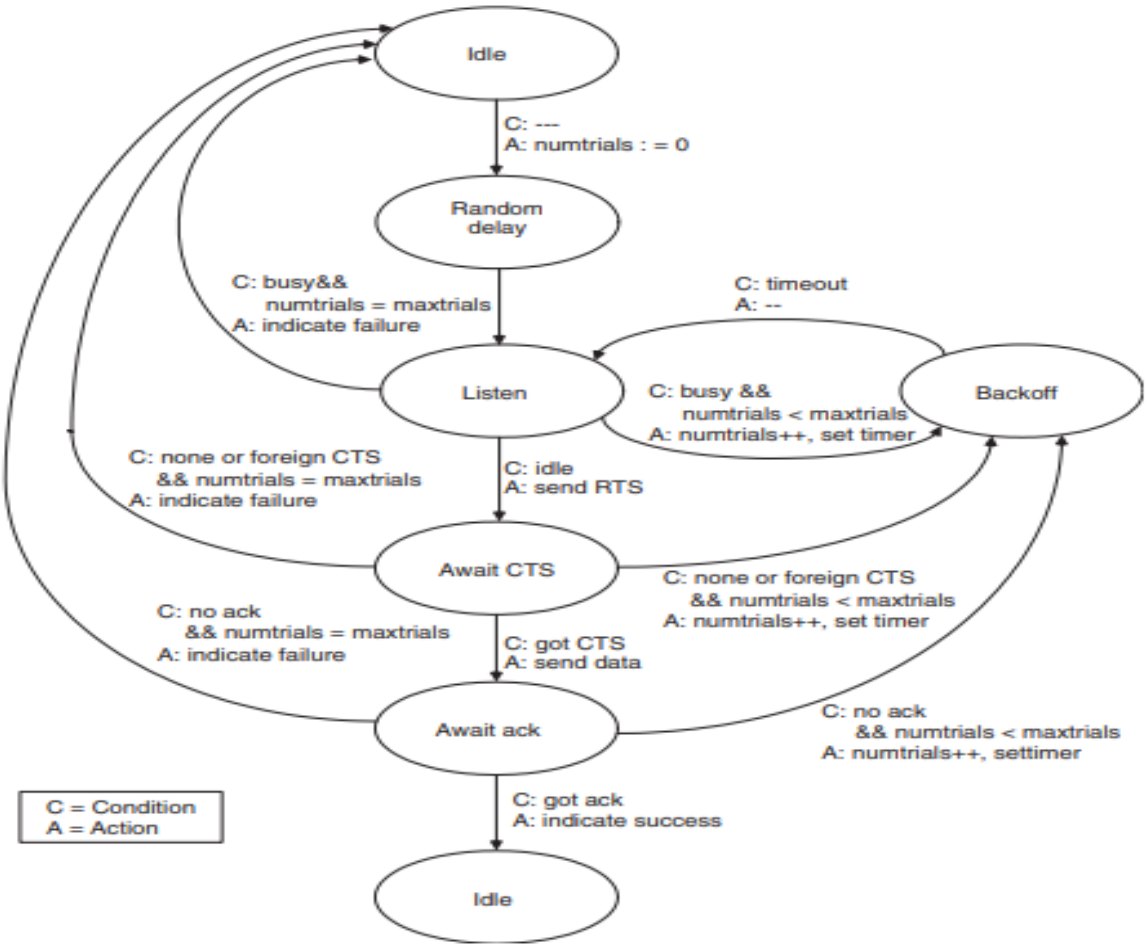


Figure 5.9 Schematic of the CSMA protocol presented in reference [888]

Step1: ["Idle state"]

- Normally the nodes are in "idle state".

Step 2: ["Random delay"]

- When it receives the packet from upper layer for transmission to lower layer (called as downstream node), it restarts the "Random Delay".
- Counter "numtrials" is =0;
- ***The purpose of "Random delay" is to desynchronized the nodes if initially synchronized by the external event.***

Step3: ["Listen"]

- The nodes perform carrier listening for some time
- If the medium is found busy, it goes to **"Backoff"** mode.
- If the medium is found free, the node transmits "**RTS"** packet and enters **"Await CTS state"**.

Step4: ["Backoff"]

- Here nodes wait for a random amount of time for the channel to be free and then goes to sleep state.
- **"Backoff"** period is used by application layer for the **"phase change" i.e.** ***to desynchronize the periodic traffic of different nodes***.
- **After the "Backoff"** period nodes listens again.

Step5: ["Await CTS state"]

- Here the node waits for CTS packet.
- If CTS packet arrives in time then node sends its data packet and waits for
- Acknowledgement and enter into **"Await ack"** state.
- Otherwise go back to **"Backoff"** state or drop the packet depending upon "numtrials" values.

Step6: ["Await ack state"]

- It can be explicit ack or parent node piggybacks the ack on packet and then forwarded to grandparent.

5	Write short note on 1) XMPP 2)COAP 3)MQTT 4)HTTP [10]

MQTT (Message Queuing Telemetry Transport)

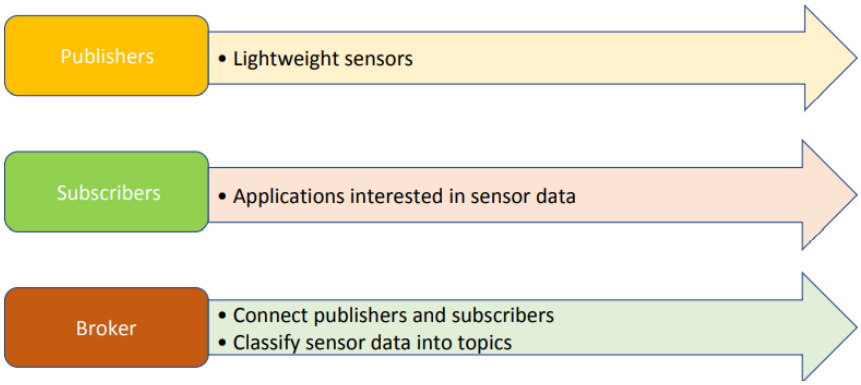
• An open source protocol for machine-to-machine (M2M)/"Internet of Things" connectivity

• (Telemetry dictionary meaning is measuring and sending values or messages to far off places by radio or other mechanism)

• Created by IBM IN 1999, as a constrained environment protocol.

• Designed to provide connectivity (mostly embedded) between applications and middle-wares (M2M/IOT objects) on one side and networks and communications (WEB Objects) on the other side

MQTT Components



XMPP (Extensible Messaging and Presence Protocol)

XMPP uses XML technology for real time communication includes instant messaging (used in multiuser chat) Presence Collaboration.

The protocol is used in constrained environment for messaging.

XMPP (Extensible Messaging and Presence Protocol)

X- Extensible: XMPP is designed to be extensible, in has been designed to grow and accommodate changes.

M-Messaging: XMPP has been designed to send instant message.

P-Presence: The presence indicator tells the server that you are online/offline/busy. Protocol:

XMPP is a protocol; a set of standards to talk to each other. It is widely used across web but is unadvertised

Constrained Application Protocol (**CoAP**) is a specialized Internet application protocol for constrained devices, as defined in RCF272.

It enables those constrained devices called "nodes" to communicate with the wider Internet using similar protocols.

CoAP is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.

CoAP is a service layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as Multicast support, very low overhead, and

simplicity.Multicast, low overhead, and simplicity are important for IoT and M2M communication, which tend to be deeply Embedded and have much less memory and power supply than traditional internet devices have.

Hyper text transfer Protocol (HTTP) uses port number 80.

A WEB HTTP Server listens to port number 80 only and respond to port number 80 only.

The port number is specified after TLD (Top level Domain) like http://www.vtu.ac.in:80/test.html

HTTP is an web's application-layer protocol: Used for transmitting various forms of data between sever and client like plaintext, hypertext, image and sound.

HTTP is an client server protocol: It allows two machines to communicate using a reliable, connection oriented transport service such as TCP.

HTTP is flexible and connectionless: The HTTP client (browser) initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server processes the request and re-establishes the connection with the client to send a response back.

HTTP is media independent: Any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content.

HTTP is a very light protocol: It has a **small format and is fast.**

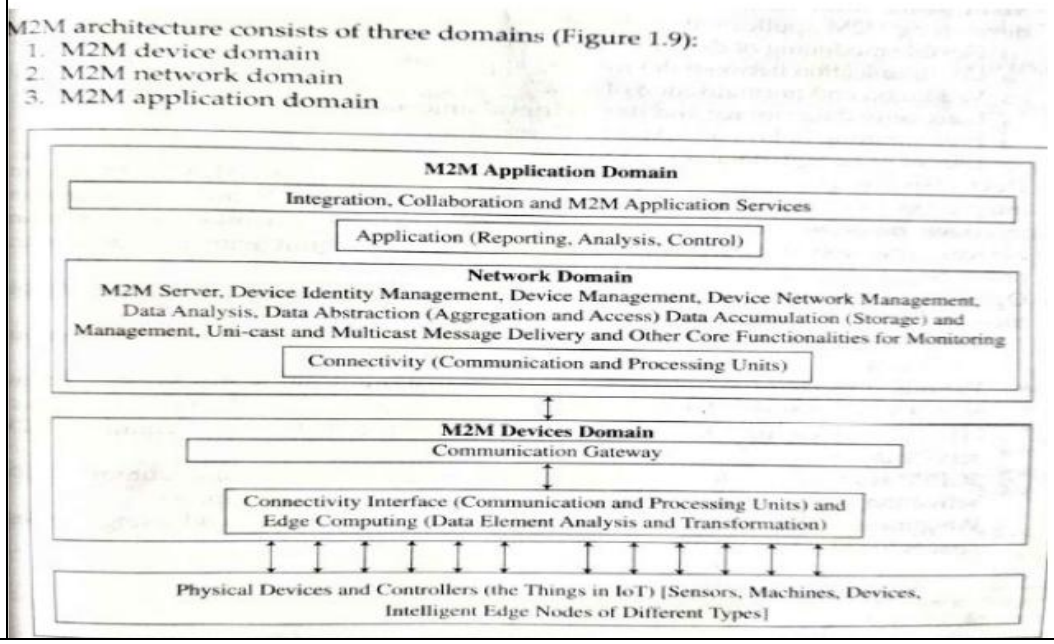
HTTP is based on Object Oriented Programming System (OOPS): The objects are identified by URL.

HTTP is stateless: The server and client are aware of each other only during a current request.

6 Explain three domains of M2M Architecture. What are the differences between IoT and M2M?.[10]

M2M refers to the process of communication of the physical devices or machines or smart devices with the other machines of same type without intervention of humans.

M2M architecture consists of three domains (Figure 1.9):
1. M2M device domain
2. M2M network domain
3. M2M application domain



M2M	IoT
Simple device-to-device communication usually within an embedded software at client site	Grand-scale projects and want-it-all approach
Isolated systems of devices using same standards	Integrates devices, data and applications across varying standards
Limited scalability options	Inherently more scalable
Wired or cellular network used for connectivity	Usually devices require active Internet connection
Extensive background of historical applications	State-of-the-art approach with roots in M2M

7 Give five applications of IOT. [10]

1. Smart Homes

One of the best and the most practical applications of IoT, smart homes really take both, convenience and home security, to the next level. Though there are different levels at which IoT is applied for smart homes, the best is the one that blends intelligent utility systems and entertainment together. For instance, your electricity meter with an IoT device giving you insights into your everyday water usage, your set-top box that allows you to record shows from remote, Automatic Illumination Systems, Advanced Locking Systems, Connected Surveillance Systems all fit into this concept of smart homes. As IoT evolves, we can be sure that most of the devices will become smarter, enabling enhanced home security.

2. Smart City

Not just internet access to people in a city but to the devices in it as well – that's what smart cities are supposed to be made of. And we can proudly say that we're going towards realizing this dream. Efforts are being made to incorporate connected technology into infrastructural requirements and some vital concerns like Traffic Management, Waste Management, Water Distribution, Electricity Management, and more. All these work towards eliminating some day-to-day challenges faced by people and bring in added convenience.

3. Self-driven Cars

We've seen a lot about self-driven cars. Google tried it out, Tesla tested it, and even Uber came up with a version of self-driven cars that it later shelved. Since it's human lives on the roads that we're dealing with, we need to ensure the technology has all that it takes to ensure better safety for the passenger and those on the roads.

The cars use several sensors and embedded systems connected to the Cloud and the internet to keep generating data and sending them to the Cloud for informed decision-making through Machine Learning. Though it will take a few more years for the technology to evolve completely and for countries to amend laws and policies, what we're witnessing right now is one of the best applications of IoT.

4. IoT Retail Shops

If you haven't already seen the video of Amazon Go – the concept store from the eCommerce giant, you should check it out right away. Perhaps this is the best use of the technology in bridging the gap between an online store and a retail store. The retail store allows you to go cashless by deducting money from your Amazon wallet. It also adds items to your cart in real-time when you pick products from the shelves.

If you change your mind and pick up another article, the previous one gets deleted and replaces your cart

	with the new item. The best part of the concept store is that there is no cashier to bill your products. You don't have to stand in line but just step out after you pick up your products from shelves. If this technology is effective enough to fetch more patronage, this is sure to become a norm in the coming years. 5. Farming Farming is one sector that will benefit the most from the Internet of Things. With so many developments happening on tools farmers can use for agriculture, the future is sure promising. Tools are being developed for Drip Irrigation, understanding crop patterns, Water Distribution, drones for Farm Surveillance, and more. These will allow farmers to come up with a more productive yield and take care of the concerns better.
8	Explain IPV4 and IPV6 with necessary figures [10] ➢ IPV6 Provides a large address space (total 2^128 addresses) ➢ Big size datagram (128 bits). ➢ Uses routers, subnet and interfaces for the delivery of services. ➢ Manages device mobility, security and configuration aspects. ➢ Support unicast, multicast and anycast addressing. ➢ Permits hierarchical address allocation. ➢ Provisions additional optimisation for the delivery of services using routers, subnet and interfaces. ➢ Extensibility of options. ➔ IPv4 is **an unreliable and connectionless** datagram protocol ➔ If reliability is required, **IPv4 must be paired with a reliable protocol such as TCP.** ➔ This means that each datagram is handled independently, and **each datagram can follow a different route to the destination** and can arrive out of order. ➔ ***IPv4 provides no error control or flow control*** ➔ IPv4 relies on a higher-level protocol to take care of all these problems. **Packets in IPV4 are called datagrams**