Unit I
Introduction to IoT

Dr. Prabhakar D. Khandait

HOD (ETC)

KDKCE, Nagpur

IoT

Unit I: Introduction to IoT (4)

- IoT definition & Characteristics,
- Advantages and disadvantages,
- IoT functional blocks, sensing , actuation ,
- Physical design of IoT,
- Logical design of IoT,
- Constraints affecting design in IoT .

RTMNU Questions S-23

1.	a)	Define Internet of Things. Also discuss the various characteristics of IOT.	7
	b)	Explain the IOT functional blocks in detail.	7
		OR	
2.	a)	Discuss the physical design of IOT.	7
	b)	Explain the various constraints affecting design in IOT.	7

RTMNU Questions W-23

1. a) Define IoT. List the advantages & disadvantage of IoT. 6

   b) Explain the physical and logical design of IoT in detail. 8

OR

2. a) Explain the IoT function blocks in detail. 8

   b) List out the features of IoT. 6

Introduction

- Internet of Things (IoT) comprises things that have unique identities and are connected to the internet.
- Existing devices , such as networked computers or 4G enabled mobile phones already have some form of unique identities and are also connected to the internet, the focus on IoT is in the configuration, control and networking via the internet of devices or things , that are traditionally not associated with the Internet.
- These include devices such as thermostats, utility meters, a blue tooth- connected headset, irrigation pumps and sensor or control circuits for an electric car's engine

Introduction …….

- Experts already forecasted that by the year 2020 there will be a total of 50 billion devices/ things connected to the internet.
- The scope of IoT is not limited to just connected things(Devices, appliance, machines) to the Internet.
- Applications on IoT networks extract and create information from lower level data by filtering, processing , categorizing, condensing and contextualizing the data.
- The information obtained is then organized and structured to infer knowledge about the system and or its user, its environment and its operations and progress towards its objectives, allowing a smarter performance.

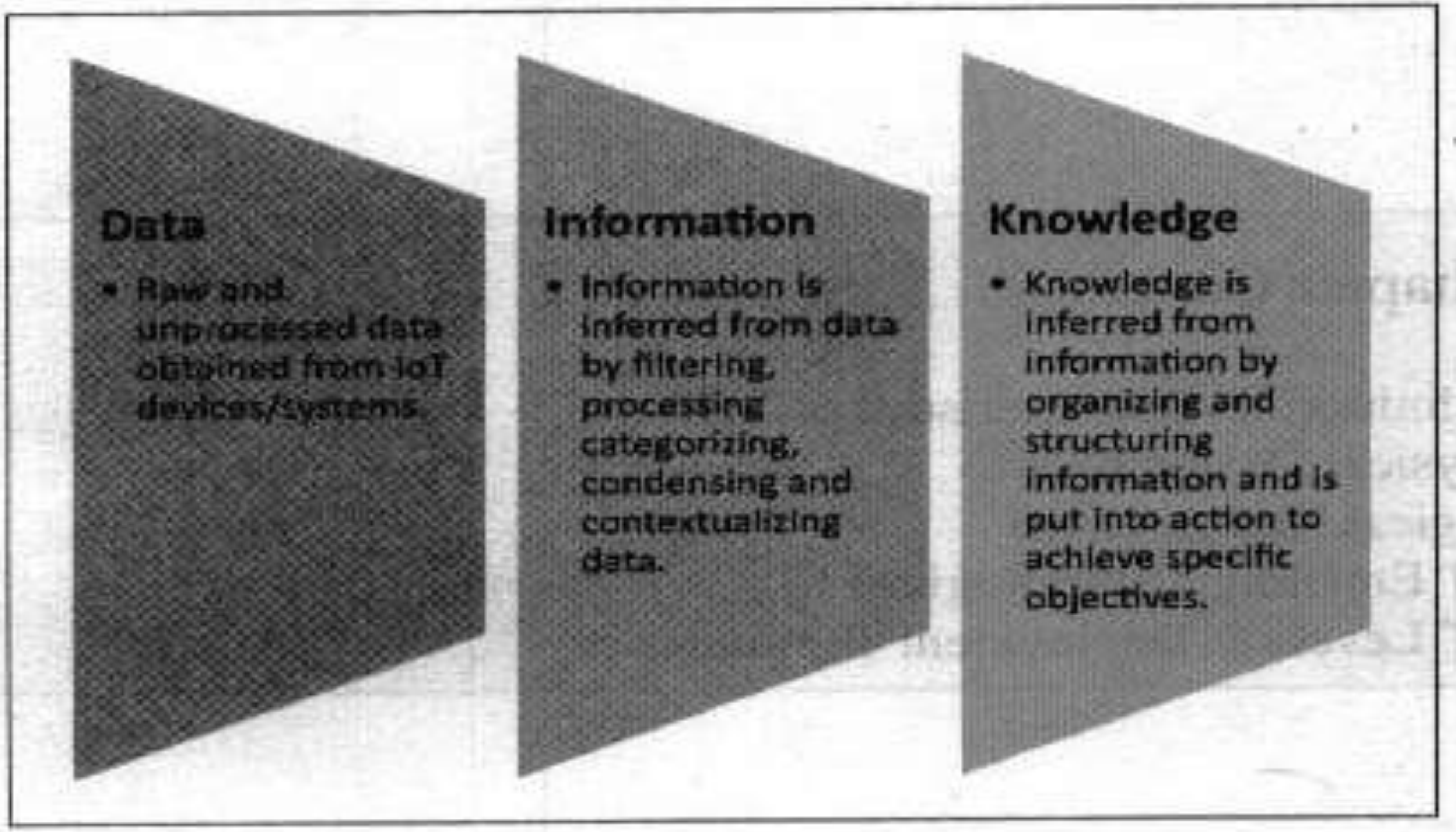


Figure 1.1: Inferring information and knowledge from data

IoT definition & Characteristics

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

IoT definition….

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

IoT definition….

- Internet of Things (IoT) has been defined as

Definition: A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual Things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, often communicate data associated with users and their environments.

IoT Characteristics

Dynamic & Self-Adapting: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions besed on their operating conditions, user's context, or seed environment. For example, consider a surveillance system comprising of a number of surveillance cameras. The surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether day or night. Cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same.

In this example, the surveillance system is adapting itself based on the context and changing (e.g.dynamic) conditions.

Self-Configuring: IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability configure themselves (in association with the IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.

- Interoperable Communication Protocols: IoT devices may support a number of Interoperable communication protocols and can communicate with other devices and also with the infrastructure.
- Unique Identity: Each loT device has a unique identity and a unique identifier (such as an IP address or a URI). IoT systems may have intelligent interfaces which adapt based on the context, allow communicating with users and the environmental contexts.
- IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure.

Integrated into Information Network: loT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves (and their characteristics) to other devices or user applications.

For example, a weather monitoring node can describe its monitoring capabilities to another connected node so that they can communicate and exchange data.

Integration into the information network helps in making loT systems "smarter" due to the collective intelligence of the individual devices in collaboration with the infrastructure. Thus, the data from a large number of connected weather monitoring IoT nodes can be aggregated and analyzed to predict the weather.

Key Features of IOT

1. Connectivity

- **Definition:** The ability of devices to connect with each other and to centralized servers or cloud platforms through various communication protocols.
- **Technologies:** Wi-Fi, Bluetooth, Zigbee, LTE, 5G, LoRaWAN, and Ethernet.
- **Importance:** Without connectivity, IoT devices cannot function as a network, limiting data collection and automation.

2. Data Collection and Sensing

- **Definition:** IoT devices are equipped with sensors to monitor real-world parameters such as temperature, humidity, motion, light, etc.
- **Types of Sensors:** Temperature sensors, accelerometers, gyroscopes, gas sensors, RFID tags, etc.
- **Role:** Sensors collect raw data, which is crucial for monitoring, analysis, and decision-making.

Key Features of IOT

3. Data Processing and Analytics

- **Definition:** After data collection, IoT systems process and analyze this data to derive meaningful insights.
- **Methods:** Edge computing (processing data closer to the source) and cloud computing.
- **Purpose:** Real-time processing helps in quick decision-making, reducing latency for critical applications (e.g., autonomous vehicles).

4. Device Autonomy and Control

- **Definition:** IoT systems can make decisions based on processed data without human intervention.
- **Example:** A smart thermostat adjusts room temperature automatically based on environmental data and user preferences.
- **Automation:** Reduces the need for manual control, enhancing efficiency and convenience.

Key Features of IOT

5. Scalability

- **Definition:** IoT networks can easily expand by adding more devices without affecting performance.
- **Challenges:** As networks grow, they require efficient data management, robust communication protocols, and scalable cloud infrastructure.

6. Interoperability

- **Definition:** The ability of different IoT devices and platforms to work together seamlessly, regardless of the manufacturer or technology used.
- **Standards:** MQTT, CoAP, HTTP, OPC UA, etc.
- **Benefit:** Ensures that devices from different vendors can communicate effectively.

Key Features of IOT

7. Security and Privacy

- **Definition:** Measures to protect data integrity, confidentiality, and availability in IoT systems.
- **Threats:** Data breaches, unauthorized access, and cyberattacks.
- **Techniques:** Encryption, secure boot, device authentication, and regular firmware updates.

8. Energy Efficiency

- **Definition:** IoT devices, especially battery-powered ones, are designed to consume minimal energy to prolong operational life.
- **Techniques:** Low-power hardware components, optimized communication protocols (e.g., BLE), and sleep modes.
- **Importance:** Crucial for remote or hard-to-reach devices where frequent charging is not feasible.

Key Features of IOT

9. Real-Time Monitoring and Feedback

- **Definition:** IoT systems can monitor environments in real-time and provide instant feedback.
- **Applications:** Smart cities (traffic control), healthcare (patient monitoring), and industrial automation (predictive maintenance).
- **Advantage:** Enables quick responses to dynamic changes, improving efficiency and safety.

10. Cloud Integration

- **Definition:** Most IoT systems are integrated with cloud platforms for data storage, processing, and remote access.
- **Benefits:** Centralized data management, advanced analytics, remote device control, and scalability.
- **Platforms:** AWS IoT, Microsoft Azure IoT Hub, Google Cloud IoT Core.

Key Features of IOT

11. Cost Efficiency

- **Definition:** Although initial setup can be expensive, IoT reduces long-term costs through automation, predictive maintenance, and optimized resource usage.
- **Impact:** Energy savings, reduced downtime in industries, and improved operational efficiency.

12. Artificial Intelligence and Machine Learning Integration

- **Definition:** IoT devices often leverage AI/ML for advanced data analytics, pattern recognition, and decision-making.
- **Example:** Smart cameras that detect unusual activities or predictive maintenance systems that forecast equipment failures.

Advantages of IoT

- Internet of things facilitates several advantages in our daily lives. Some of its advantages are given below:
- **Minimize human effort:** As IoT devices interact and communicate with each other, they can automate the tasks helping to improve the quality of a business's services and reducing the need for human intervention.
- **Save time:** By reducing the human effort, it saves a lot of our time. Saving time is one of the primary advantages of using the IoT platform.
- **Enhanced data collection:** Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real-time. Hence these devices can access information from anywhere at any time on any device.
- **Improved security:** If we have an interconnected system, it can assist in the smarter control of homes and cities through mobile phones. It enhances security and offers personal protection.

Advantages of IoT….

- **Efficient resource utilization:** We can increase resource utilization and monitor natural resources by knowing the functionality and how each device works.
- **Reduced use of other electronic equipment:** Electric devices are directly connected and can communicate with a controller computer, such as a mobile phone, resulting in efficient electricity use. Hence, there will be no unnecessary use of electrical equipment.
- **Use in traffic systems:** Asset tracking, delivery, surveillance, traffic or transportation tracking, inventory control, individual order tracking, and customer management can be more cost-effective with the right tracking system using IoT technology.
- **Useful for safety concerns:** It is helpful for safety because it senses any potential danger and warns users. For example, GM OnStar is an integrated device that identifies a car crash or accident on the road. It immediately makes a call if an accident or crash is found.

Advantages of IoT....

- **Useful in the healthcare industry:** Patient care can be performed more effectively in real-time without needing a doctor’s visit. It gives them the ability to make choices as well as provide evidence-based care.

Advantages	Disadvantages
Minimizes the human work and effort	Increased privacy concerns
Saves time and effort	Increased unemployment rates
Good for personal safety and security	Highly dependent on the internet
Useful in traffic and other tracking or monitoring systems	Lack of mental and physical activity by humans leading to health issues.
Beneficial for the healthcare industry	Complex system for maintenance
Improved security in homes and offices	Lack of security
Reduced use of many electronic devices as one device does the job of a lot of other devices	Absence of international standards for better communication

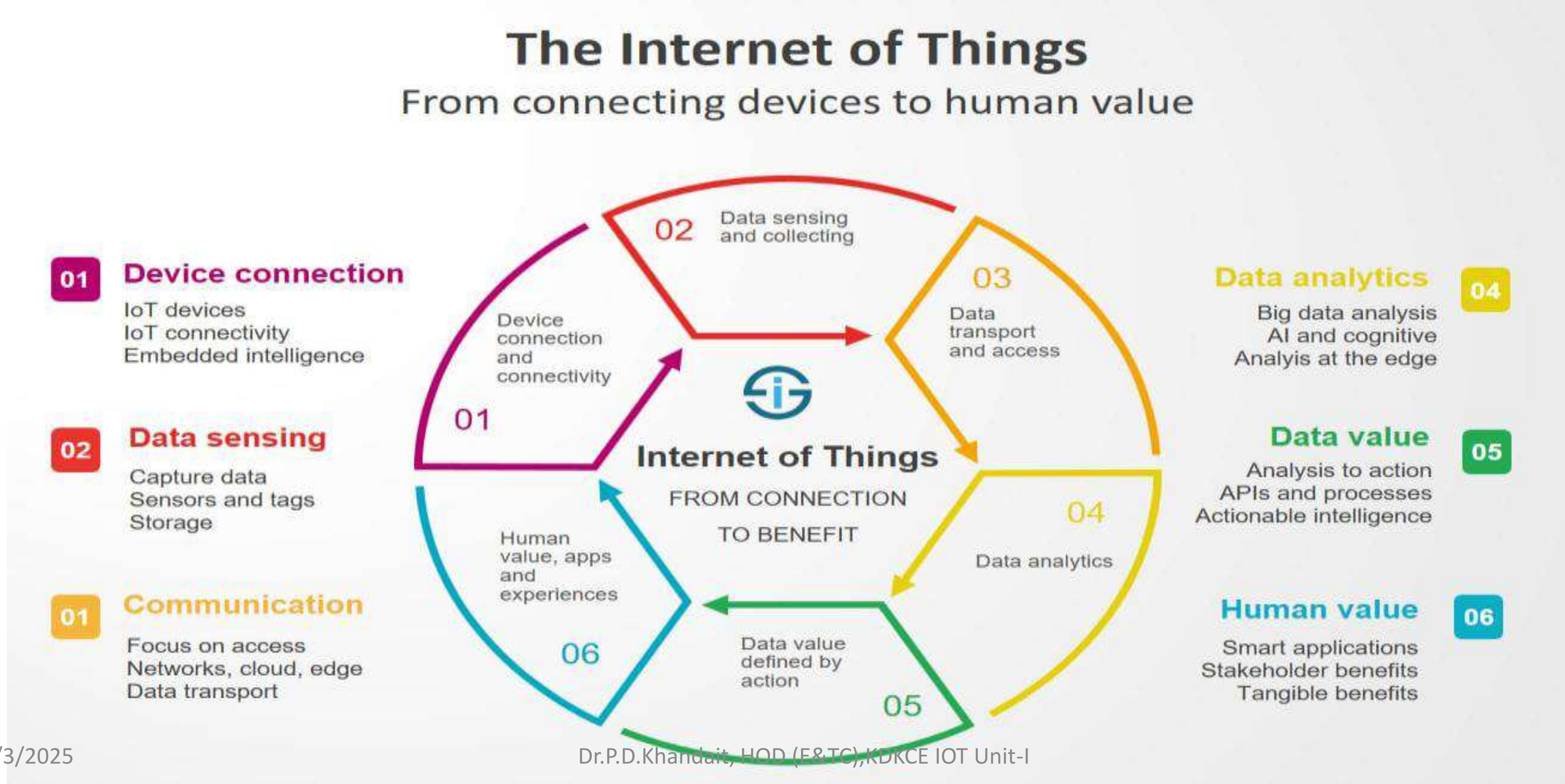
Disadvantages of IoT

- As the Internet of things facilitates advantages, it also creates a significant set of drawbacks. Some of the IoT disadvantages are given below:
- **Security issues:** IoT systems are interconnected and communicate over networks. So, the system offers little control despite any security measures, and it can lead to various kinds of network attacks.
- **Privacy concern:** The IoT system provides critical personal data in full detail without the user's active participation.
- **Increased unemployment:** Unskilled workers or even the skilled ones are at a high risk of losing their jobs, leading to high unemployment rates. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing the humans who would earlier do these works.

Disadvantages of IoT…

- **The complexity of the system:** The designing, developing, maintaining, and enabling the extensive technology to IoT system is quite complicated.
- **High chances of the entire system getting corrupted:** If there is a bug in the system, it is possible that every connected device will become corrupted.
- **Lack of international standardizations:** As there is no international standard of compatibility for IoT, it is problematic for devices from different manufacturers to communicate with each other.
- **High dependency on the internet:** They rely heavily on the internet and cannot function effectively without it.
- **Reduced mental and physical activity:** Overuse of the internet and technology makes people ignorant because they rely on smart devices instead of doing physical work, causing them to become lethargic and inactive.

In general; all complete IoT systems are the same in that they represent the integration of four distinct components: sensors/devices, connectivity, data processing, and a user interface.



Applications of IOT

- Before going to read about IoT applications , just watch this reference video- https://youtu.be/91aXs9E0qAI

- The applications of Internet of Things span a wide range of domains including (but not limited to)…

- Homes, cities, environment, energy systems, retail, logistics, industry, agriculture and health as listed in Figure 1.2.

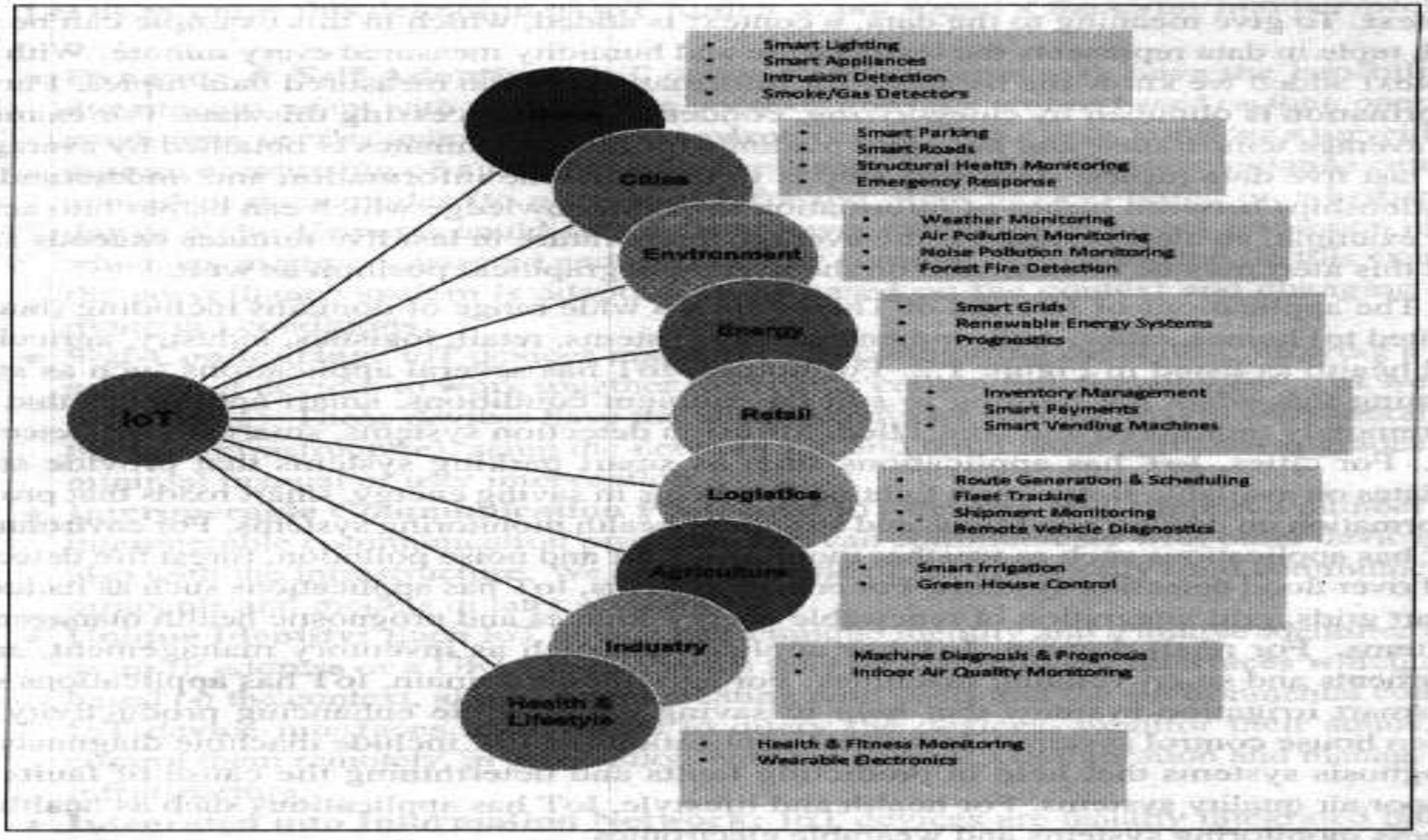


Figure 1.2: Applications of IoT

Applications of IOT…..

- For homes, IoT has several applications such as smart lighting that adapt the lighting to suit the ambient conditions, smart appliances that can be remotely monitored and controlled, intrusion detection systems, smart smoke detectors, etc.
- For cities, IoT has applications such as smart parking systems that provide status updates on available slots, smart lighting that helps in saving energy, smart roads that provide information on driving conditions and structural health monitoring systems.

Applications of IOT.....

- For environment, IoT has applications such as weather monitoring, air and noise pollution, forest fire detection and river flood detection systems.
- For energy systems, IoT has applications such as including smart grids, grid integration of renewable energy sources and prognostic health management systems.
- For retail domain, IoT has applications such as inventory management, smart payments and smart vending machines.

Applications of IOT…..

- For agriculture domain, loT has applications such as smart irrigation systems that help in saving water while enhancing productivity and green house control systems.
- Industrial applications of loT include machine diagnosis and prognosis systems that help in predicting faults and determining the cause of faults and indoor air quality systems.
- For health and lifestyle, loT has applications such as health and fitness monitoring systems and wearable electronics.

Physical Design of IoT

- Things of IoT
- The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, Actuating and monitoring capabilities.
- IoT devices can exchange data with other connected devices and applications (directly or indirectly), or collect data from other devices and process the data locally or send the data to Centralized servers or cloud based applications back ends for processing the data or from some task locally and other task within the IoT infrastructure, based on temporal and space constraints (ie : Memory, processing calibrators, communication latencies and speed and deadlines).

Things of IoT ……

- An IoT device may consist of several interfaces connections to other devices, both wired and wireless. See fig 1.3.
- These include

I)IoT interfaces for sensors

II) interfaces for internet connectivity

III) memory and storage interfaces

IV) audio video interfaces.

- An IoT Device can collect various types of data from the onboard or attached sensors, such as temperature , humidity, light intensity.

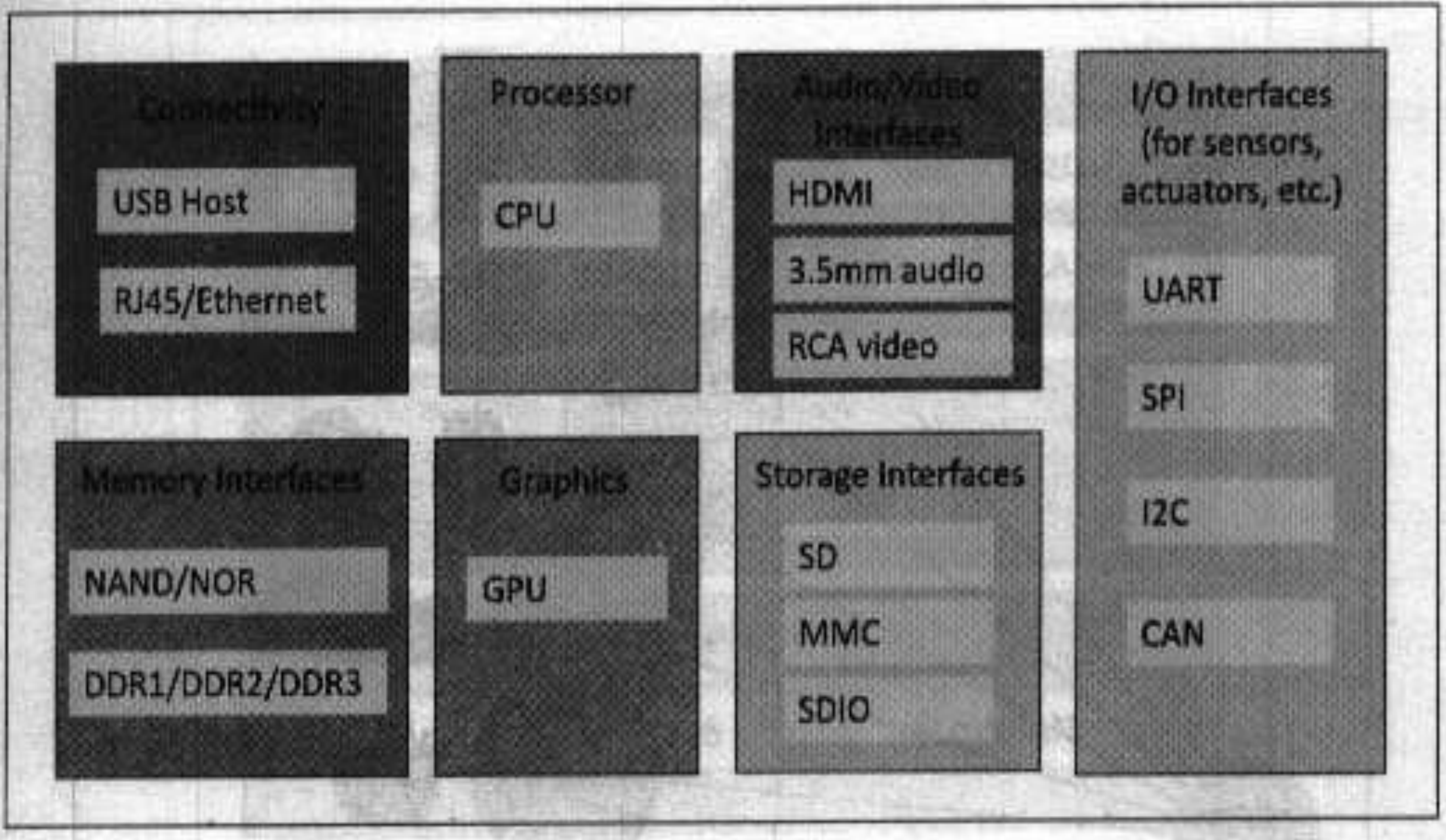


Figure 1.3: Generic block diagram of an IoT Device

Things of IoT ……

- IoT devices can also be varied types, for instance, wearable sensors, smart watches, LED light automobiles and industrial machines.
- Almost all IoT devices generate data in Some form or the other which when processed by Data Analytics systems leads to Useful information to guide further actions locally or remotely.
- For instance sensor data generated by a soil moisture monitoring device in a Garden when processed can help in determining the optimum watering schedule. Fig.1.4 shows different IoT devices.

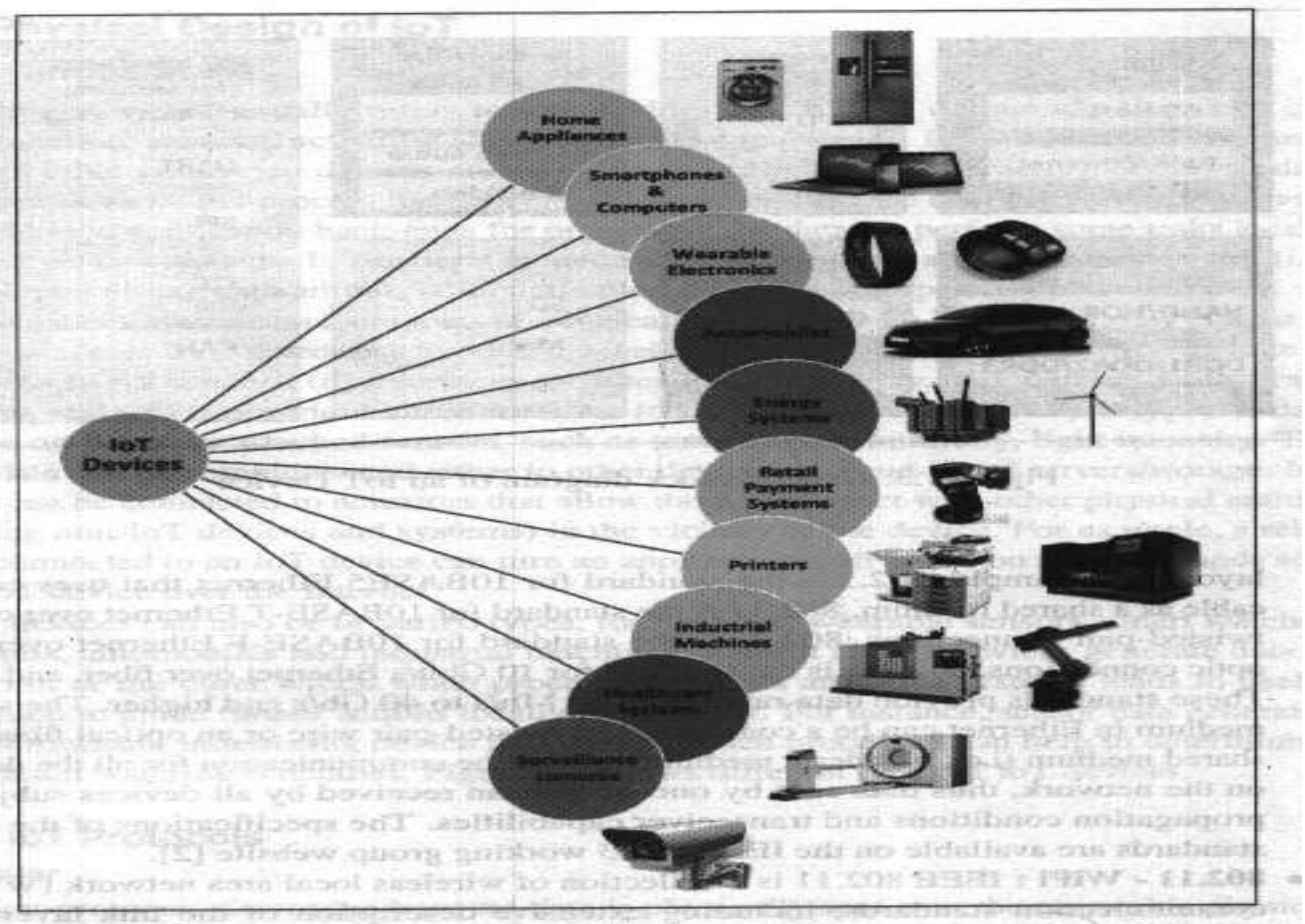


Figure 1.4: IoT Devices

IoT Devices

1. ***Consumer electronics:*** Camcorders, cameras, etc.

2. ***Household appliances:*** Television, DVD players, washing machine, fridge, microwave oven, etc.

3. ***Home automation and security systems:*** Air conditioners, sprinklers, intruder detection alarms, closed circuit television cameras, fire alarms, etc.

4. ***Automotive industry:*** Anti-lock breaking systems (ABS), engine control, ignition systems, automatic navigation systems, etc.

5. ***Telecom:*** Cellular telephones, telephone Switches, handset multimedia applications, etc.

6. ***Computer peripherals:*** Printers, scanners, fax machines, etc.

IoT Devices……

7. ***Computer networking systems:*** Network routers, switches, hubs, firewall etc.

8. ***Healthcare:*** Different kinds of scanners, EEG, ECG machines etc.

9. ***Measurement & Instrumentation:*** Digital multi meters, digital Oscilloscopes, logic analyzers, PLC systems, etc.

10. ***Banking & Retail:*** Automatic teller machines (ATM) and currency counters, point of sales (POS)

11. ***Card Readers:*** Barcode, smart card readers, hand held devices etc.

IoT Protocol

- Link Layer:
- Link Layer protocols determine how the data is physically sent over the network’s physical layer or medium (example copper wire, electrical cable, or radio wave).
- The Scope of The Link Layer is the Local Network connections to which host is attached.
- Host on the same link exchange data packets over the link layer using the link layer protocol.
- Link layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (such as Coaxial Cable).

- 802.3-Ethernet:
- IEEE 802.3 is a collections of wired Ethernet standards for the link layer.
- For example 802.3 is a standard for 10BASE5 Ethernet that uses coaxial cable as a shared medium,
- 802.3.i is standard for 10BASE-T Ethernet over copper twisted pair connection, 802.3.j is standard for 10BASE-F Ethernet over fiber optic connection
- 802.ae is the standard for 10Gbits/s Ethernet over fiber, and so on.
- These standards provides data rate from 10 Mb/s to 40 gigabits per second and the higher.
- The shared medium is Ethernet can be a coaxial cable , twisted pair wire or and Optical fiber. The Shared medium(i.e. broadcast medium) carries the communication for all the devices on the network.

- 802.11- Wi-Fi:

- IEEE 802.11 is a collection of wireless Local area network (WLAN) communication standards, including extensive descriptions of the link layer.
- For example 802.11a operate in the 5 GHz band,
- 802.11b and 802.11g operate in the 2.4 GHz band.
- 802.11n operates in the 2.4/5GHz band.
- 802.11ac operates in the 5GHz band.
- 802.11ad operates in the 60 GHz band.
- These standards provides data rate from 1Mb/s to 6.75Gb/s.

- 802.16-wiMAX:

- IEEE 802.16 is a collection of wireless broadband Standards, including extensive descriptions for the link layer (also called WiMax).

- **WiMax** standard provides a data rates from 1.5 Mb/s to 1Gb/s. The recent update (802.16m) provides data rates of 100Mb/s for mobile stations and 1Gb/s for fixed stations.

- 802.15.4 LR-WPAN:

- IEEE 802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN).These standards form the basis of specifications for high level communication protocols such as Zigbee. LR-WPAN standards provide data rates from 40 kb/s to 250kb/s. These standards provide low cost and low speed Communications for power constrained devices.

- 2G / 3G / 4G- Mobile communications:

- These are different generations of mobile communication standards including second generation (2G including GSM and CDMA),3rd Generation (3G-including UMTS and CDMA2000) and 4th generation (4G- including LTE).
- IoT devices based on these standards can communicate over cellular networks.
- Data rates for these standards range from 9.6kb/s (for 2G) to upto 100Mb/s (for 4G).

- Network / Internet layer :

- The network layers are responsible for sending of IP datagrams from the source network to the destination network.
- This layer Performs the host addressing and packet routing.
- The datagrams contains a source and destination address which are used to route them from the source to the destination across multiple networks.
- Host Identification is done using the hierarchical IP addressing schemes such as IPv4 or IPv6.

- IPv4: Internet protocol version 4(IPv4) is the most deployed internet protocol that is used to identify the devices on a Network using a hierarchical addressing scheme.
- IPv4 uses 32 bit addresses scheme that allows total of 2^32 addresses. As more and more devices got connected to the internet these addresses got exhausted in the year 2011.
- The IPv4 has succeeded by IPv6.

- IPv6: It is the newest versions of internet protocol and successor to IPv4. IPv6 uses 128 bit address schemes that allows total of 2^128 addresses.
- 6LoWPAN: 6LoWPAN (IPv6 over low power wireless personal area networks) brings IP protocol to the low power device which have limited processing capability. It operate in the 2.4 GHz frequency range and provide the data transfer rate off to 250 kb/s.
- 6LoWPAN works with the 802.15.4 link layer protocol and defines compression mechanism for IPv6 datagrams over IEEE 802.15.4 based Network.

- Transport layer :

- The Transport layer protocols provides end-to-end message transfer capability independent of the underlying network. The message transfer capability can be set up on connections, either using handshake (as in TCP) or without handshakes/ acknowledgements (as in UDP). It provides functions such as error control , segmentation, flow control and congestion control.

- TCP: Transmission Control Protocol(TCP) is the most widely used transport layer protocol, that is used by the web browsers (along with HTTP , HTTPS application layer protocols) email program (SMTP application layer protocol) and file transfer (FTP).
- TCP is a connection Oriented and stateful protocol. while IP protocol deals with sending packets, TCP ensures reliable transmissions of packets in order. TCP also provide error detection capability so that duplicate packets can be discarded and lost packets are retransmitted.
- The flow control capability of TCP ensures that the rate at which the sender sends the data is not too high for the receiver to process.

- UDP: unlike TCP, which requires carrying out an initial setup procedure, UDP is a connectionless protocol.

- UDP is useful for time sensitive application that have very small data units to exchange and do not want the overhead of connection setup.

- UDP is a transactions oriented and stateless protocol.

- UDP does not provide guaranteed delivery, ordering of messages and duplicate eliminations.

- Application layer :

- Application layer protocol define how the application interfaces with the lower layer protocols to send the data over the network.
- The Application data are typically in files, is encoded by the application layer protocol and encapsulated in the transport layer protocol .Application layer protocol enable process-to-process connection using ports.
- Port numbers are used for application Addressing (e.g. Port 80 for HTTP, Port 22 for SSH etc)

- HTTP: Hypertext Transfer Protocol (HTTP) is the application layer protocol that forms the foundations of world wide web (WWW). HTTP includes commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS etc. The protocol follows a request-response model where the client sends request to server using the HTTP commands. HTTP is a stateless protocol and each HTTP request is independent of the other requests. An HTTP client can be a browser or an application running on the client (e.g. application running on an IoT device ,the mobile applications or other software.)
- HTTP protocol uses Universal Resource Identifiers (URIs) to identify HTTP resources.

- CoAP: Constrained application protocol is an application layer protocol for machine to machine (M2M) application.
- M2M meant for constrained environment with constrained devices and constrained networks. Like HTTP, CoAP is a web transfer protocol and uses a request- response model, however it runs on the top of the UDP instead of TCP. CoAP uses a client –server architecture where client communicate with server using connectionless datagrams. It is designed to easily interface with HTTP. Like HTTP, CoAP supports method such as GET, PUT, POST & DELETE .

- WebSocket: Websocket protocol allows full duplex communication over a single socket connections for sending message between client and server. WebSocket is based on TCP and Allows streams of messages to be sent back and forth between the client and server while keeping the TCP connection open. The client can be a browser, a mobile application and IoT device

- MQTT :Message Queue Telemetry Transport (MQTT) is a light-weight messaging protocol based on public-subscribe model. MQTT uses a client server Architecture where the clients (such as an IoT device) connect to the server (also called the MQTT broker) and publishes message to topics on the server.
- The broker forward the message to the clients subscribed to topic.
- MQTT is well suited for constrained environments where the devices have limited processing and memory resources and the Network bandwidth is low.

- XMPP: Extensible Messaging and Presence Protocol(XMPP) is a protocol for real-time communication and streaming XML data between network entities.XMPP powers wide range of applications including messaging, presence, data syndication, gaming multiparty chat and voice / voice calls. XMPP Allows sending small chunks of XML data from one network entity to another in near real time. XMPP supports both client to server and server to server communication paths.

- DDS: Data distribution service (DDS) is the data centric middleware standard for device-to-device or machine to machine communication. DDS uses a publish subscribe model where publishers (e.g. device that generate data) create topics to which subscribers(e.g. device that want to consume data) can subscribe. Publisher is an object responsible for data distribution and the subscriber is responsible for receiving published data. DDS provide quality of service (QoS) control and configurable reliability

- AMQP: Advanced Message Queuing protocols (AMQP) is an open application layer protocol for business messaging. AMQP support both point to point and publisher/subscriber models, routing and queuing.
- AMQP broker receive message from publishers (e.g. devices or applications that generate data) and route them over connections to consumers (application that process data) Publishers publish the message to exchanges which then distribute message copies to queues.

Logical design of IoT

- Logical design of an IoT system refers to an abstract representation of the entities and processes without going into low level specifics of the implementations .

- An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation ,communication and Management.

• The functional blocks are---

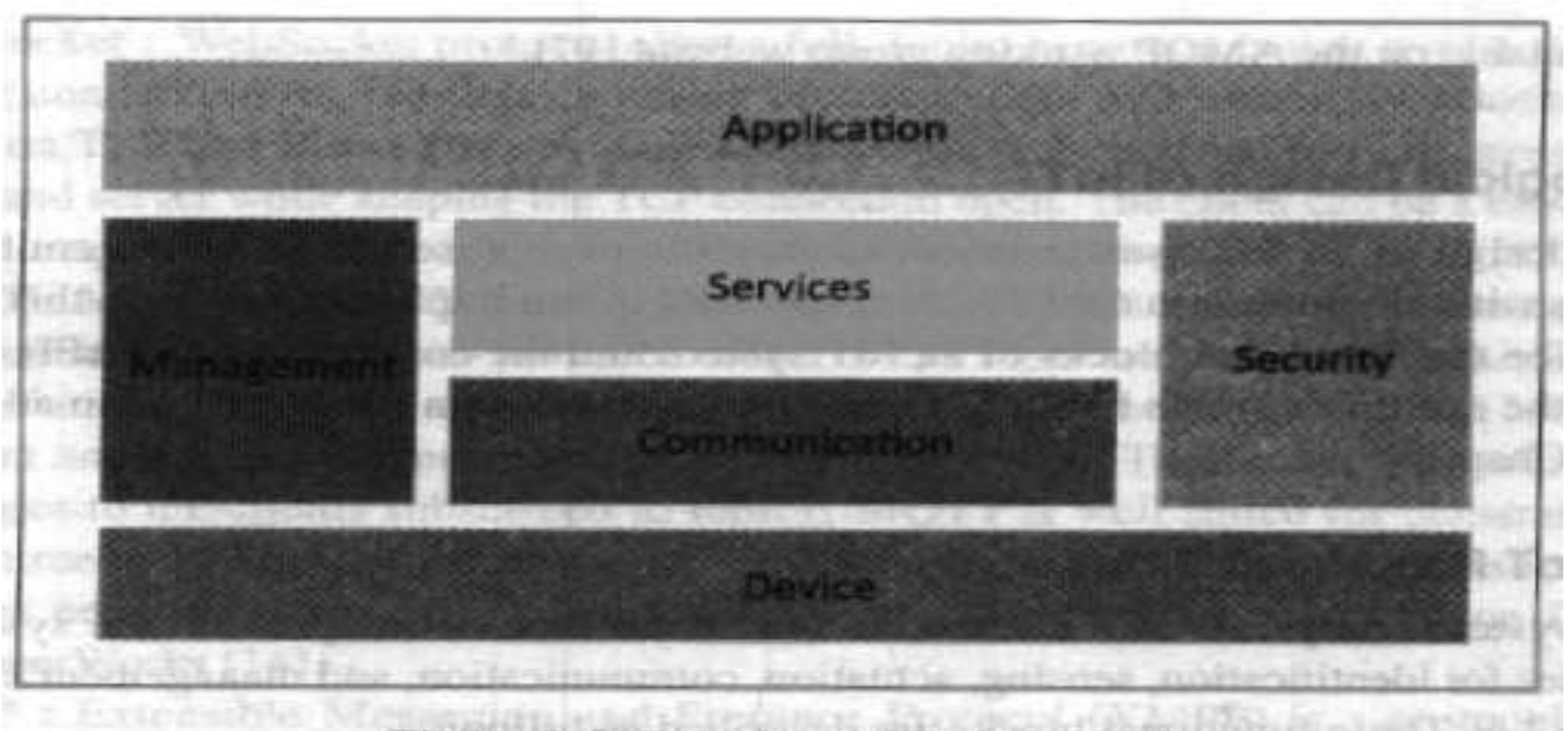


Figure 1.6: Functional Blocks of IoT

• Devices: An IoT system comprises of the devices that provide sensing, actuation, monitoring and control function.

• Communication: Communication block handle the communication for the IoT systems.

IoT functional block ……

- Services : An IoT system uses various types of IoT services such as services for device monitoring ,device control services ,data publishing services and services for device Discovery.
- Management: Management Functional blocks provide various functions to govern the IoT system
- Security: Security functional block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity and data security.

IoT functional block ……

- Application: IoT application provides an interface that the users can use to control and monitor various aspects of the IoT system.
- Application also allow users to view the system status and view or analyze the processed data.

IoT communication models

- Request response model: Request-response is a Communications model in which the client sends request to the server and the server responds to the requests.
- when the server receives a request it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.
- Request-response model is a stateless communication model and each request response pair is independent of others. Figure 1.7 shows the client-server interactions in the request response model.

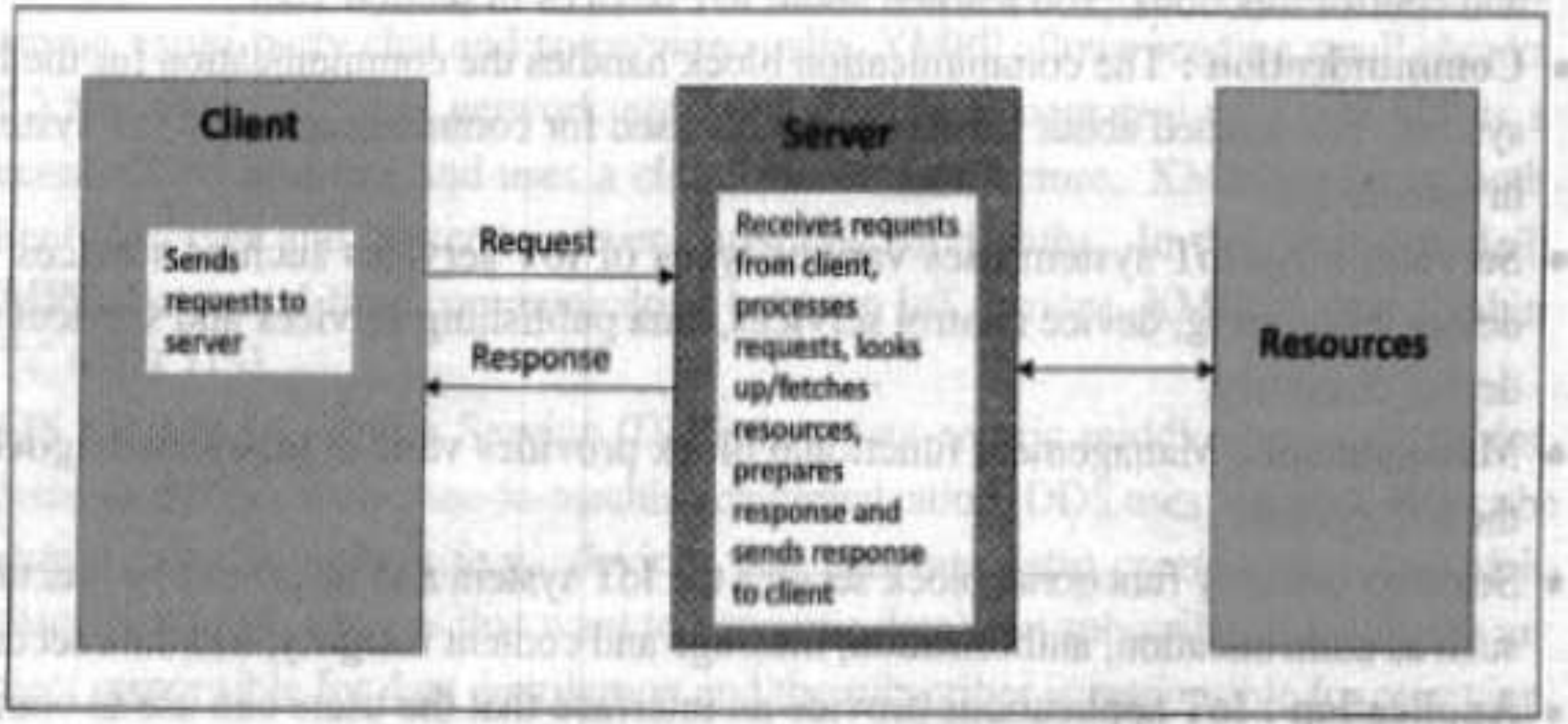


Figure 1.7: Request-Response communication model

IoT communication model …..

- Publish – Subscribe model: Publish-Subscribe is a communication model that involve publishers, brokers and consumers.
- Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumer.
- Consumers Subscribe to the topics which are managed by the broker. When the broker receives the data for a topic from the publisher, it sends the data to all the subscribed consumers. See fig 1.8 for this model.

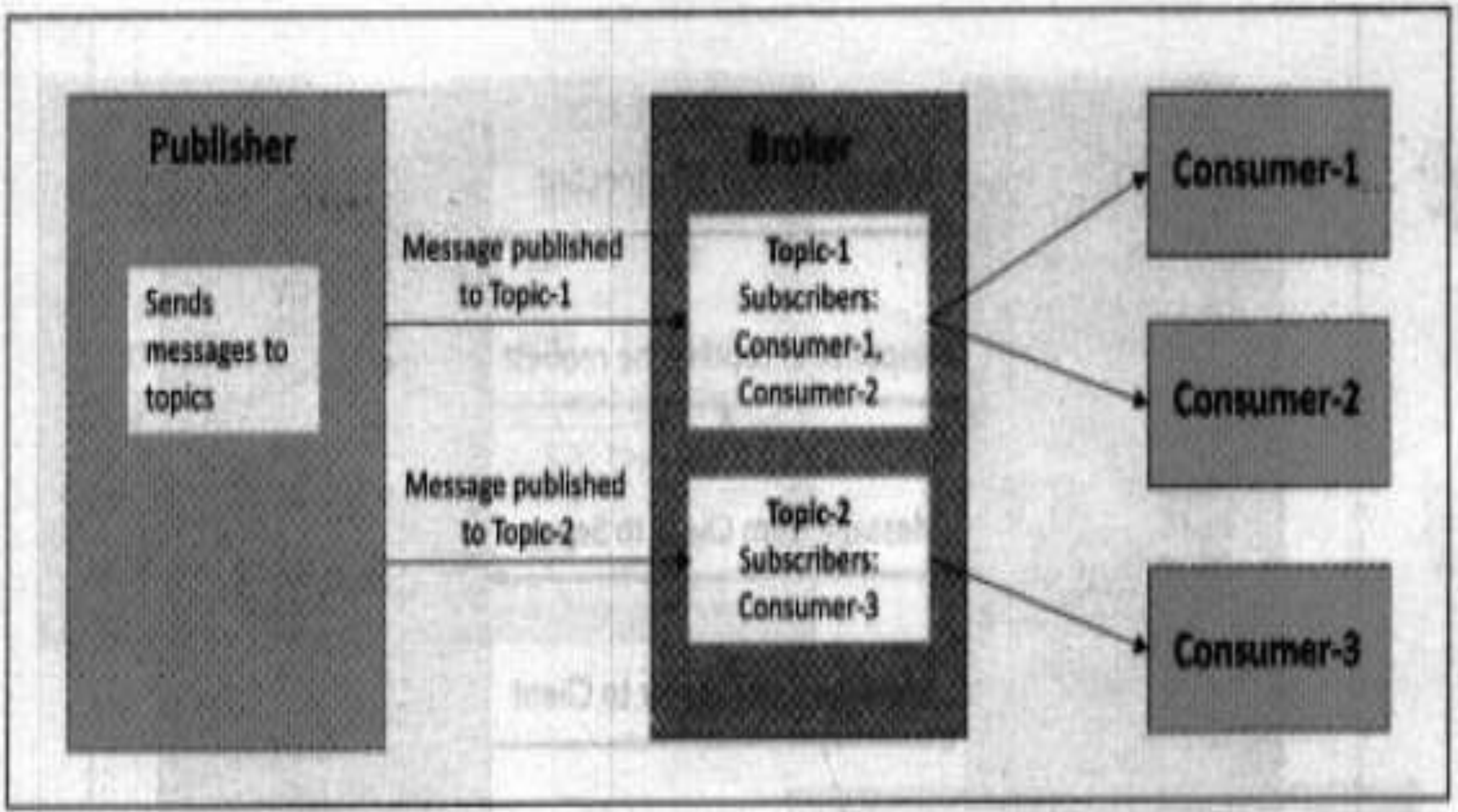


Figure 1.8: Publish-Subscribe communication model

IoT communication model .....

- Push pull model: Push pull is communication model in which the data producers push the data to queues and the consumers pull the data from the queues.
- Producers do not need to be aware of the consumer.
- Queues help in decoupling the messaging between the Producers and Consumers .
- Queues also acts as a buffer which helps in situations when there is a mismatch between the rate at which the produces push data and the rate at which the consumers pull the data. See fig 1.9 for the model.

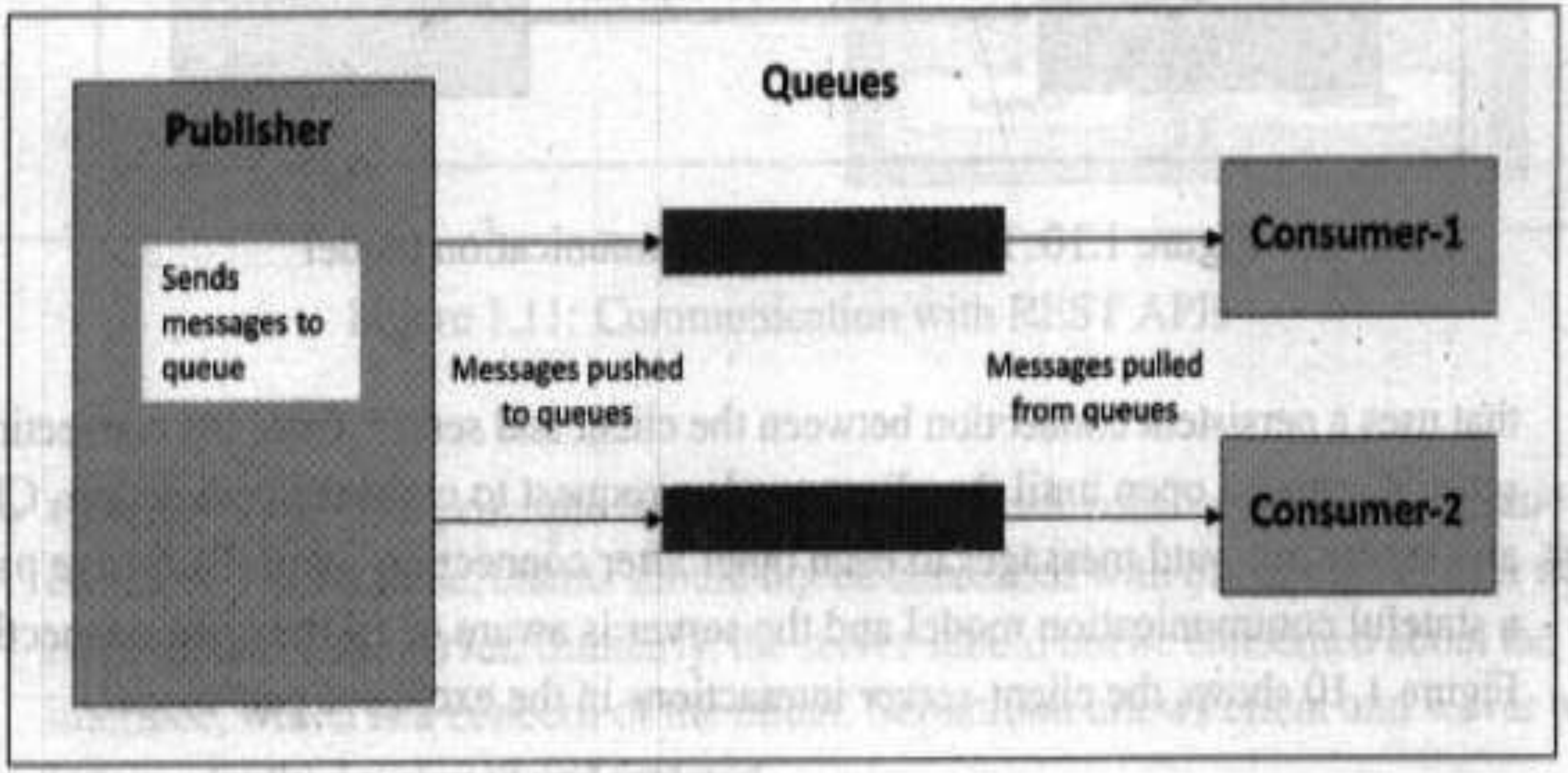


Figure 1.9: Push-Pull communication model

IoT communication model .....

- Exclusive pair: Exclusive pair is a bi directional, fully duplex communication model that uses a persistent connections between the client and the server.
- Once the connection is setup it remains open until the client sends a request to close the connection.
- Client and server can send messages to each other after connection setup. Exclusive pair is a stateful Communication model and the server is aware of all the open connections. See fig 1.10 for the model

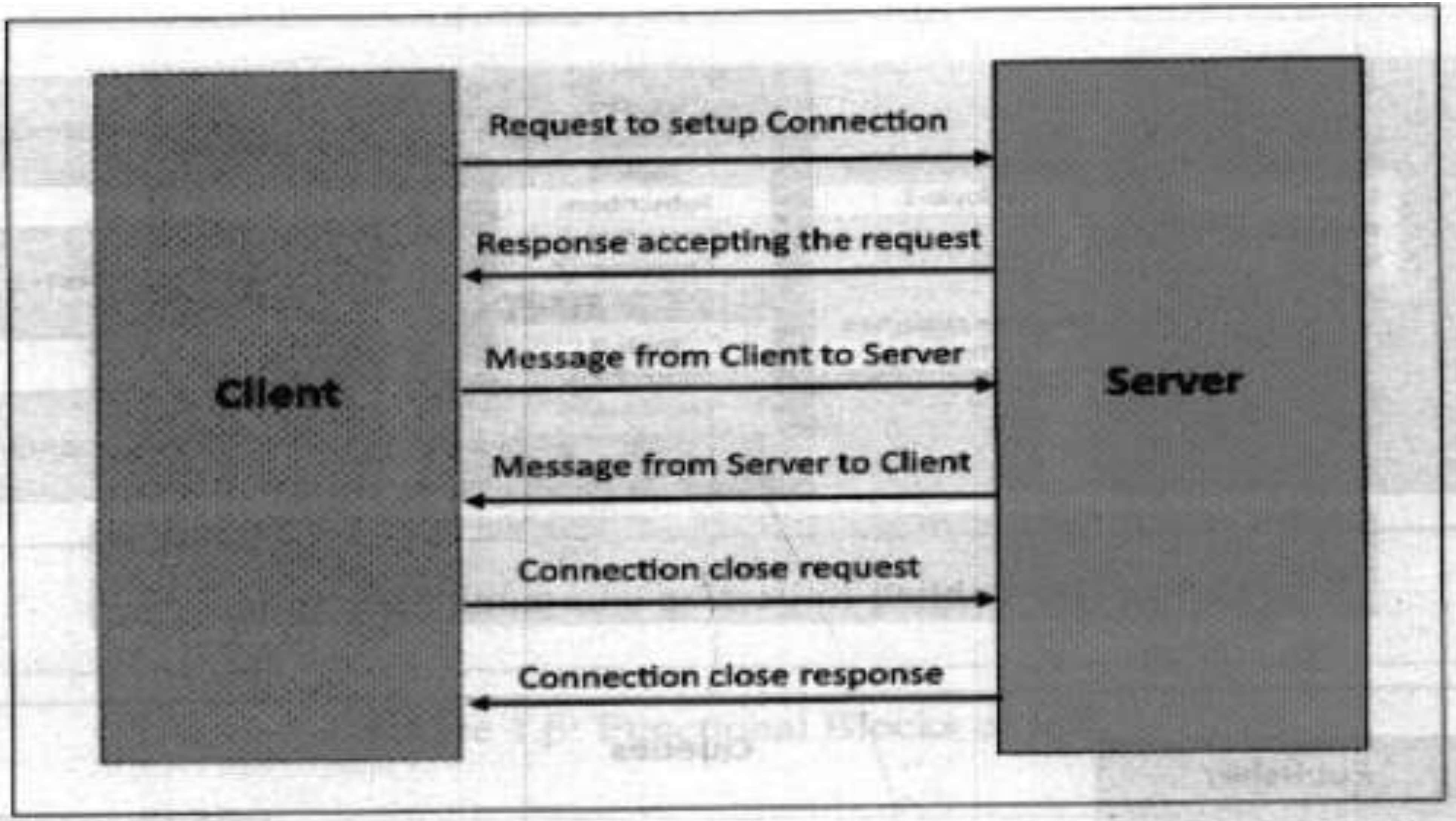


Figure 1.10: Exclusive Pair communication model

IoT communication Application Programming Interfaces (APIs)

- REST- based communication API:
- Representational state transfer (REST) is a set of architectural principles by which you can design web service and Web API that focus on a system’s resources and how resources states are addressed and transferred. REST API follow the request- response communication model.
- The REST architectural constraints apply to the components, connectors, and data elements within a distributed hypermedia systems

REST architectural constraints

- Client server:
- The principle behind the client-server constraint is separation of concerns. For example, client should not be concerned with the storage of data which is a concern of the server.
- Similarly the server should not be concerned about the user interface which is a concern of the client.
- separation allows client and server to be independently developed and updated.

IoT communication APIs ….

- Stateless: Each request from client to server must contain all the information necessary to understand the request , and cannot take advantage of any stored context on the server . The session state is kept entirely on the client.

- Catch-able: Catch constraint requires that the data within the response to a request be implicitly or explicitly labeled as catch-able or non-catch-able. If a response is catch-able then a client cache is given the right to reuse that response data for later, equivalent requests. Catching can partially or completely eliminate some attractions and improve efficiency and scalability.

IoT communication APIs ….

- Layered system:
- Layered System constraint, constrains the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting.
- For example client cannot tell whether it is connected directly to the end server or to an intermediary along the way.
- System scalability can be improved by allowing intermediaries to respond to request instead of the end server, without the client having to do anything different.

IoT communication APIs ….

- Uniform interface:
- Uniform interface constraints requires that the method of communication between client and server must be uniform.
- Resources are identified in the request (by URIs in the Web based System) and are themselves separate from the representation of the resources that are returned to the client.
- When client holds a representation of a resource it has all the information required to update or delete the resource (provided the client has required permissions).
- Each message includes enough information to describe how to process the message.

IoT communication APIs ….

- Code on demand : Servers can provide executable code or scripts for clients to execute in their context.
- This is the only optional constraint

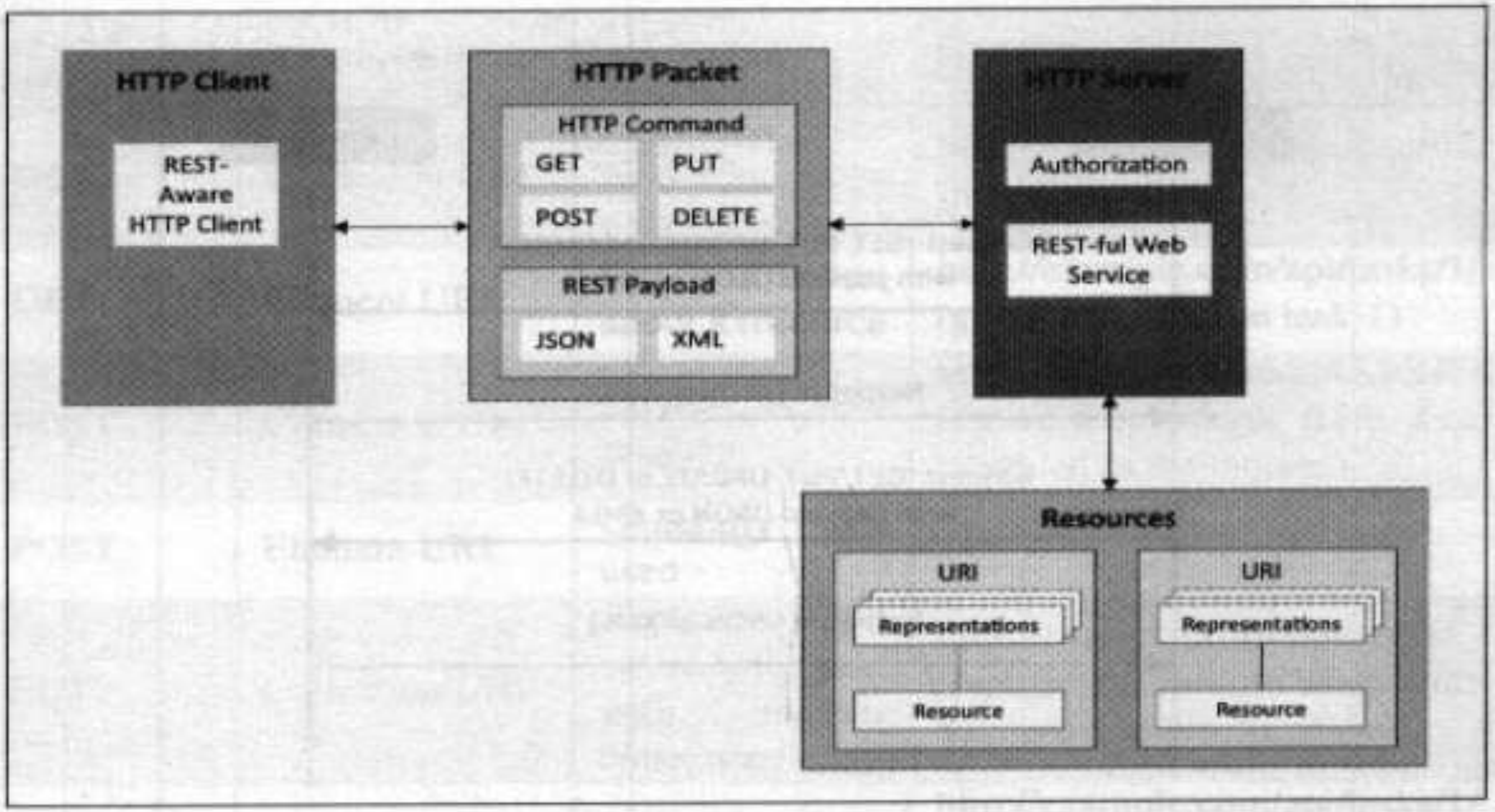


Figure 1.11: Communication with REST APIs

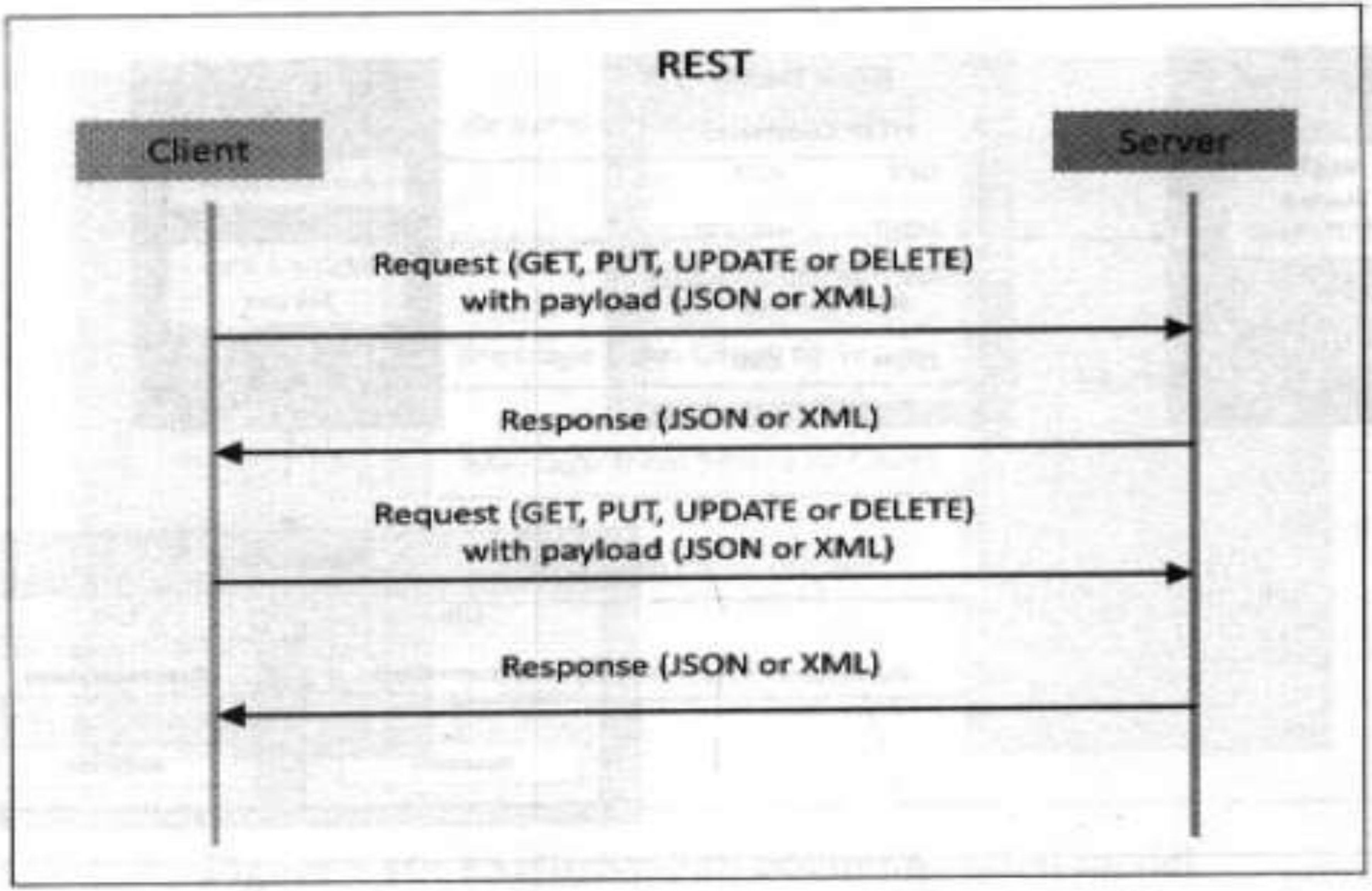


Figure 1.12: Request-response model used by REST

HTTP Method	Resource Type	Action	Example
GET	Collection URI	List all the resources in a collection	http://example.com/api/tasks/ (list all tasks)
GET	Element URI	Get information about a resource	http://example.com/api/tasks/1/ (get information on task-1)
POST	Collection URI	Create a new resource	http://example.com/api/tasks/ (create a new task from data provided in the request)
POST	Element URI	Generally not used	
PUT	Collection URI	Replace the entire collection with another collection	http://example.com/api/tasks/ (replace entire collection with data provided in the request)
PUT	Element URI	Update a resource	http://example.com/api/tasks/1/ (update task-1 with data provided in the request)
DELETE	Collection URI	Delete the entire collection	http://example.com/api/tasks/ (delete all tasks)
DELETE	Element URI	Delete a resource	http://example.com/api/tasks/1/ (delete task-1)

Table 1.1: HTTP request methods and actions

WebSocket based communication API:

- WebSocket API allow bi directional, full duplex communication between client and servers. WebSocket API follows exclusive pair communication model.
- Unlike request-response APIs such as REST, the WebSocket APIs allow full duplex communication and do not require new connection to be set up for each message to be sent.
- WebSocket communication begins with connection setup request send by the client to the server. This request (called as WebSocket handshake) is sent over HTTP and the server interprets it as an upgrade request.

WebSocket based communication API….

- If the server supports WebSocket Protocol, the server responds to the WebSocket handshake response. After the connection is setup the client and the server can send data/messages to each other in full duplex mode.
- WebSocket API reduce network traffic and latency as there is no overhead for connection setup and termination requests for each message.
- WebSocket is suitable for IoT applications that have low latency or high throughput requirements

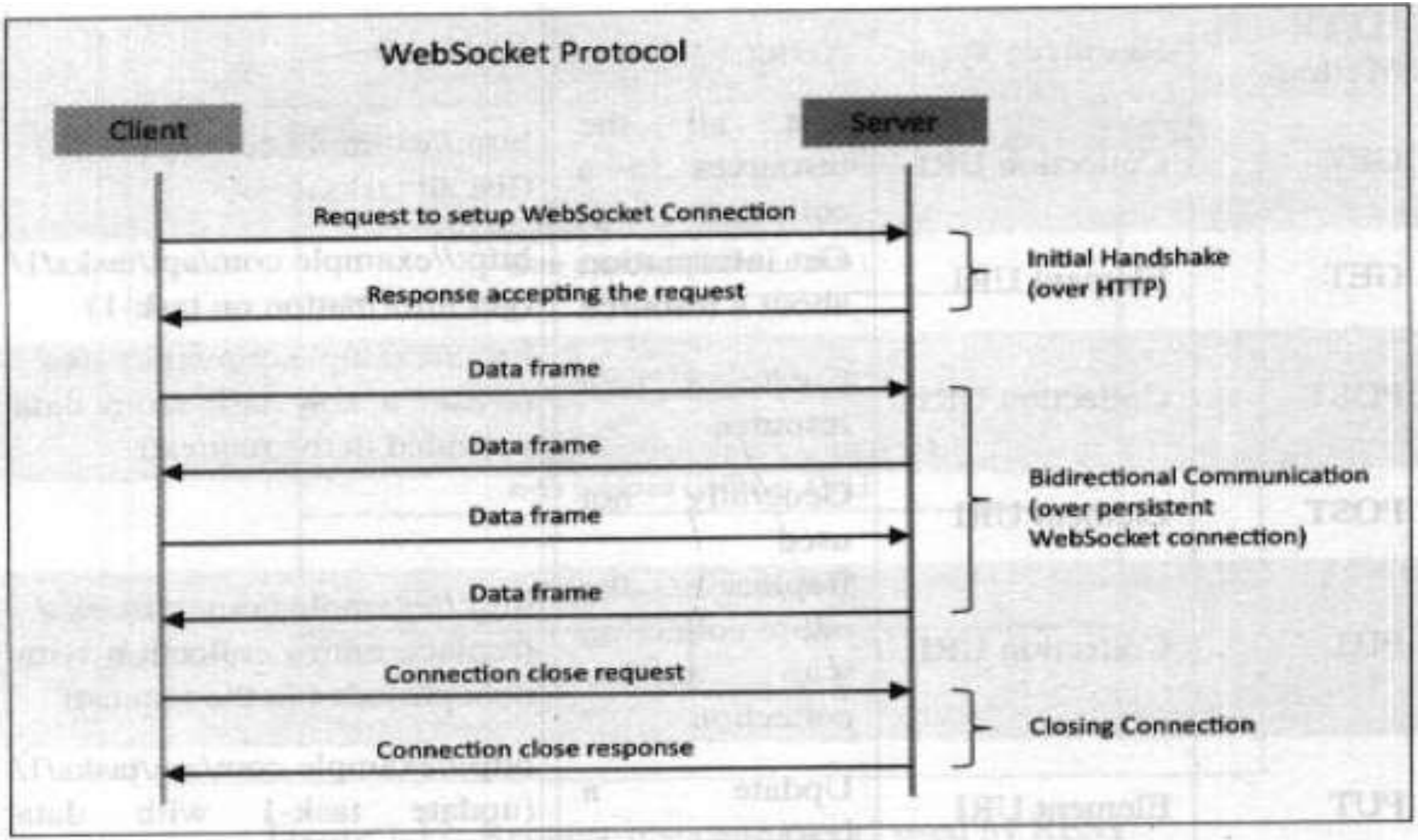


Figure 1.13: Exclusive pair model used by WebSocket APIs

IoT enabling Technologies

- It is enabled by several Technologies including wireless sensor networks, cloud computing, big Data Analytics, embedded system, security protocols and architectures, communication protocols, web service, mobile internet and semantic search engine .

wireless sensor network

- Wireless sensor network (WSN) comprise of distributed devices with the sensor which are used to monitor the environmental and physical conditions.
- A WSN consists of a number of end nodes and routers and a coordinator.
- End nodes have several sensors attached to them. End node can also act as a routers.
- Routers are responsible for routing the data packet from end nodes to the coordinator.
- The coordinator node collect the data from all the nodes.
- Coordinator also act as a Gateway that connects the WSN to the internet.

Examples of IoT systems with WSN….

- Weather monitoring systems use WSN in which the nodes collect temperature, humidity and other data which is aggregated and analyzed .
- Indoor air quality monitoring systems use WSN to collect data on the indoor air quality and concentration of various gases.
- Soil moisture monitoring systems use WSN to monitor soil moisture at various location.
- Surveillance systems use WSN for collecting surveillance data(such as motion detection data)
- Smart grid use wireless sensor network for monitoring the grid at various point.
- Structural health monitoring systems use WSN to monitor the health of structure (buildings , bridges) by collecting vibration data from sensor nodes deployed at various points in the structure.

WSNs are enabled by wireless communication protocols such as IEEE 802.15.4. ZigBee is one of the most popular wireless technologies used by WSNs. ZigBee specifications are based on IEEE 802.15.4. ZigBee operates at 2.4 GHz frequency and offers data rates upto 250 KB/s and range from 10 to 100 meters depending on the power output and environmental conditions. The power of WSNs lies in their ability to deploy large number of low-cost and low-power sensing nodes for continuous monitoring of environmental and physical conditions. WSNs are self-organizing networks. Since WSNs have large number of nodes, manual configuration for each node is not possible. The self-organizing capability of WSN makes the network robust. In the event of failure of some nodes or addition of new nodes to the network, the network can reconfigure itself.

Cloud computing:

- Cloud Computing is a transformative computing paradigm that involves delivering applications and services over the internet.
- Cloud Computing involves provisioning of computing networking and storage resources on demand and providing these resources as metered services to the users, in a " pay as you go" model.
- cloud Computing resources can be provisioned on demand by the user without requiring interactions with the Cloud Service Provider.
- The process of provisioning resources used automatic Cloud Computing resources can be accessed then it worked using standard access mechanism that provide platform-independent access through the use of heterogeneous client platforms such as workstations laptops tablets and Smartphones the computing and storage resources provided by Cloud Service Provider our food to serve multiple user using multi Tenancy. Multi-tenant aspects on the multiple users to be served by the same physical hardware .
- Cloud Computing services are offered to user in different forms like IaaS, PaaS, SaaS

Infrastructure as a service(IaaS) :

- IaaS provides the user the ability to provision computing and storage resources.
- These resources are provided to the users as virtual machine instances and virtual storage.
- Users can start, stop configure and manage the virtual machines instance on the virtual storage. Users can deploy operating systems and applications of their choice on the actual resources provisioned in the cloud .
- Cloud Service Provider manages the underlying infrastructure.
- Virtual resources provisioned by the users are billed based on a pay-per-user paradigm.

Platform as a service(PaaS) :

- Platform as a service provides the user the ability to develop and deploy application in the cloud using the development tools, application programming interfaces (APIs), software libraries and services provided by the Cloud Service Provider.
- The Cloud Service Provider manages the underlying cloud infrastructure including servers, network, operating systems and storage .
- The users themselves are responsible for developing, deploying, configuring and managing applications on the cloud infrastructure.

Software as a service(SaaS) :

- SaaS Provides the user a complete software applications or the user interface to the application itself .
- The Cloud Service Provider manage the underlying cloud infrastructure including servers, network, operating systems, storage and application software, and the user is unaware of the underlying architecture of the cloud.
- Applications are provided to the user through a thin client interface (for example Browser). SaaS applications are platform independent and can be accessed from various client devices such as workstations,laptop,tablet and smartphones, running different operating systems.
- Since the cloud service provider manages both the application and data, the users are able to access the applications from anywhere.

Big Data Analytics

- Big data is defined as collections of data set whose volume, velocity in terms of its temporal variations or variety, is so large that it is difficult to store, manage, process and analyze the data using traditional database and data processing tools.
- Big Data Analytics involving several steps starting from Data cleaning, data munging, data processing and visualization.

Examples of big data generated by IoT systems …

1. Sensor data generated by IoT system such as weather monitoring stations
2. Machine sensor data collected from sensor embedded in Industrial and energy system for monitoring their files and protecting failure
3. Health and fitness data generated by IoT devices such as wearable fitness band.
4. Data generated by IoT system for Location tracking of vehicle.
5. Data generated by retail inventory monitoring system.

Characteristics of data (VVV):

- Volume: Through there is no fixed threshold for volume of data to be considered as big data, however the term big data is used for massive scale data that is difficult to store, manage and process using traditional data bases and data processing architecture. The
- volume of data generated by modern IT, industrial and Healthcare systems for example is a growing exponentially driven by the lowering cost of data storage and processing architectures and the need to extract valuable insights from the data to improve business processes, efficiency and services to consumer.

Characteristics of data…

- Velocity: Velocity is another important characteristics of big data and the primary reasons for exponential growth of data velocity of the data of a store how fast the data is generated and how frequently it varies. Modern IT Industrial and other systems are generating data at increasing the highest speeds.
- Variety: Variety refers to the forms of the data. Big data comes in for different forms such as structured or unstructured data including text data, audio, video and sensor data .

Communications protocol:

- Communications protocols form the backbone of IoT system and enable network connectivity and coupling to applications.
- Communications protocols allow device to exchange data over the network.
- These protocols define the data exchange formats and data encoding schemes for devices and routing of packets from source to destination.
- Other function of the protocol include sequence control flow control and transmissions of Lost packet.

Embedded systems

- An Embedded system is computer system that has computer hardware and software embedded perform specific task.
- In contrast to general purpose computers or personal computers which can perform various types of tasks, embedded systems are designed to perform a specific set of tasks.
- Embedded system include Microprocessor and Microcontroller, memory (RAM, ROM, cache), networking units (Ethernet WI-FI adaptor), input/output unit, display keyboard , display and storage such as Flash Memory.
- some embedded system have specialist processes such as digital signal processor (DSP), graphic processor and application.

IoT levels and Deployment Templates

- IoT level 1:
- Level One IoT system has a single node / device that performs sensing and/or actuation, stores data, reforms analysis and the host to the application.
- Level 1 IoT systems are suitable for modeling low cost and low complexity solutions where the data involving is not big and the analysis requirements are not computationally intensive.

Level 1 IoT system (e.g. Home automation)

- This system consists of the single node that allows controlling the lights and appliances in your home remotely .
- The device used in this system interface with their lights and appliances using electronic relay switches.
- The status information of each light or appliance is maintained in a local database.
- REST service deployed locally; Allow retrieving and updating the state of the each light or appliances in the status database.

Home automation…

- The controller service continuously monitor the state of each light or appliance and triggers the relay switches accordingly.
- The applications which is deployed locally has a user interface for controlling the lights or appliances.
- Since the device is connected to the internet, the application can be accessed remotely as well.

IoT level 2:

- Level 2 IoT system has a single node that performs sensing and/or actuation and local analysis.
- Data is stored in the cloud and application is usually cloud based systems are suitable for solutions where the data in world is big, however the primary analysis requirement is not computationally intensive and can be done local itself.
- Example of Level 2 IoT system: e.g. smart irrigation.

Smart irrigation.

- The system consists of the single node that monitor the soil moisture level and control segregation system.
- The device used in this system collect soil moisture data from sensor the controller service continuously monitor the moisture level.
- If the moister level drops below a threshold t , the irrigation system is turned on.
- For controlling the irrigation system actuators such as solenoid valve can be used.
- REST Web Services is used for storing and retrieving data which is stored in the cloud database.
- A cloud based application is used for visualizing the moisture level over a period of time, which can help in making decisions about irrigation schedules.

IoT Level 3:

- Level 3 system has a single node .
- Data is stored and analyzed in the cloud application is cloud-based.
- Level 3 IoT system is suitable for solutions where the data involved is big and analysis requirements computationally intensive.
- Example of Level 3 IoT system say tracking package handling.

Tracking package handling

- The system consists of a single node that monitors the vibration level for package being shipped.
- The device in the system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller service send sensor data to the cloud in real time using a website service. The data is stored in the cloud and also visualized using a cloud based application.
- The analysis component in the cloud can Trigger alert the vibration level become greater than threshold. The benefit of using websocket service instead of the REST service this example the sensor data can be sent in real-time to the cloud.
- Cloud based application can subscribe to the sensor data feeds for you in the real-time data.

IoT level 4

- A level 4 IoT system has multiple nodes that perform local analysis.
- Data is stored in the cloud and 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.
- Observer node can process information and use it for various applications, however observer nodes do not perform any control function.
- 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.

Noise Monitoring

- Let us consider an example of level four IoT system for Noise Monitoring.
- The system consists of multiple nodes placed in different locations for monitoring noise level in an area. In this example with sound sensor. Nodes are independent of each other each node runs in one controller service that sends the data to the cloud.
- The data is stored in a cloud database the analysis of the data collected from a number of nodes is done in the cloud

IoT Level 5:

- IoT system has multiple end nodes and one coordinator node and nodes that perform sensing and / or actuation.
- Coordinator node collects data from the entry and send to the cloud. Data is stored and analyzed in the cloud and applications is cloud based.
- Level 5 IoT system are suitable for forest fire detection. The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and carbon dioxide levels in a forest.

Forest fire detection

- The endnodes in this example are equipped with various sensors such as temperature humidity and to CO2.
- The coordinator node collects the data from the end nodes and act as a Gateway that provides internet connectivity to the IoT system.
- The controller service on the coordinator device sends the collected data to the cloud .
- The data is stored in the cloud database. The analysis of the data is done in the computing cloud to aggregate the data and make prediction.

IoT Level 6:

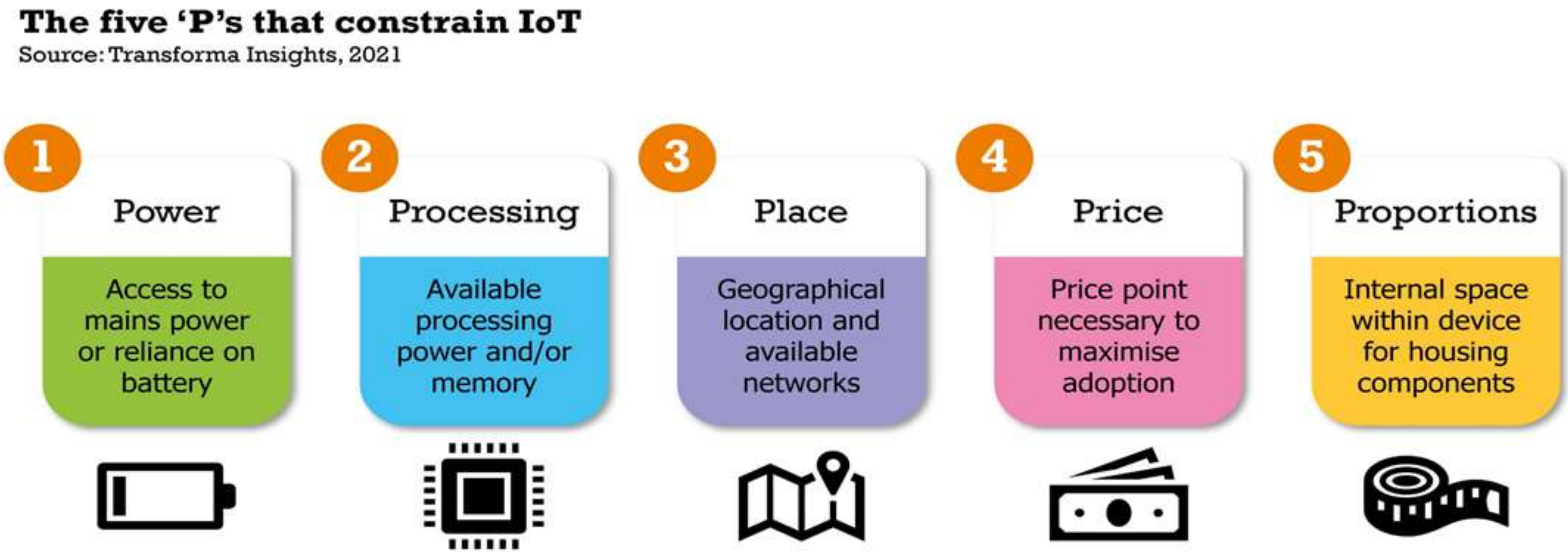
- IoT Level 6 system has multiple Independent end nodes that perform sensing and / or actuations and send data to the cloud.
- Data is stored in the cloud and applications is cloud based .
- The analytics component analyze the data and store the results in the cloud database.
- The results are visualized with the cloud based application. The centralized controller is aware of the status of all the end nodes and send control commands to the nodes.

Weather monitoring

- Consider an example of level 6 IoT system for weather monitoring.
- The system consists of multiple nodes placed in different location for monitoring temperature, humidity and pressure in an area.
- The end nodes are equipped with various sensors such as temperature ,pressure and humidity.
- The end nodes send the data to the cloud in real time using a websocket service .
- The data is stored in a cloud database.
- The analysis of the data is done in the cloud to aggregate the data and make predictions.
- A cloud based applications is used for visualizing the data.

Constraints affecting design in IoT

- These constraints consist of what we term the 5 ‘P’s of IoT: power, processing, place, price and proportions, as illustrated in the image below.



Constraints affecting design in IoT…

The 5 'P's

- **Power**

- Specifically the access to mains power, is a key determinant of how an IoT application is architected.
- The **use of battery power necessitates numerous compromises** in terms of connectivity technology used, communications protocols, processing and more.
- All of those choices have implications for the power usage and require some sort of trade off.
- According to ’ **analysis of real world IoT deployments**, over one-quarter of enterprise IoT deployments today are reliant on battery power, and with the increasing prevalence of LPWA technologies, the ability of enterprises to deploy applications where there is no mains power will only increase.
- By 2030 it’s easily possible that 50% of enterprise IoT deployments will be heavily or exclusively based on battery-powered devices.

Constraints affecting design in IoT…

- **Processing**
- This includes all of the semiconductor capabilities on the device including CPU and memory. This is expensive.
- Moore's law has obviously helped to reduce that cost, assisted by hardware techniques such as system on a chip (SoC) and chip on board (CoB) which have helped to reduce the cost for the same grade of equipment.
- The latest development in the field is ARM's PlasticARM solution. On the software side, a raft of embedded operating systems including Amazon FreeRTOS, RIOT, TinyOS and Zephyr have come available with very small footprints, giving greater capability on processing constrained devices.

Constraints affecting design in IoT…

- **Place**
- Where the device is located is a constraint when it limits access to specific networks (and power) and/or the ability of people to access the device.
- Geographically remote devices may have very limited options of how to be connected, often being limited to technologies that are low bandwidth or costly, or both.
- This might create a strong impetus for increasing processing on the device, using machine learning to automate local decision making.This helps to minimise what traffic needs to be sent.
- This limitation also has strong implications for, for instance, which networking protocols might be used, favouring less chatty ones such as MQTT-SN.
- Furthermore, being in a remote location can also limit the ability of people to make changes to the device manually (necessitating remote management).

Constraints affecting design in IoT…

- **Price**

- Always going to be consideration and a limitation on what a developer can do with an IoT device. There are almost no applications that are completely price insensitive, meaning there is always an incentive to keep prices low.
- The link between price reduction and adoption is not linear; a halving of the cost of putting a device into the field, whether that be connectivity or hardware costs, will likely mean much more than double the sales.
- As an example, disposable devices might be viable at a high price point for tracking high value assets such as pharmaceuticals or precious metals, but the volumes of those devices will be tiny.
- Cut the price by 90% and it becomes viable for millions of much lower value assets. Cut it by 99% and the sky's the limit.

Constraints affecting design in IoT…

- **Proportions**
- This relates to the dimensions of the device and the inherent limitations that come from that.
- A monitoring device attached to a piece of industrial equipment can probably be of any size, within reason (although will probably need some consideration of ruggedisation to cope with vibrations, dust, heat and cold).
- A smart watch, in contrast, has a very strict set of dimensions it needs to keep to. This has implications particularly for trading off against other of the 5 ‘P’s, particularly price: smaller components tend to be more expensive.

All the constraints interact

- In truth any given constraint is likely to be a combination of, or involve the interaction of, several of these.
- For instance, devices that need to rely on low bandwidth networks may need additional capabilities for pre-processing the data on-device.
- Similarly, with unlimited funds most of the other challenges can be resolved, for instance through very small components or the use of expensive network technologies.
- All of these need to be traded off when deciding on the best combination of technologies and device specifications to use.