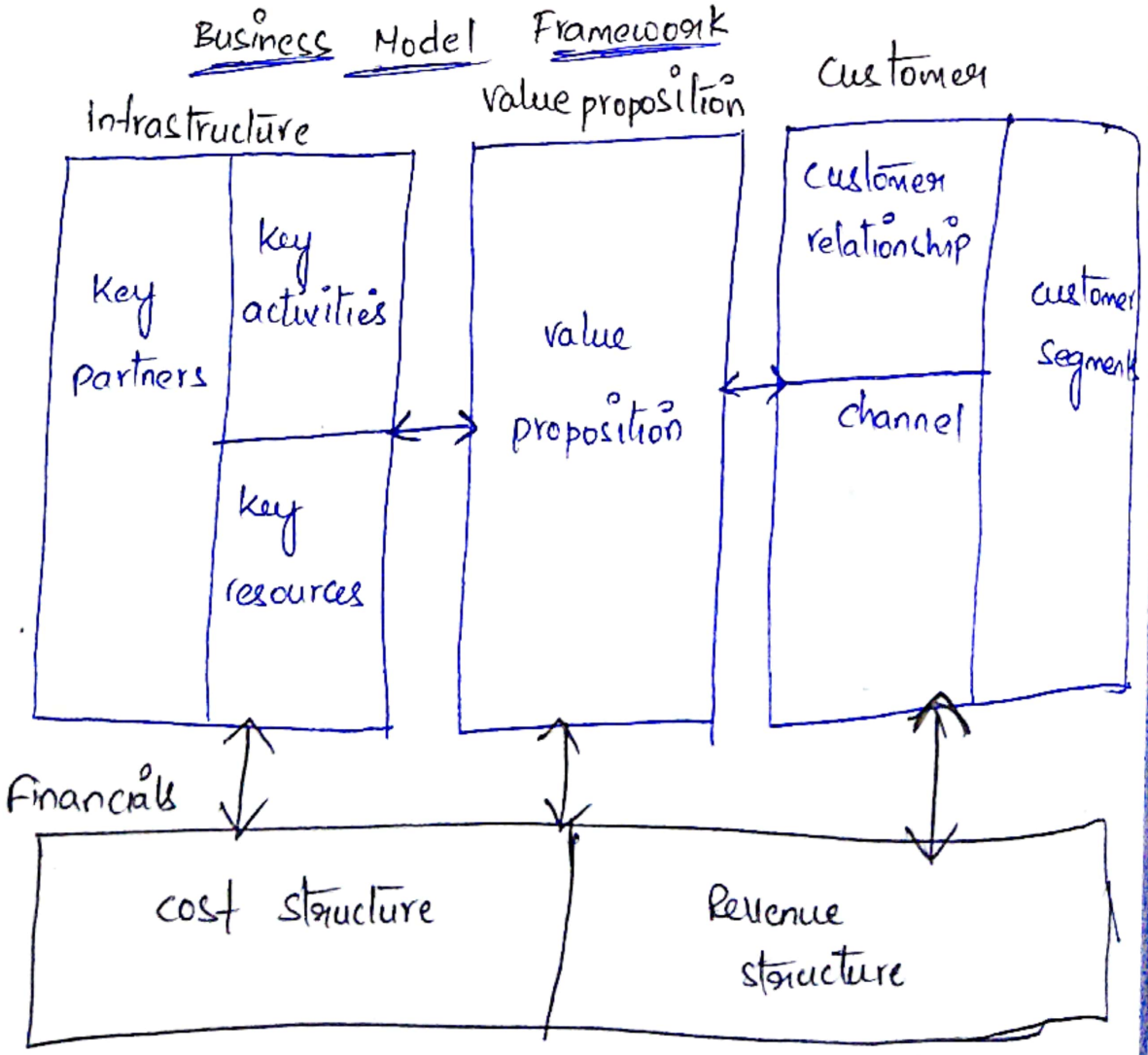
unit-II:- Syllabus

Business Models for business processes in internet of things, IOT/M2M systems, Layers and design Standardlizations. Modified OSI stack for the IOT/M2M systems, ETSI M2M domains and high level capabilities, Communication technologies, Data Enrichment and consolidation and device management gateway ease of designing and affordability.

1) Business Models for Business processes in internet of things:-



A plan for the successful operation of a business, identifying sources of revenue, the intended customer base, products and details of financing. Types of models are:—

i) subscription model:—

→ Data generated by IoT devices is "consumable, measureable and repeatable."

→ It is capable of generating "recurring" revenue.

→ using this model:

i) Instead of one-time charge, customers are offered a regular subscription.

ii) Here, a fee is charged for periodic usage.

→ provides predictable, recurring revenue.

→ Businesses are able to foster active relationships with customers due to repeated post-subscription interaction.

ii) outcome-based Model:—

→ Businesses deliver to the customers the outcome/benefits that the product/service provides - "pay-per-outcome."

→ customer is relieved from the responsibilities of ownership and maintenance.

→ It brings together the businesses and their customers to monetize the solutions

iii) Asset-sharing Model:—

→ Businesses virtually consolidate and share their IoT enabled assets among multiple customers or with other business entities in exchange of revenue.
→ Revenue is charged based on time or nature of usage.
→ Aim is to minimize downtime and maximize utilization of the assets.
→ can be used for Smart energy.

iv) platform-based business Model:—
→ It combines manufacturers and consumers in the marketplace to benefit both.
→ The key to it interoperability and inter connection of the devices and the business to generate revenue from related transcations.

v) Asset-tracking Model:—
→ This business model can also track the supply chain to identify inefficiencies, optimize workflows and increase visibility into usage.
→ Connected devices in the supply chain help businesses identify, monitor and track assets in real-time.

vi) service-adjacent model:—
→ Your business offers a service that enhances the use of the IoT device, but doesn't necessarily sell the device itself. The device is the enabler of your service, not the main point of your business.

vii) Data-driven model:—

→ This model works well if you have many devices out in the field collecting data and if you've notified customers that you're using their data for this.

→ It is powered by the data generated by your devices.

Business processes in IoT:—

→ Business processes refers to a series of activities, often a collection of interrelated processes in a logical sequence within an enterprise, leading to specific result.

→ There are several types of business processes such as management, operational and supporting all of which aim at achieving a specific mission objective.

→ In the M2M era, connected devices can be clearly identified and with the help of services, this integration leads to active participation of the devices to the business processes.

→ A Business processes Model provides graphical notation.

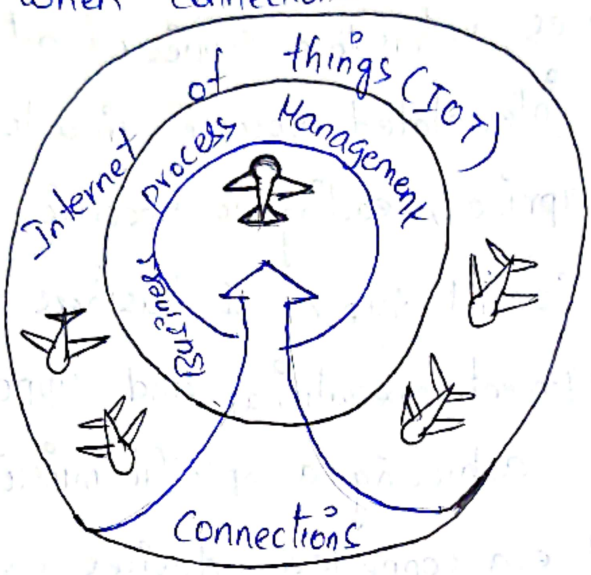
→ A business process model is the representation of business process.

→ Each business process is enacted by a single organization, but it may be interact with business processed performed by other organizations.

→ It is a vital component of any device that has IoT Connectivity.

→ Its role in terms of the IoT is to determine what is to be done with data received from other devices.

→ The added benefit is that because it is data driven, it provides a wealth of data about what, where and when connections are made and for what purpose.



2) IOT/M2M system layers and design standardlization:

→ Designing a communication framework for connecting devices, for their local area networking and provisions for data gathering.

→ Designing a data enrichment, data consolidation and data transformation framework.

→ Designing gateway components for connecting the device's network with the web/Internet.

→ Need of application and applications-support frameworks for services, applications and processes.

Design standardizations:-

→ Internet Engineering Task force (IETF), an international body initiated actions for addressing and working on the recommendations for the engineering specifications for the Internet of things.

→ IETF suggests the specifications for the layers, and the engineering aspects for the IoT communication, networks and applications.

Design standards:-

1) ITU-T 2) ETSI 3) OGC.

① International Telecommunication Union for telecommunication (ITU-T) suggested a reference model for IoT domain, network and transport capabilities for the IoT services and the applications at the application and application-support layers.

② European Telecommunication standards Institute (ETSI) initiated the development of a set of standards for the network, and devices and gateway domains for the communication between Machines (M2M). ETSI proposed high level architecture for applications and service capabilities.

③ open geospatial consortium, an international industry consortium, has also suggested open standards

for sensors, discovery, capabilities, quality and others aspects with support to geographical information web support;

3) Modified OSI stack for the IoT/M2M systems:-

→ The modifications are proposed by IETF.

→ Each layer proposes the received data and creates a new data stack which transfers it to the next layer.

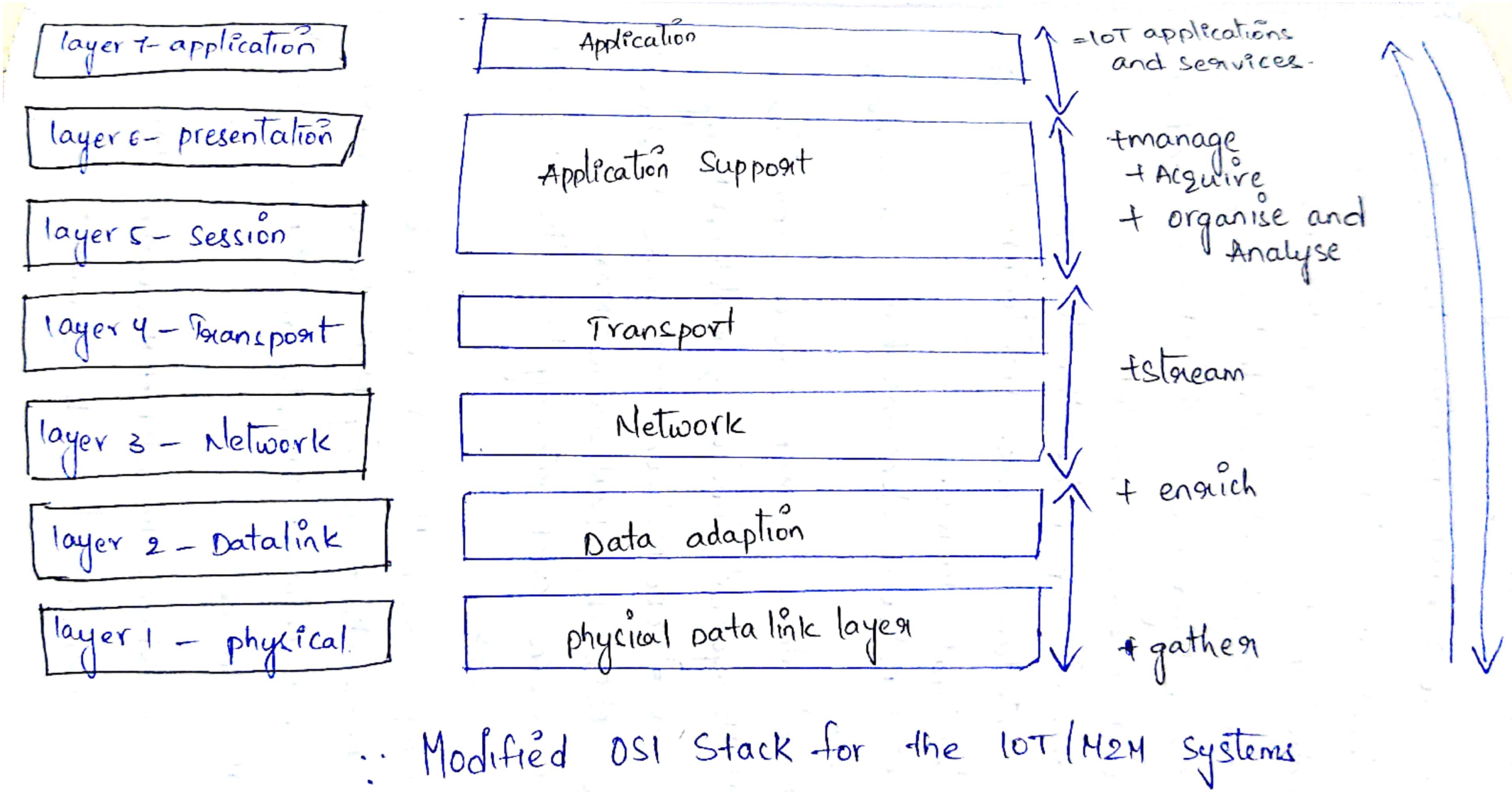
→ The processing takes place at the intermediate layers between the functional layer to the top layer.

→ Device end also receives the data from the application/service after processing.

→ This shows a similarity to the operation of the equation 2 w.r.t Conceptual framework as given below:

Gather & enrich & stream & Manage & Acquire & organise & analyse = IoT with connectivity to Datacenter, Enterprise or cloud..

Diagram:-



∴ Modified OSI Stack for the IoT/M2M systems

4) ETSI M2M Domains and high level capabilities:-

→ Like ITU-T, ETSI specifies the functional areas for a high-level architecture and reference model for communicating the data from IOT / M2M devices.

→ It also depicts the architectural correspondance with the 6-layer modified OSI model and 4 layers of ITU-T Reference model.

→ A domain specifies the functional areas. high-level architecture means architecture for functional and structural views.

→ The ETSI network domains has 6 capabilites & functions.

(i) M2M applications ; (ii) M2M service capabilities (iii) M2M Management functions ; (iv) Network Management Functions ; (v) CORE Network ex: 3G and IP Networks; (vi) Access Network, WLAN and Wi-MAX.

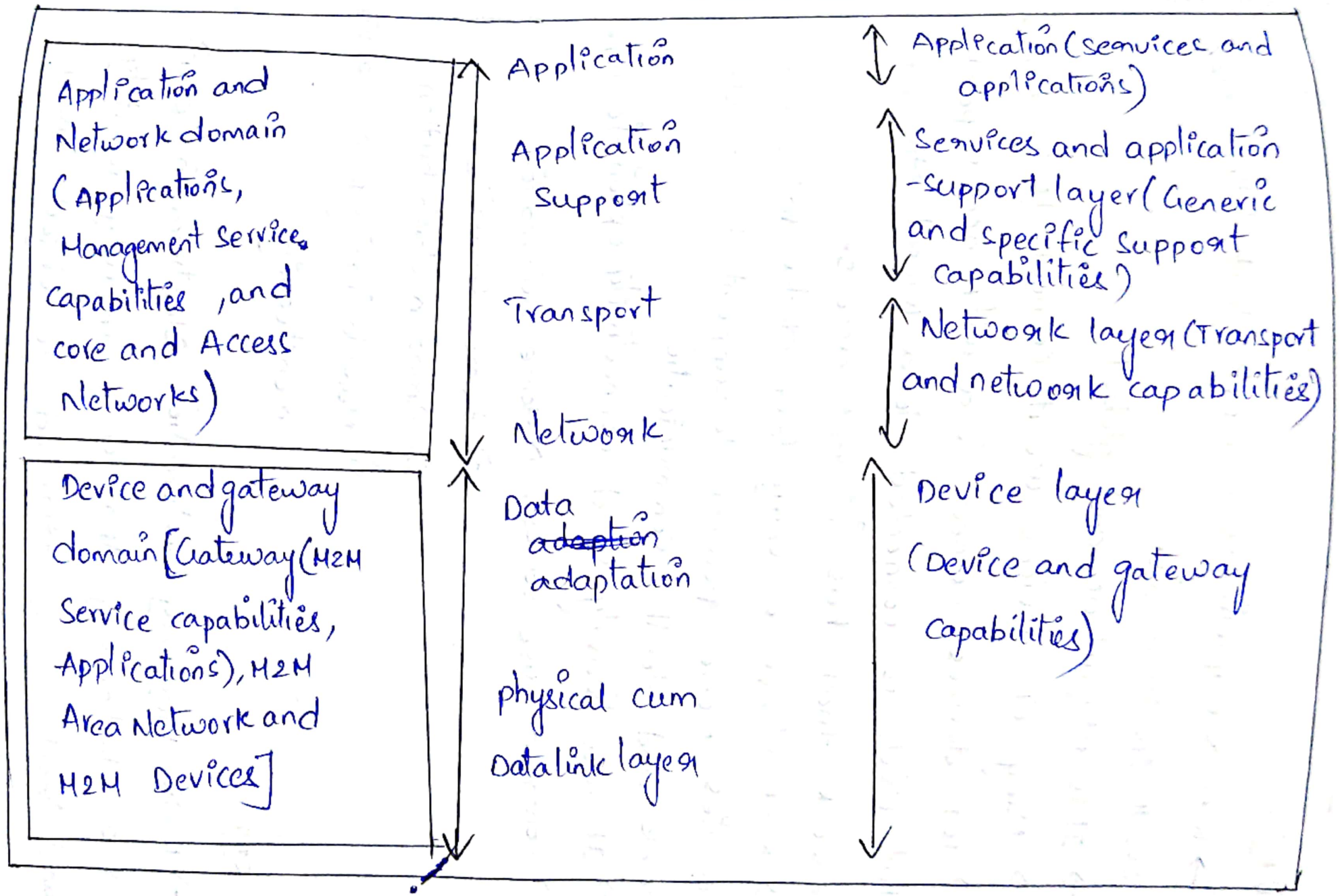
→ ETSI device and gateway have the following functional units:

(i) Gateway between M2M area network, CORE and access network, processing M2M service capabilities.

(ii) M2M area network (Bluetooth, zigBee, NFC, PAN)

(iii) M2M Devices.

Diagram:- It shows the ETSI M2M domains and high level capabilities of each domain.



... ETSI M2M Domains and high level capabilities.

5) Communication Technologies:-

i) wifi:-

→ wifi is any wireless network that follows IEEE 802.11 specifications.

→ It is ubiquitous and global

→ Many IoT devices use it Connect to the network.

→ IoT devices connect to a wifi access point that itself is connected to a wired ethernet network that has internet access.

→ wifi offers a very fast data rates but requires more power to support the constant back and forth communication.

→ It is a heavily used connectivity option for IoT.

→ Common use cases: 1) Home automation
2) Home security
3) Amazon dash button
4) Manufacturing plant machine monitoring.

ii) RFID:-

→ Radio Freguency ~~automation~~ identification (RFID) is a technology that can uniguely identify and track tags attached to objects using radio-frequency electromagnetic waves.

→ A RFID system typically includes a tag, a reader and an antenna.

→ RFID tags can be either active or passive. Active RFID tags have their own power source and therefore can be read over a long range (up to 100 meters). passive RFID tags do not have their own power source. They are powered by the electromagnetic energy transmitted from the RFID reader. Therefore, they can only be read over a short distance (<25m).

→ RFID can be used in variety of applications:

1) Access management
2) Tracking of goods
3) Timing sporting events
4) Tracking and billing processes.

iii) Bluetooth :—

→ As a well established short range connectivity technology, Bluetooth is considered to be the key solution.

→ with cost-effectiveness and reduced power consumption in mind, the bluetooth-low-energy (BLE) protocol requires very little power from the

device.

→ Yet, this comes with a compromise: when transferring frequently higher amounts of data, BLE may not be the most effective solution.

→ It was designed for low power needs and a less frequent data exchange rate.

→ There is typically a gateway device that is both part of the bluetooth network and also linked to the internet.

(iv) Zig Bee:-

→ It covers multiple layers of the protocol stack

→ It is the network protocol, the Transport layer, and an application framework that is the underpinnings of a customer developed application layer.

→ The range is short, upto 100 meters line of sight, but it can travel long distances by passing data through a mesh network of other zigBee devices.

→ Data rates are low and devices tends to be simple.

→ The data transmission is periodic and intermittent.

-> A fully functioning device can act as a
i) network co-ordinator and operates in both
star and mesh topologies.
ii) A reduced functionality device only communicates
with a network co-ordinator and works in a
star topology.

6) Data enrichment and consolidation gateway:—

Gateway includes the following functions:—

1) Transcoding
2) privacy, Security
3) Integration
4) Compaction and fusion.

① Transcoding:—

→ It means data adaption, conversion and change of protocol, format or code using software.

→ The gateway renders the web response the web and messages in formats and representations required and acceptable at an IoT device.

Ex:- Conversion from ASCII to unicode at the Server.

② privacy, security:- The data such as medical records, logistics, and inventories of a company may need privacy and protection. The following are the components of privacy model.

i) Devices and applications identity-Management
ii) Authenication
iii) Authorization
iv) Trust
v) Reputation

Secure data access:- Access to data needs to be Secured. End to End ~~protocol~~ security is a feature which uses a Security protocol at each layer.

③ Data gathering and Snrichment:-

It refers to data acquisition from the devices/devices network. Four models are:

polling:- Data Sought from a device by addressing.

Event-based gathering:- Data Sought from a device on event.

Scheduled interval:- Data Sought from a device at select intervals.

Continous monitoring:- Data Sought from a device continously.

④ Data enrichment/Data dissemination (compaction and fusion)

It refers to adding value, security and usability of the data. Three steps for data enrichment.

① Aggregation:— process of joining together present and previous received data frames after removing redundant or duplicate data.

② compaction:— making information short without changing the meaning or context.

③ fusion:— formatting the information received in parts.

→ Energy efficient computations can be made use of by using the concepts of data aggregations, compaction and fusion.

⑦ Device Management gateway:—

→ Device Management means provisioning for the devices ID or address which is distinct from other resources, device activating, configuring, registering, deregistering, attaching and detaching.

→ DM also means accepting subscription for its resources.

→ Open Mobile Alliance (OMA) - DM and several Standard are used for device Management.

1→ Gateway functions for Device Management are:

i) Does forwarding function when DM server and device can interact without reformatting (or) structuring.

ii) Does protocol conversion when the device and DM server use distinct protocols.

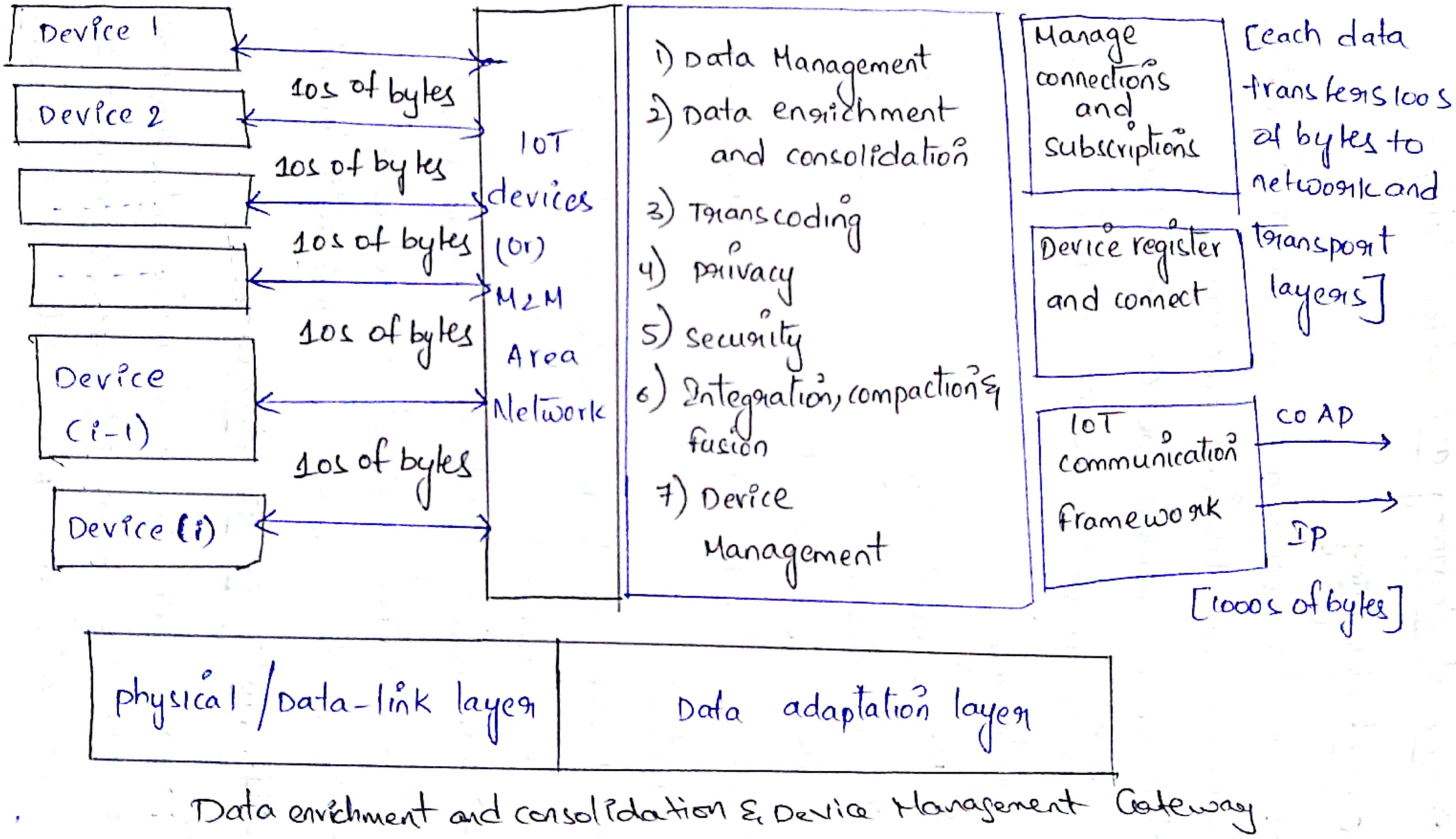
iii) Does proxy function in case an intermediate pre-fetch is required in a lossy environment.

Diagram:-

The diagram shows gateway consisting of data enrichment and consolidation, device management of IOT/M2M.

→ Functions of gateway at data-adaption layer are

1) Data privacy
2) Data Security
3) Data enrichment
4) Data consolidation, transformation
5) Device Management.


Device 1
Device 2
Device (i-1)
Device (i)
10s of bytes
10s of bytes
10s of bytes
10s of bytes
IOT devices (or) M2M Area Network
1) Data Management
2) Data enrichment and consolidation
3) Transcoding
4) Privacy
5) Security
6) Integration, compaction & fusion
7) Device Management
Manage connections and subscriptions
Device register and connect
IOT communication Framework
CoAP
IP
[each data transfers 100s of bytes to network and transport layers]
[1000s of bytes]
physical / Data-link layer
Data adaptation layer
Data enrichment and consolidation & Device Management Gateway

8) Ease of designing and affordability:-

Ease of designing:-

→ Design for connected devices for IoT Applications, services and business processors.

→ Designer considers the ease in designing the devices physical, data link, adaption layers and gateway.

→ Means availability of sensors, actuators, controllers and IoT devices.

→ low in cost and hardware.

→ use preferably open source components and protocols.

→ Device hardware should embed minimum of components.

→ use ready solutions for ease in designing local devices personal area network.

→ Ensure the secure connectivity with the Internet.

Affordability of IoT devices:-

The card: An embedded micro controller, memory, OS, NFC peripheral interfaces, access point based device activation, RF module and transreceiver

and all that at low cost.

→ for example, wireless sensors use Mote (mobile terminal)

→ Mote: low cost devices with open source os (tiny os) and software components.

→ provides ease and affordance in the WSN networks;