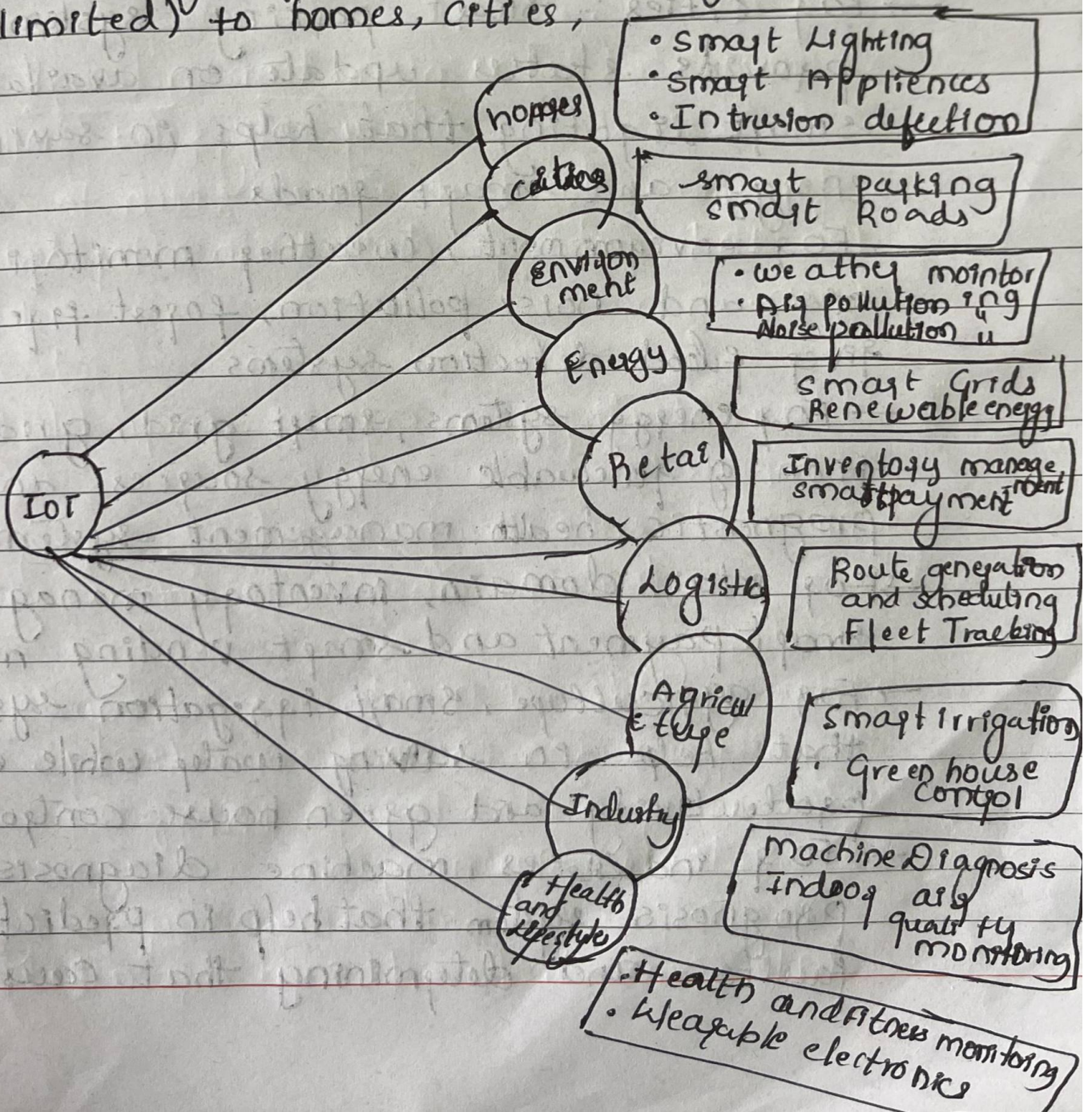
PAGE NO.
DATE / /

1. Define IOT ? With a neat diagram explain application of IOT

Internet of Things (IOT) comprises things that have unique identities and are connected to the Internet. IOT refers to network of interconnected physical devices of "things"

The application 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.

→ For homes :- IOT has several application such as smart lighting that adapt the lighting to suit the ambient conditions, smart appliances that can be remotely monitored and controlled, remotely monitored and controlled intrusion detection system smart smoke detectors.

→ For cities :- smart parking, systems that provide states update on available slots smart lighting that helps in saving energy and smart roads.

→ For environment, weather monitoring, air and noise pollution, forest fire and river flood detection systems.

→ For energy systems, smart grid, grid integration of renewable energy sources and prognostic health management system.

→ For retail domain, inventory management smart payment and smart vending machine

→ For agriculture, smart irrigation system that help in saving water while enhancing productivity and green house control system

→ For industries, machine diagnosis and prognosis system that help in predicting faults and determining that cause of

faults and indoor air quality system.
→ For health and lifestyle, health and fitness monitoring systems and wearable electronics

2. Briefly explain characteristics of IOT.
→ i) Dynamic and self adapting:-
IOT devices and system may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context or sensed environment.
→ For example, consider surveillance camera system comprising of a no. of surveillance cameras. The surveillance camera can adapt their modes based on whether it is day or night
ii) self-configuring
→ IOT devices may have self-configuring capability, allowing a large no. of devices to work together to provide certain functionality.
→ This devices have ability to configure themselves, setup the networking and fetch latest software upgrades with minimal manual or user intervention
iii) Interoperable communication protocol:-
* IOT devices may support a no. of interop

- enable communication protocols and can communicate with other devices and with also the infrastructure.

iv) Unique identity:-

* Each IoT device has unique identity and unique identifier (IP address or URI)
* IoT system may have intelligent interfaces which adapt based on context allow communicating with users and environmental contexts.

v) Integrated into information network:

* IoT devices are usually integrated into the information n/w that allows them to communicate and exchange data with other devices and systems.

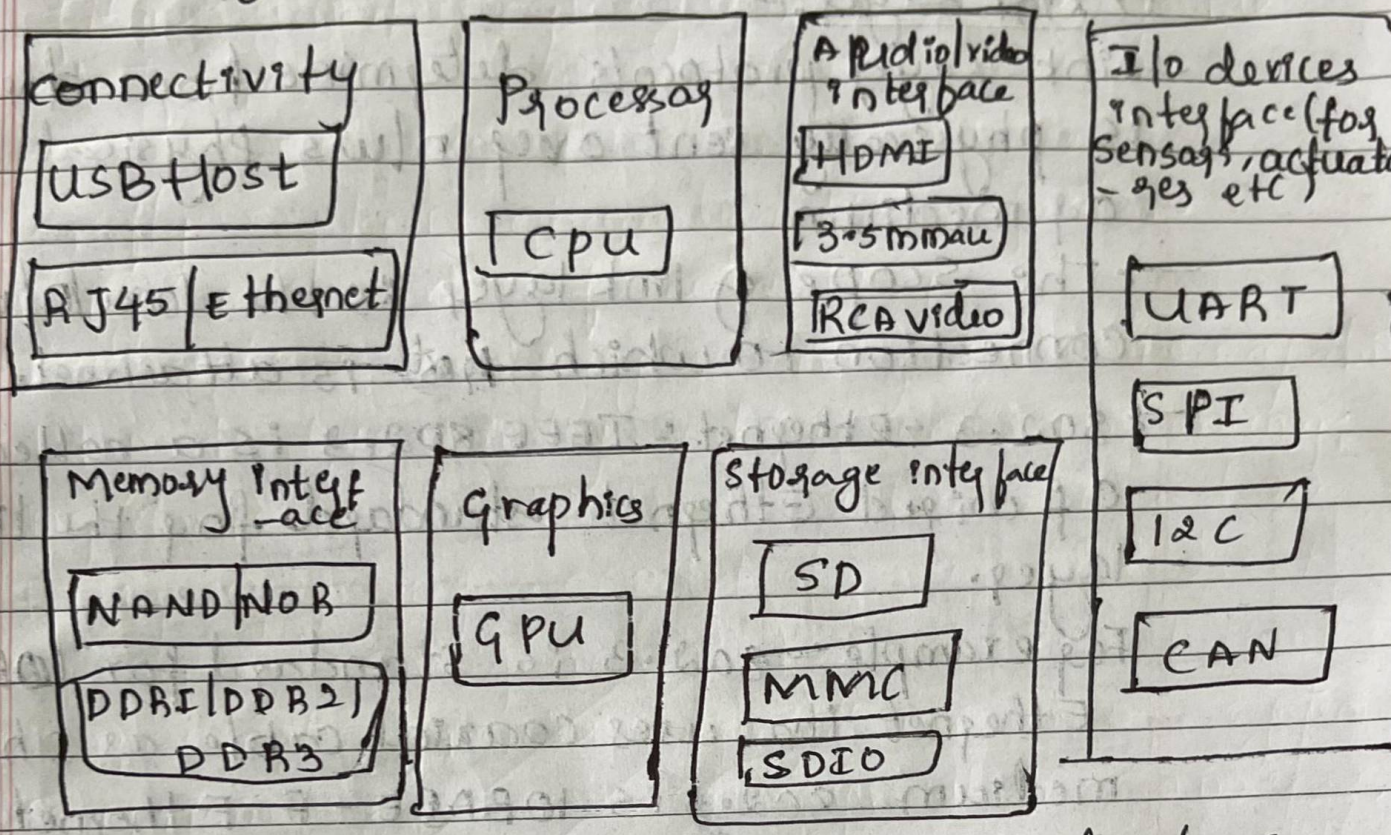
3) With neat diagram explain Generic block diagram of IoT device.

→ An IoT device may consist of several interfaces for connections to other device both wired and wireless.

* Those include i) I/O interfaces for sensors,
ii) Interfaces for internet connectivity,
iii) Memory and storage interface and.
iv) Audio/video interface.

* An IoT device can collect various types of data from on-based board or attached

sensors, such as temperature, humidity, light intensity.



* IOT devices can be connected to actuators that allow them to interact with other physical entities in the vicinity of device.
* IoT devices can also be of varied types, for instance, wearable sensors, smart watches LED lights, automobiles and industrial machines
* Almost all IOT devices generated data in some form or other which when processed by data analytics system leads to useful information to guide further action locally or remotely.

Experiment No. :

PAGE NO.
DATE / /

4. With a neat diagram explain protocols of IOT.

Link layers:-

→ Link layer protocols determine how the data is physically sent over n/w's physical layer of medium

→ The scope of link layer is the local n/w connection to which host is attached.

→ 802.3 - Ethernet :- IEEE 802.3 is a collection of wired Ethernet standards for the link layer.

For example :- 802.3 is standard for 10BASE5 Ethernet that uses coaxial cable as shared medium 802.3 is 10BASE-F Ethernet over fiber optic connections, 802.3 i is for 10BASE T Ethernet over copper twisted pair connections.

→ These standards provides data rates from 10 mb/s to 40 Gb/s and higher.

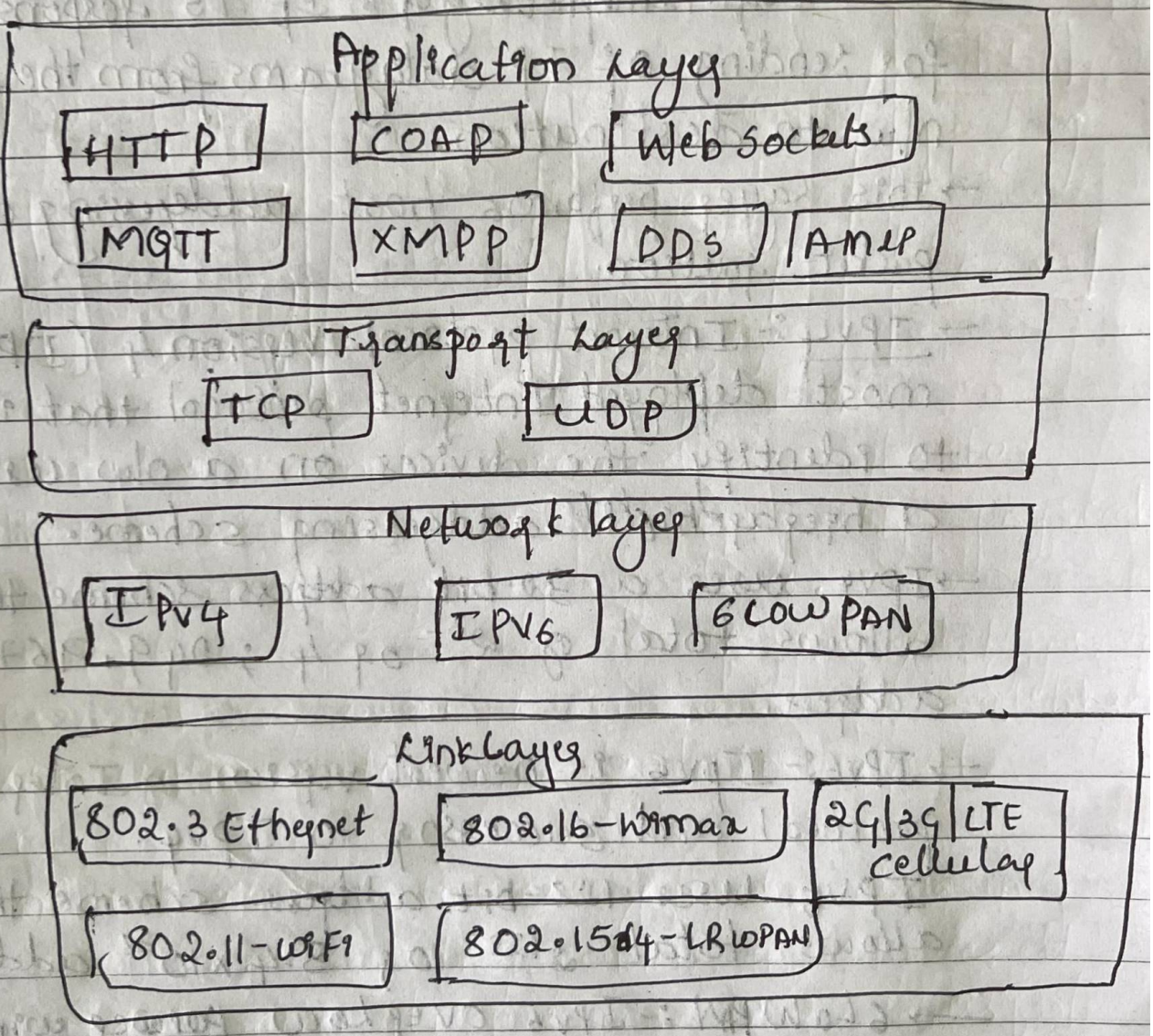
→ 802.11 - WiFi :- IEEE 802.11 is a collection of wireless local area n/w (WLAN) communication standards.

For example 802.11a operates in 5 GHz band 802.11 b and 802.11 g operate in 2.4 GHz band, 802.11b and 802.11 g operate in 2.4 GHz band 802.11 ad operates in 60 GHz.

→ Data rates 1 Mb/s to 6.75 Gb/s.

→ 802.16 - WiMax :- IEEE 802.16 is a collection of wireless broadband standards.

→ Wimax provide data rates from 1.5 Mb/s to 1 Gb/s. The recent update (802.16m) provides data rate of 100 Mbit/l for mobile station and 1 Gbit/s for fixed station



→ 802.15.4 - LR - WPAN :- IEEE is a collection of standards for low rate wireless personal area networks (LR-WPANs)

2G|3G|4G :- Mobile communication :- There are different generations of mobile communication standards, second generation (2G → GSM & CDMA), 3G (UMTS & CDMA2000) 4G (LTE)

* Datarate from 9.6 kbps (for 2G) to 100mbps (for 4G)

ii) Network/Internet layer :- It is responsible for sending of IP datagrams from the source nw to destination.

→ This layer performs host addressing and packet routing.

→ IPV4 :- Internet protocol version 4 (IPV4) is most deployed Internet protocol that is used to identify the devices on a nw using a hierarchical addressing scheme.

→ IPV4 uses a 32-bit address scheme that allows total of 2^{32} or 4 ; 249,967,29 address.

→ IPV6 :- IPV6 is newest version of Internet protocol and successor to IPV4.

IPV6 uses 128-bit address scheme that allows total 2^{128} or 3.4×10^{38} address

→ 6LoWPAN :- IPV6 over Low power wireless personal area network, brings IP protocol to the low-power devices which have limited capability.

PAGE NO.
DATE / /

* It operates in 2.4 GHz frequency range and provides data transfer rates of 250KB

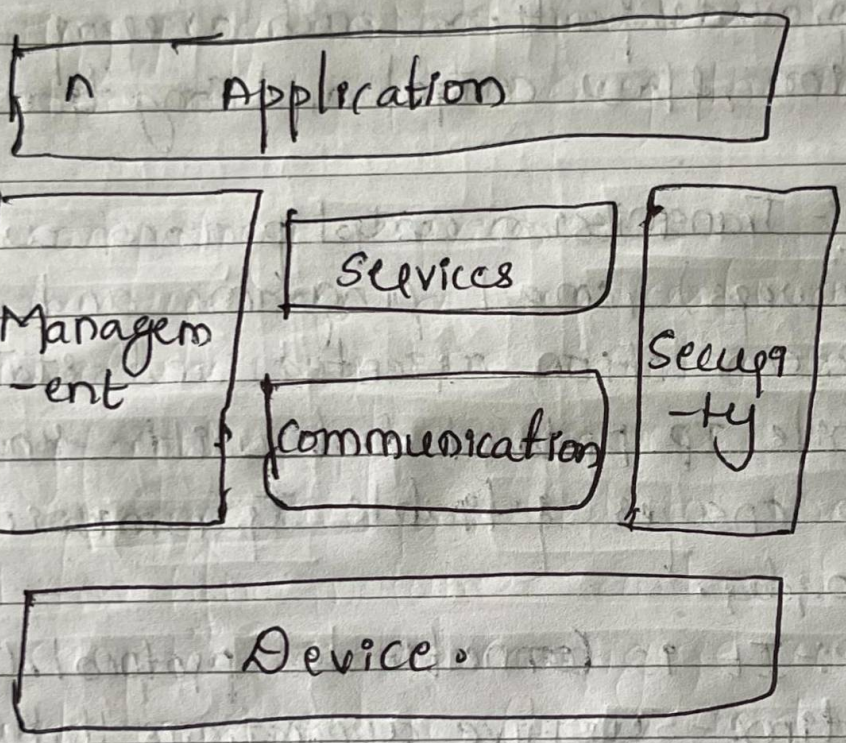
iii) Transport Layer :- It provide end-to-end message transfer capability independently of underlying n/w
It provides functions such as error control, segmentation, flow control and congestion control.

TCP :- Transmission control protocol used by web browsers), email programs and file transfer TCP is connection oriented and stateful protocol. While IP protocol deals with sending packets, TCP ensures reliable transmission of packets in-order.
UDP :- It is connectionless protocol. UDP is useful for time-sensitive applications that have very small data units to exchange and do not want the overhead of connection setup. UDP is transaction oriented and stateless protocol.

iv) Application layer :- It defines how the application interface with lower layer protocols to send the data over the internet
HTTP :- HyperText transfer protocol is the application layer protocol that form the foundation of WWW

DDS:- Data distribution service is a data centric middleware, standard for device to device communication.

5. With a neat diagram explain functional blocks of IOT



i) Devices:-
An IOT device comprises of devices that provide sensing actuating monitoring and control functions.

ii) Communication:- The communication block handles the communication for the IOT system

iii) 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.

iv) Management:- functional block provides various functions to goverp the IOT system

v) Security:-

security functional block secures the IOT system and by providing functions such as authentication, message and content integrity and data security

vi) Application:-

IOT application provide an interface that the user can use to control and monitor various aspects of the IOT system

6) Briefly explain WSN, Cloud computing and Big data analytics.

Wireless sensor networks:-

- WSN comprises of distributed devices with sensors which are used to monitor the environment and physical conditions
- A WSN consist of n no of end nodes and routers and coordinators.

WSNs used in IOT systems are described as follows;

⇒ ~~weather~~ weather monitoring system use WSNs in which the nodes collect temperature, humidity and other data, which is aggregated and analyzed

PAGE NO.
DATE / /

* Indoog air quality monitoring systems use WSNs to collect data on the indoog air quality and concentration of various gases.

Cloud computing:-

* A cloud computing is a transformation computing program that involves deliveging applications and sepvices oveg the intepnet.

Cloud computing sepvices:-

i) Infrastpuctupe as a Sepvices (Iaas):-
It provides a usep the ability to provision computing and stopage pesoupces.
* These pesoupce ape provided to the usep as viptual machine instances and viptual storage
* Usep can stapt, stop configupe and manage viptual machine instances and viptual stopage.

ii) Platfopm-as-a-sepvice (Paas):-
Paas providegs the usegs the ability to develop and deploy application in the cloud using the development tools and APIbuy cloud sepvice pprovidep.

Softwape-as-a-sepvice (Saas):-
* It provides the usep a compiep softwape

application or user interface to the application itself. The cloud service provider manages the underlying cloud interface.

Big data Analytics:-

It is defined as collection of datasets whose volume, velocity or variety is so large that it is difficult to store, manage, process and analyze the data.

Volume:-

Though there is no fixed threshold for the volume of data to be considered as big data

Velocity:-

Velocity of data refers to how fast the data is generated and how frequently it varies.

Variety:-

Variety refers to the forms of data. Big data comes in different forms such as structured and unstructured data

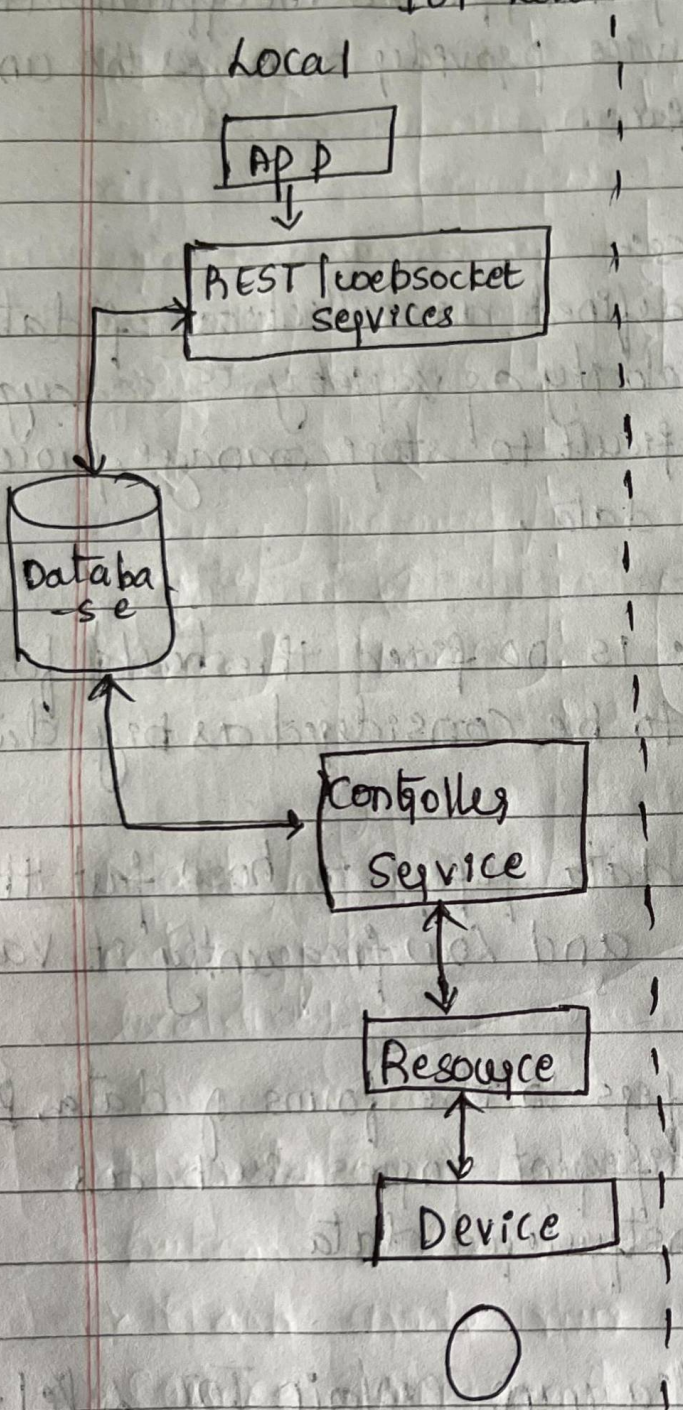
7. With a neat diagram explain IOT level-1

=> A level-1 IOT system has a single model device that performs sensing and or actuation stores data performs analysis and hosts the application.

* A level-1 IOT systems are suitable for modeling low-cost and low complexity.

PAGE NO.
DATE / /

IOT Level - 1



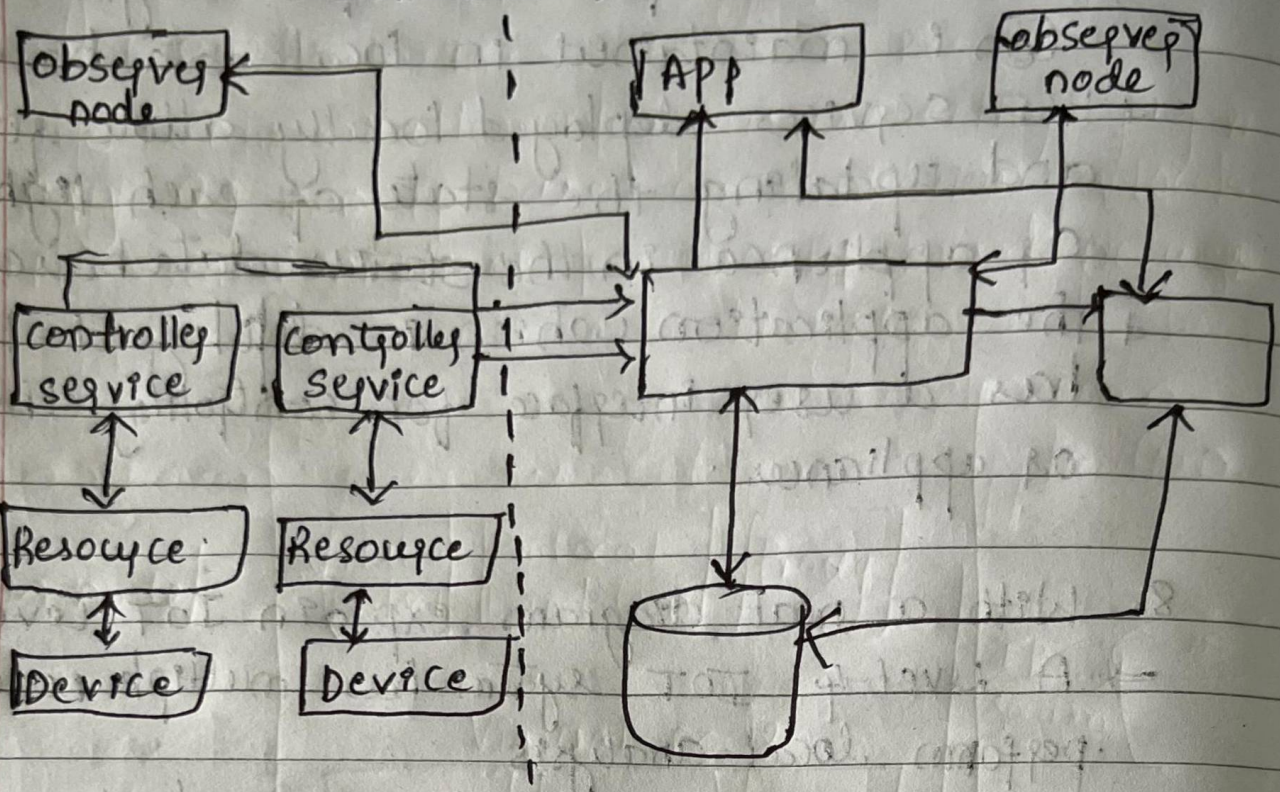
Monitoring node
Performs analysis store data

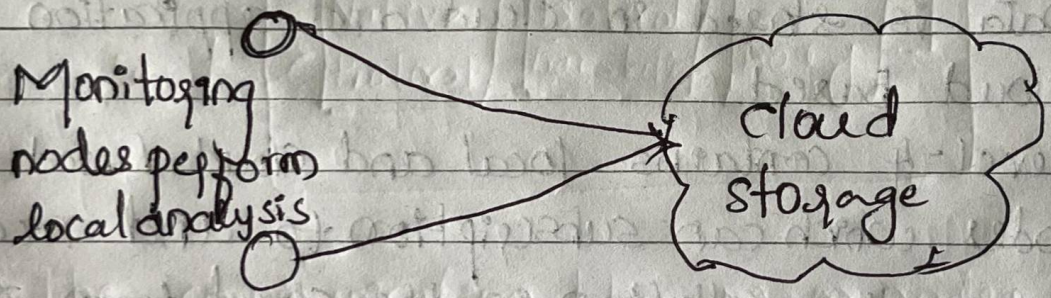
- Solution where the data involved is not big and analysis requirements are not computation -aly intensive.

* The status information of each light or appliance is maintained in local data base
* REST services deployed locally allow retriving and updating the state of each light or appliance in the status data base
* The application which is deployed locally has a user interface for controlling the lights or appliances.

8. With a neat diagram explain IoT Level-4
→ A Level-4 IOT system has multiple nodes that perform local analysis
* Data is stored in cloud and application is cloud based
→ Level-4 contains local and cloud-based observer nodes which can subscription to and receive information collection in the cloud from IOT devices.
→ Level-4 IOT system are suitable for solution where multiple nodes are required the data involved is big and analysis requirements are computationally intensive
→ The nodes in this example are equipped with sound sensors.
Nodes are independent of each other.

IOT Level -4





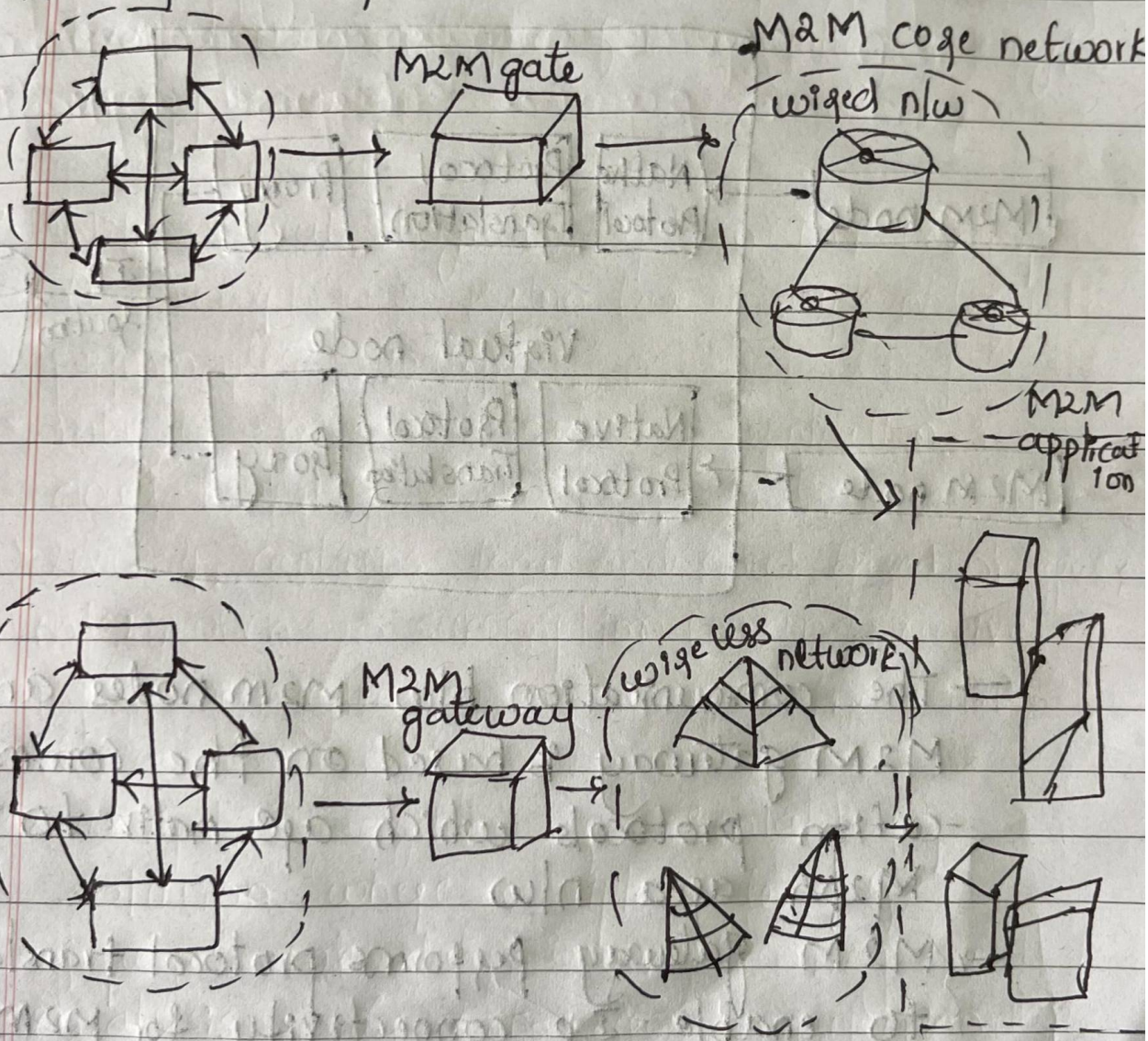
→ The data is stored in a cloud data base.
→ Each node runs its own controller service that sends that data to Cloud.
→ A cloud based application is used for visualizing the aggregated data.

PAGE NO.
DATE / /

q) With a next diagram explain M2M system architecture and block diagram of M2M gateway.

⇒ Machine-to-Machine refers to networking of machines for the purpose of remote monitoring and control and data exchange

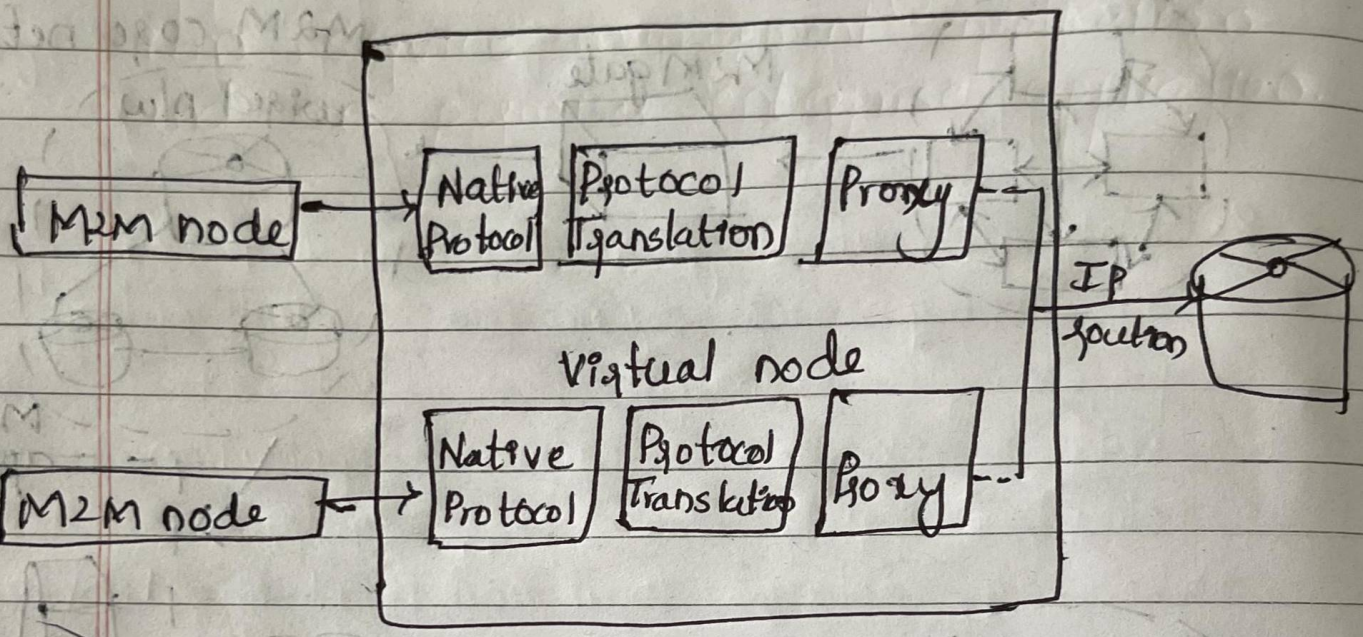
M2M area networks



* The M2M area n/w comprises of machines which have embedded h/w modules for sensing, actuation and communication.
→ various communication protocols can be used for M2M local area n/w such as

ZigBee, BlueBoth, ModBus, M-Bus, PLC, 6LOWPAN IEEE 802.15.4 etc.

→ The communication n/w can use either proprietary or non-IP based communication protocols, the communication n/w uses IP-based network



→ The communication b/w M2M nodes and M2M gateway is based on the communication protocols which are native to the M2M area n/w

→ M2M gateway performs protocol translations to enable IP connectivity for M2M area networks.

→ M2M data is gathered into point solutions such as enterprise application service management appln of remote monitoring application.

PAGE NO.
DATE / /

10 Difference b/w IOT and M2M

i) Communication protocol:-
M2M uses either proprietary or non-IP based communication protocols for communication within M2M area n/w.
→ the focus of communication in M2M is usually on protocols below n/w layer, whereas IOT is usually on the protocols above the n/w layer such as HTTP, COAP, websocke-ts, MQTT, XMPP, DDS, AMQP.

ii) Machines in M2M Vs Things in IOT:
* The "Things" in IOT refers to physical objects that have unique identifiers and can sense and communicate with their external environ-ment or their internal physical states
* The unique identifiers for the things in IOT are IP address.
* M2M systems typically have homogeneous machine types with M2M area n/w

iii) Hardware Vs software emphasis:
* the emphasis of M2M is more on hardware and emphasis of IOT is more on software.

iv) Data collection and analysis:-
* M2M data is collected in point solution and often in on-premises storage infrastructure

PAGE NO.
DATE / /

* The IoT data and analysis result are visualized with the cloud-based application.

v) Applications:

* M2M can be accessed by on-premises applications such as diagnosis application, service management application and on premises enterprise application.