Eighth - Semester B.E Degree Examination, ~~June/July~~ 2019. (17CS81)

Time: 3hrs.

Max. marks: 80 marks. Internet of Things.

Module-01

1. a What is IOT? Explain in detail on Genesis of IOT. — 10 marks

IOT is a technology transition in which devices will allow us to Sense and control the Physical world by making objects Smarter & connecting them through an intelligent network.

Genesis of IOT:

The age of IOT is often said to have started between the years 2008 and 2009. During this time period, the number of devices connected to the internet eclipsed the world's population.

The person credited with the creation of the term "IOT" is Kevin Ashton.

Keven has Subsequently explained that IOT now involves the addition of Sense to computers.

He was quoted as saying: "In the twentieth Century, Computers were brains without senses.

Computers depended on humans to input data & knowledge through typing, bar codes, & so on.

As shown in Fig 1.1, the evolution of the internet can be categorized into four phases.

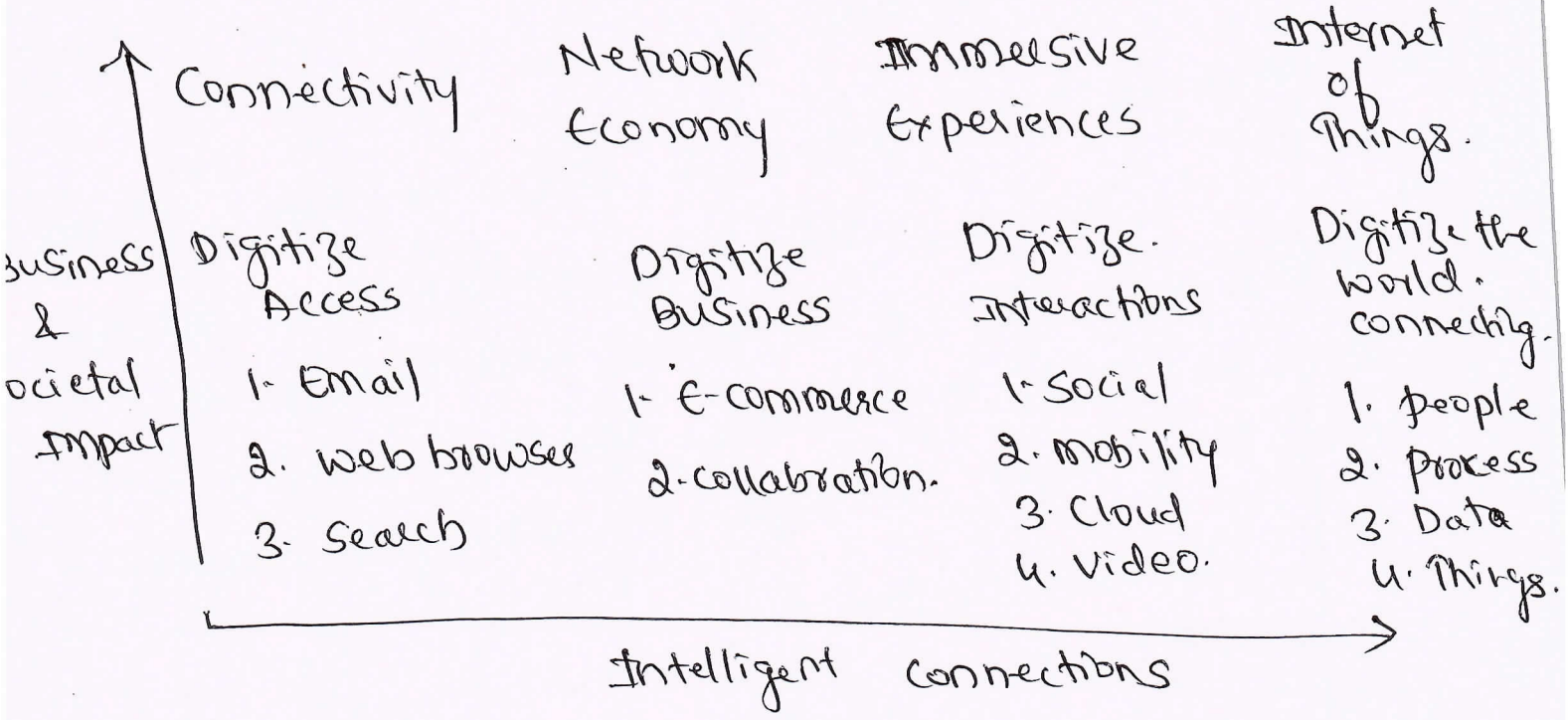


Fig. 1.1 Evolutionary Phases of the Internet.

1.b. what does IOT & digitization mean? Elaborate on this concept. - 04 marks

IOT & digitization are teems that are often used interchangeably. In most contexts, this duality is fine, but there are key differences to be aware of.

At a high level, IOT focuses on connecting "things", such as objects & machines to a computer Network such as the internet. IOT is a well understood term used across the industry as a whole. On the other hand, digitization can mean

different things to different people but generally encompasses the connection of "things" with the data they generate & the business insights that result.

Digitization, as defined in its simplest form, is the conversion of information into a digital format.

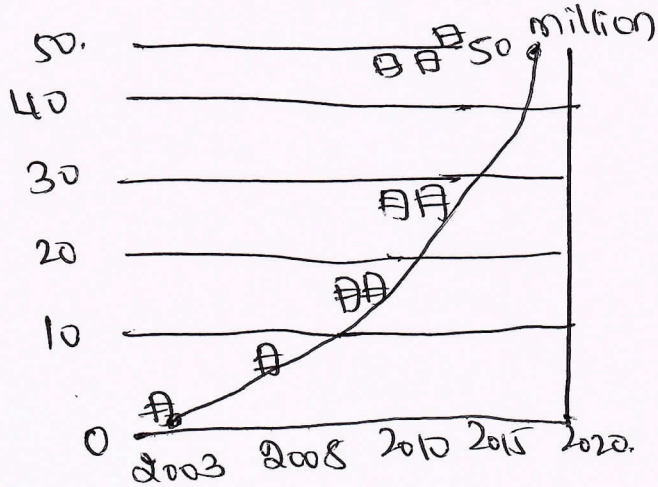
Digitization has been happening in one form or another for several decades.

In the context of IOT, digitization brings together things, data & business process to make networked connections more relevant & valuable.

1.C. write a short on "IOT impact in Real world". — 04 mark

Projections on the potential impact of IOT are impressive. About 14 billion, or just 0.007. of things are connected to the internet today.

Fig 1.2 provides a graphical look at the growth in the number of devices being connected.



What these numbers mean is that IOT will fundamentally shift the way people & business interact with their surroundings.

Managing & monitoring smart objects using real-time connectivity enables a whole new level of data driven decision making.

The following example illustrate some of the benefits of IOT & their impact.

1- Connected Roadways
2- Connected factory,
3. Smart connected Buildings

2.a Discuss IOT Challenges. - 8marks.

Many parts of IOT have become reality, but certain obstacles need to be overcome for IOT to become ubiquitous throughout industry & our everyday life.

Table. highlights a few of the most significant challenges & problems that IOT is currently facing.

	Challenge	Description
1.	Scale.	While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger.

2. Security — With more "things" becoming connected with other "things" & people, Security is an increasibly complex issue for IOT.

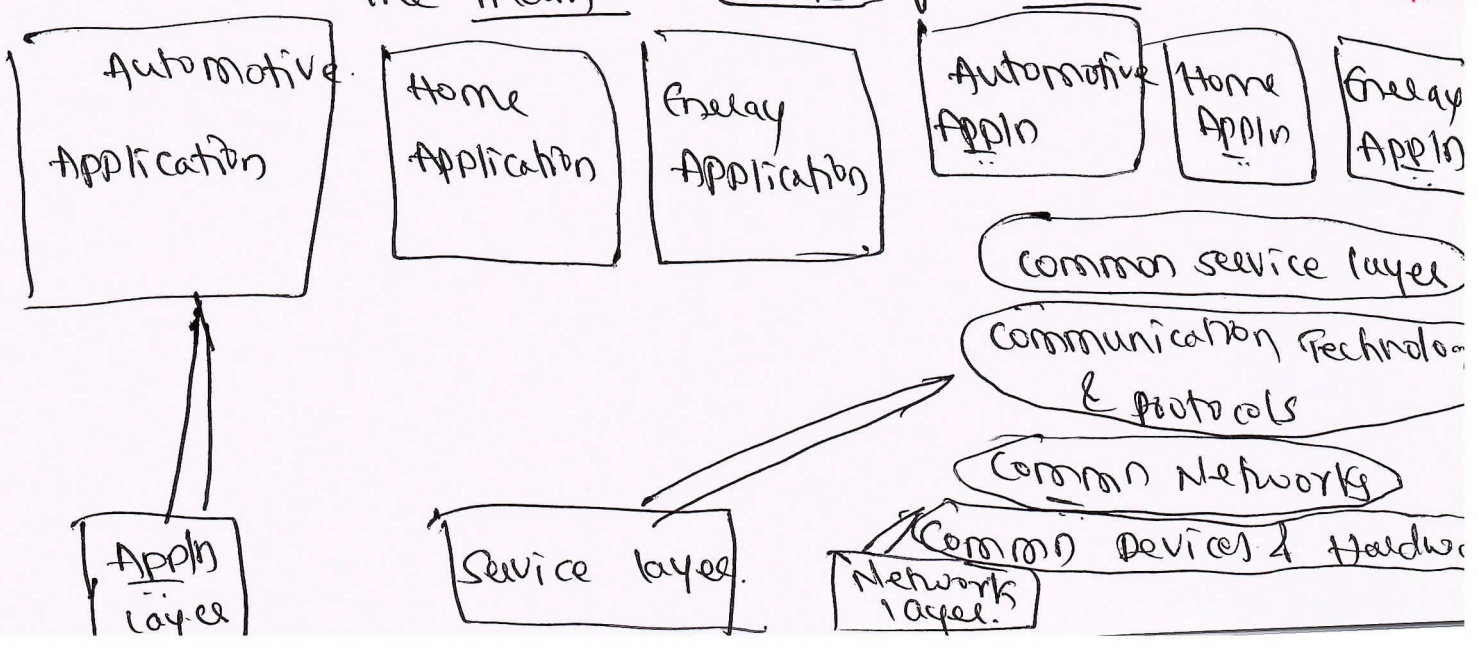
3. Privacy — An Sensors become more prolific in our everyday lives, much of the data they gathes will be specific to individuals & their activities

4. Big data & data Analytics — IOT and its large number of sensors is going to trigger a deluge of data that must be handled.

5- Interoperability — As with any other nascent technology, various protocols & architectures are Jockeying for market share & Standardization within IOT.

2.b. With a neat diagram, explain architecture of IOT.

The main Elements of IOT Architecture - cuma



One of the greatest challenges in designing an IoT architecture is dealing with the heterogeniy of devices, Software & access methods.

By developing a horizontal platform architecture one can is developing standards that allow interopera-bility at all levels of the IoT Stack.

For example you might want to automate your HVAC System by connecting it with wireless tempeature Sensors Spread throughout your Office.

2.c. Explain Core IoT functional Stack. 04marks

IoT networks are built around the concept of things or smart objects performing functions & delivering new connected Services.

These objects are "Smart" because they use a combination of contextual information & Configured goals to perform actions. These actions can be Self-contained.

From an architectural Standpoint, Several Components have to work together for an IoT network to be ~~opti~~ operational.

1. Things layer.
2. Communication network layer
3. Access network Sublayer.
4. Gateways & backhaul network Sublayer.

5. Network transport Sublayer.

6. IoT network management Sublayer.

7. Application & analytics layer.

Module -02.

3.a. List & explain different types of Sensors. -08 marks

Sensor Types	Example.
1) Position	Potentiometer.
2) Occupancy & motion	Electric eye.
3) Velocity & accelerations	Accelerometer
4) Force	Force guage.
5) Pressure	Barometer
6) Flow	Anemometer.
7) Acoustic.	Microphone.
8) Humidity	Hygrometer.
9) Light	Infrared Sensor.
10) Radiation	Geiger-muller.
11) Temperature	Thermometer.
12) Chemical	Breathalyzer.
13) Biosensors	Blood glucose biosenses.

3.b. Elaborate on Small physical objects & Small virtual objects. -04 marks.

Smart Objects: A definition of a smart object has been a bit nebulous because of the different interpretations of the term by varying sources.

In order to clarify some this confusion, we Provide here the definition of smart object.

1. Processing unit: A Smart object has some type of Processing unit for acquiring data, processing & Analyzing sensing information recieved by the Sensor.
2. Sensor(s) & actuator(s): A smart object is capable of interacting with the physical world through Sensors & actuators.
3. Communication device: The communication unit is responsible for connecting a smart object with other Smart objects & the outside world.
4. power source: Smart objects have components that need to be powered.

3.C. Explain "IOT Access Technologies". -04 marks.

For each of the IOT access Technologies a common information set is being Provided.

1. Standardization & alliances
2. Physical layer
3. MAC layer.
4. Topology.
5. Security.
6. Competitive technologies.

4.a Briefly explain Protocol Stack utilization IEEE 802.15.4. - 08 marks.

Some of the most well-known Protocol Stacks based on 802.15.4 are highlighted in Table 4.2

Protocol	Description.
1. Zigbee	Promoted through the ZigBee Alliance, Zigbee defines upper-layer components as well as application profiles. comm
2. 6LoWPAN	6LoWPAN is an IPV6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPV6 packets over IEEE 802.15.4 layer
3. ZigBee IP	An evolution of the ZigBee Protocol Stack, ZigBee IP adopts the 6LoWPAN adaptation layer.

4. ISA 100.11a — ISA 100.11a is developed by the ISA as "Wireless Systems for Industrial Automation.

5. WirelessHART — WirelessHART, promoted by the HART COMMP foundation is a protocol stack that offers a time-synchronized, self-organizing & self-healing mesh architecture.

6. Thread — Constructed on top of IETF 6LoWPAN/IPv6, thread is a protocol stack for a secure & reliable mesh network to connect & control products in the home.

4.b. What is SANET? Explain some advantages & disadvantages that a wireless based solution offers? @8 marks

A Sensor/Actuator network (SANET), as the name suggests, is a network of sensors that sense & measure their environment and/or actuators that act on their environment.

The sensors and/or actuators in a SANET are capable of communicating & co-operating in a product manner.

The following are some advantages & disadvantages that a wireless based solution offers.

Advantages

1. Greater deployment flexibility.
2. Simpler scaling to a larger number of nodes.
3. Lower implementation costs.
4. Easier long-term maintainance.
5. Effortless introduction of new sensor.
6. Better equipped to handle rapid/dynamic topology changes.

Disadvantages.

1. Potentially less secure.
2. Typically lower transmission speeds.
3. Greater level of impact/influence by environment.

Module 03

5.a. Explain working of IP as the IOT network layer.

The network transport layer sublayer that is part of the communications network layer.

It is composed of the following sections.

1. The Business case for IP: it discusses the advantages of IP from an IOT perspective & introduces the concept of adoption & adaptation.

2. The Need for optimization : It dives into the challenges of constrained nodes & devices when deploying IP.

3. Optimizing IP for IOT : It explores the common protocols & technologies in IOT networks utilizing IP, including 6LOWPAN, 6Tisch & RPL.

4. Profiles & compliances : It provides a summary of some of the most significant organisations & standards bodies involved with IP connectivity & IOT.

5b. Write note on Business Case for IP. - 04 marks

Data flowing from or to "things" is consumed, controlled or monitored by data center servers either in the cloud or in locations that may be distributed or centralized.

IP was not only ~~more~~ preferred in the IT markets but also for the OT environment.

The key advantages of Internet protocol.

1. Open & standard based
2. Versatile.
3. Ubiquitous.

4. Scalable.

5. Manageable & highly secure.

6. Stable & resilient.

7. Consumers market adoption.

8. Innovation factor.

5.C. Discuss need for optimization. - 04 marks

The following section lists why optimization is necessary for IP.

i) Constrained nodes.

IOT constrained nodes can be classified as follows.

1. Devices that are very constrained in resources, may communicate infrequently to transmit a few bytes, and may have limited security & mgmt capabilities.

2. Devices with enough power & capacities.

3. Devices that are similar to generic PC's.

ii) Constrained Networks.

Constrained Networks have unique characteristics & requirements. In contrast with typical IP networks, where highly stable & fast links are available, constrained networks are limited by low-power, low-bandwidth links.

6a. Describe application protocols for IOT. 08marks

It includes the following sections.

1. The transport layer.
2. IOT Application Transport methods.

1. The transport layer.

With the TCP/IP protocol, two main Protocols are specified for the transport layer.

1. Transmission control protocol (TCP).
2. User Datagram Protocol (UDP).

1. Transmission control protocol :-

This connection-oriented protocol requires a session to get established between the source & destination before exchanging data.

2. User datagram protocol :- With this connectionless protocol, data can be quickly sent between source & destination - but with no gualantee of delivery.

2. IOT Application Transport methods :-

The following categories of IOT application protocols & their transport methods are.

1. Application layer protocol not present.
2. Supervisory Control & data acquisition (SCADA)
3. Generic web-based protocols.
4. IOT application layer protocols.

6b. Discuss the various methods used in IOT-Application transport - 08 marks.

The following categories of IOT application Protocols & their transport methods are explored in the following Sections.

1. Application layer protocol not present:

In this case, the data payload is directly transported on top of the lower layers. No application layer Protocol is used.

2. Supervisory control & data acquition (SCADA):-

SCADA is one of the most common industrial Protocols in the world. but it was developed long before the days of IP & it has been adapted for IP networks

3. Generic web-based Protocol: Generic Protocols, Such as Ethernet, wi-fi & 4G/LTE are found on many consume

and enterprise - class IOT devices that communicate over non- constrained networks.

4) IOT - application layer protocols :- IOT application layer protocols are devised to run on constrained nodes with a small compute footprint & are well adapted to the network bandwidth constraints on cellular or ~~sta~~ satellite links or constrained 6LowPAN networks.

Message queuing Telemetry Transport (MQTT) & Constrained Application Protocol (COAP) - are two well known examples of IOT application layer protocols.

Module - 04

7-a what ~~do~~ do you mean by data & analytics for IOT? explain - 04 marks

In the world of IOT, the creation of massive amounts of data from sensors is common & one of the biggest challenges - not only from a transport perspective but also from a data management standpoint.

Depending on how data is categorized, various data analytics tools & processing methods can be applied.

Two important categorizations from an IOT perspective are whether the data is

i) Structured

ii) Unstructured.

i) Data is in motion

ii) Data is at rest.

7b. Discuss Bigdata Analytics tools & technology? 8 marks

It is a common mistake for individuals new to the world of data management to use the terms big data & Hadoop interchangeably.

Big data analytics can consist of many different software pieces that together collect, store, manipulate and analyze all different data types.

It helps to understand the landscape by defining what big data is and what is not.

Generally, the Industry look to the "three Vs" to categorize big data.

1. Velocity
2. Variety.
3. Volume.

2. With a case study relate the concept of Securing IOT? 08 marks

It is often said that if world war III breaks out, it will be fought in Cyberspace. As IOT brings more & more systems together under the umbrella of network connectivity, Security has never been more important.

From the electrical grid system that powers our world, to the lights that control the flow of traffic in a city, to the systems that keep airplanes flying in an organized & efficient way, Security of the networks devices & the applications that use them is foundational & essential for all modern communication systems.

It includes the following sections.

1. A Brief History of OT Security :- It provides an overview of how OT environments have evolved & the impact that the evolution has had on Securi operational networks.

2. Common challenges in OT Security : It provi a synopsis of different security challenges in operational environments, including legacy systems

and insecure protocols & assets.

How IT and OT security practices & systems vary:

It provides a comparison between the security practices in enterprise IT environments & operational industrial environments.

4. Formal Risk Analysis Structures: OCTAVE & FAIR:-

It provides a holistic view of securing an operational environment & a risk assesment framework that includes the people, processes, and vendor ecosystem components that make up a control system.

5. The phased Application of security in an operational Environment: It provides a description of a phased approach to introducing modern network security into largely preexisting legacy industrial networks.

8a. Explain in detail how IT and OT Security Practices & systems vary in real time. - 08 marks

The differences between an enterprise environment & an industrial-focused OT deployme

are important to understand because they have a direct impact on the Security practice applied to them. Some of these areas are touched on briefly earlier & they are more explicitly discussed in the following sections.

1. The purdue model for control Hierarchy:-

Regardless of where a security threat arises, it must be consistently & unequivocally treated.

the operational domain must also address physical safety & environmental factors as part of its security strategy. and this is not normally associated with the IT domain.

2. OT Network Characteristics impacting Security.

while IT and OT network are beginning to converge, they still maintain many divergent characteristics in terms of how they operate & the traffic they handle.

3 Security priorities: Integrity, Availability & Confidentiality

Security priorities are driven by the nature of the assets in each environment.

In an IT realm, the most critical element & the target of attacks has been information.

1. Security Focus :-

Security focus is frequently driven by the history of security impacts that an organization has experienced.

The result has been a significant investment in capital goods & human power to reduce these external threats & minimize potential internal malevolent actors.

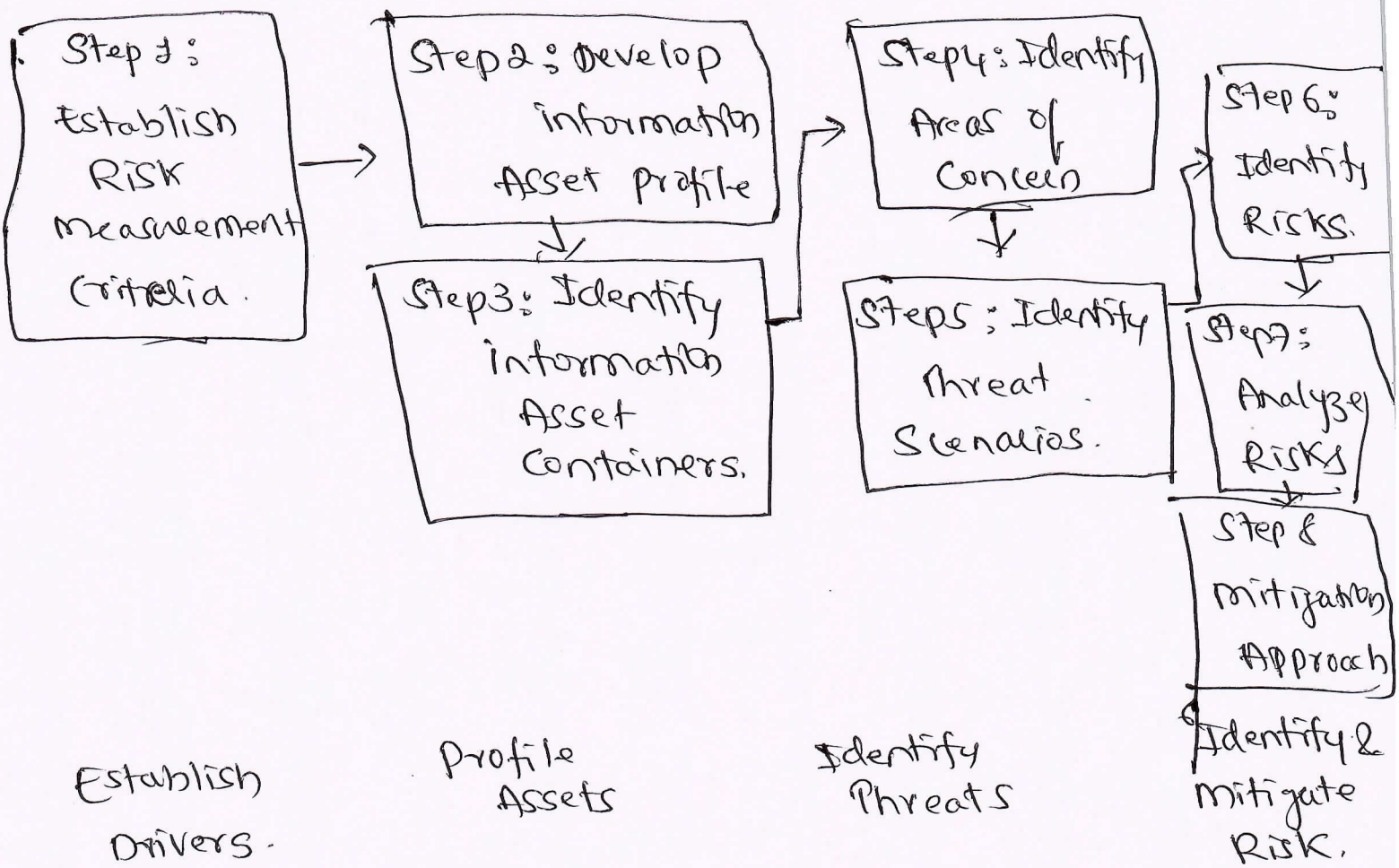
8b. Discuss OCTAVE and FAIR formal risk analysis. — 08 marks

1. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation).

* Octave has undergone multiple iterations. The vers this section focuses on is OCTAVE allegro, which is intended to be a lightweight & less burdensome pro to implement.

This approach & the assumptions it mo are quite appropriate, given that many operationa technology areas are similarly lacking in secur focused human assets.

Fig: illustrates the OCTAVE Allegro steps & phases



The first step of the OCTAVE Allegro methodology is to establish a risk measurement criterion.

The second step is to develop an information asset profile.

The third step is to identify information asset containers.

The fourth step is to identify areas of concern In the fifth step threat scenarios are identified.

At the sixth step risks are identified The seventh step is risk analysis, finally mitigation is

applied at the eighth step.

ii) FAIR:

Factor Analysis of Information Risk is a technical standard for risk definition from the open group.

While information security is the focus, much as it is for octave, Fair has clear applications within operational technology.

Like Octave, it also allows for non-malicious actors as a potential cause for harm, but it goes to greater lengths to emphasize the point.

Fair defines six forms of loss, four of them externally focused & two internally focused. Of particular value for operational teams are productivity & replacement loss.

Response loss is also reasonably measured with fines & judgements easy to measure but difficult to predict.

Finally competitive advantage & reputation are the least measurable.

Module 05

9.a. Give a brief note on Arduino UNo - 04 marks

Arduino is an Open Source electronics platform based on easy-to-use hardware & software.

Arduino UNo:

It is a microcontroller board based on the ATmega 328p.

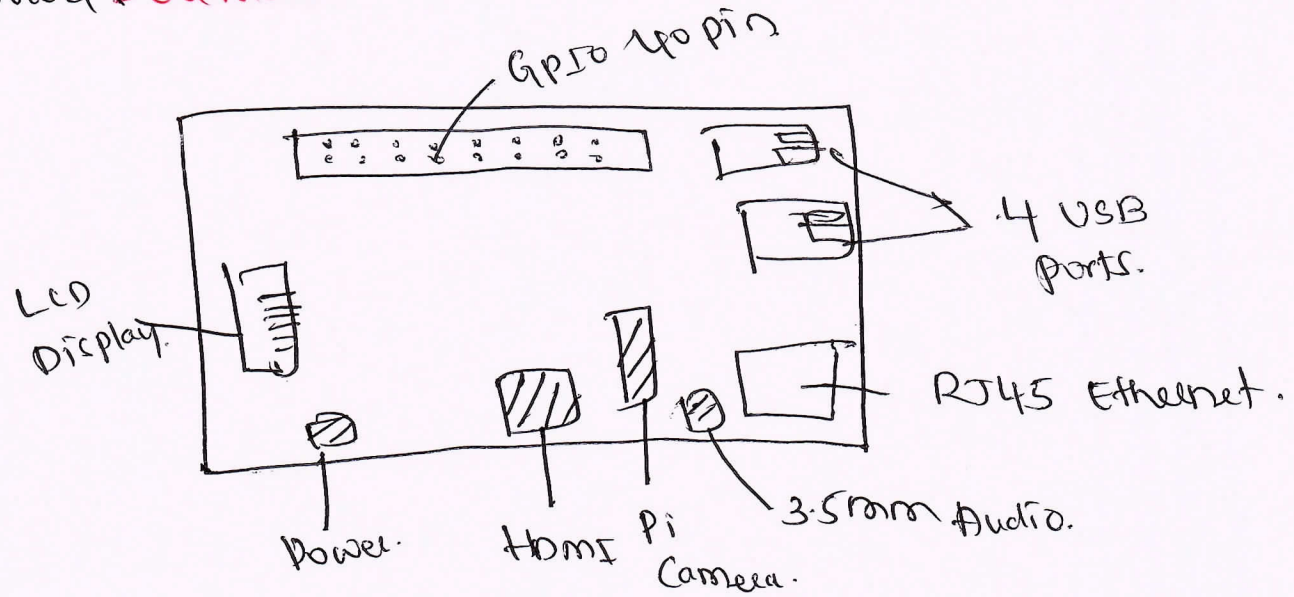
It has 14 digital input/output pins, 6 analog inputs, a 16MHz quartz crystal, a USB connection, a power Jack, an ICSP header & a reset button.

"UNo" means one in italian & was chosen to mark the release of Arduino Software (IDE) 1.0.

The UNo board & version 1.0 of Arduino software (IDE) were the reference versions of Arduino NOW evolved to newer releases.

1. Reset Button
2. AREF
3. Ground pin
4. Digital Input/output
5. PWM.
6. USB connection
7. TX/RX
8. ATmega Microcontroller
9. power LED indicator
10. Voltage regulator
11. DC power Barrel Jack
12. 3.3V pin
13. 5V pin
14. Ground pins
15. Analog pins.

9b. With a neat diagram, explain Raspberry Pi board - 04 marks.



Useful commands to run from a terminal or command line.

rasp-config :- Change your Pi configuration settings.

Startx : Start the GUI (Graphical user Interface)

if config : Get the details of ~~as~~ your Ethernet or wireless network adapter.

rPi-update : updates your Rasberry Pi firmware.

SSh : connect your Pi to other computers

Sudo : Run commands as Super user

Shutdown : This will shut down your Pi

Nano : This is your text editor for changing or adding files, Save, edit, Create.

7. c. With a neat diagram, explain wireless temperature monitoring system using Rasberry Pi. - 08 marks.

Wireless Temperature Monitoring System using Pi :—

Rasberry Pi which having ~~inbuilt~~ in-built wifi, which makes Raspberry Pi to suitable for IOT applications, so that by using IOT technology this Monitoring System works by uploading the temperature value to the thingspeak cloud by this project You can able to learn to ~~to~~ how to handle ~~to~~ cloud-based application using API keys.

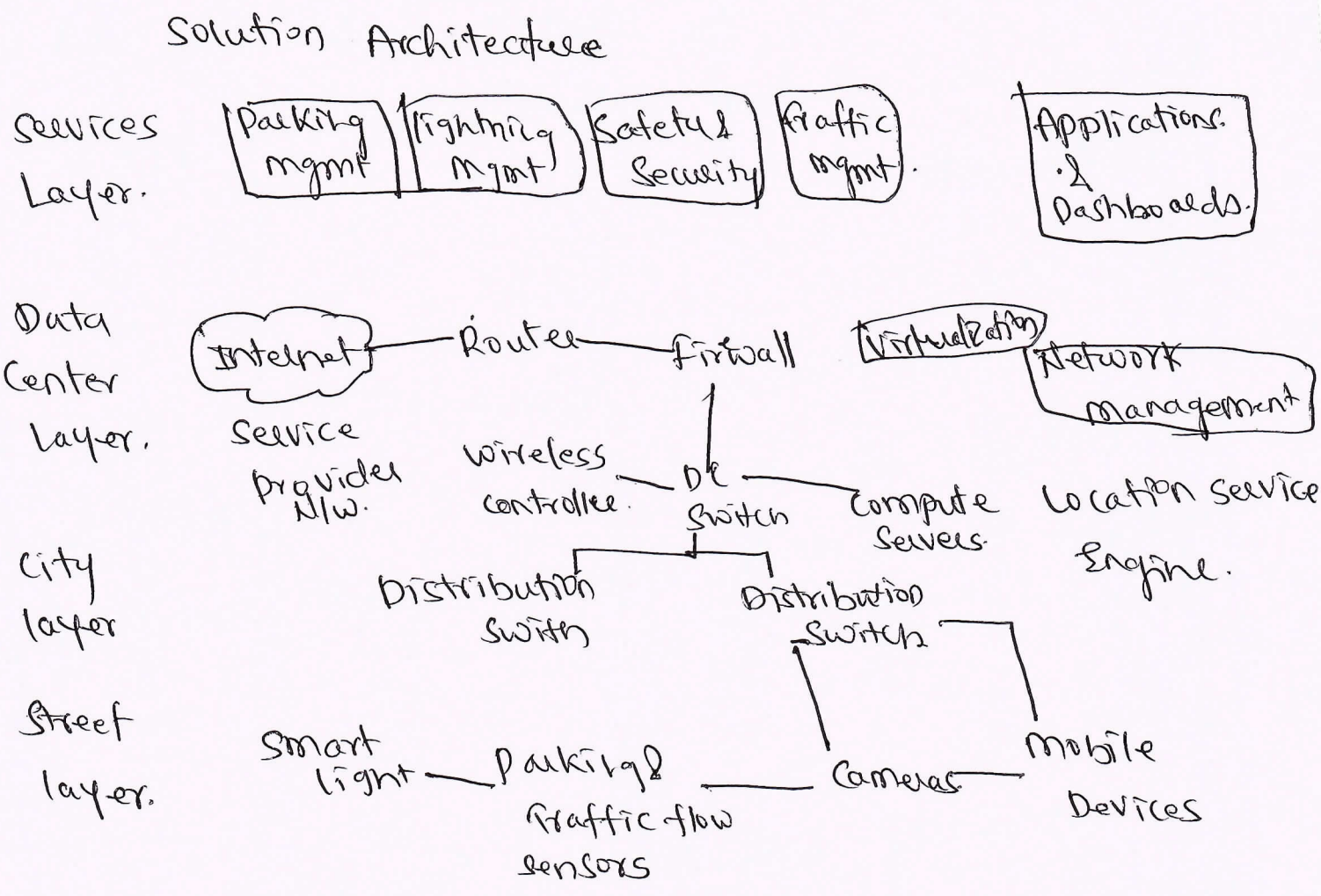
In this monitoring System, we used thingspeak clould, the cloud which is suitable to view the Sensor logs in the form of graph plots.

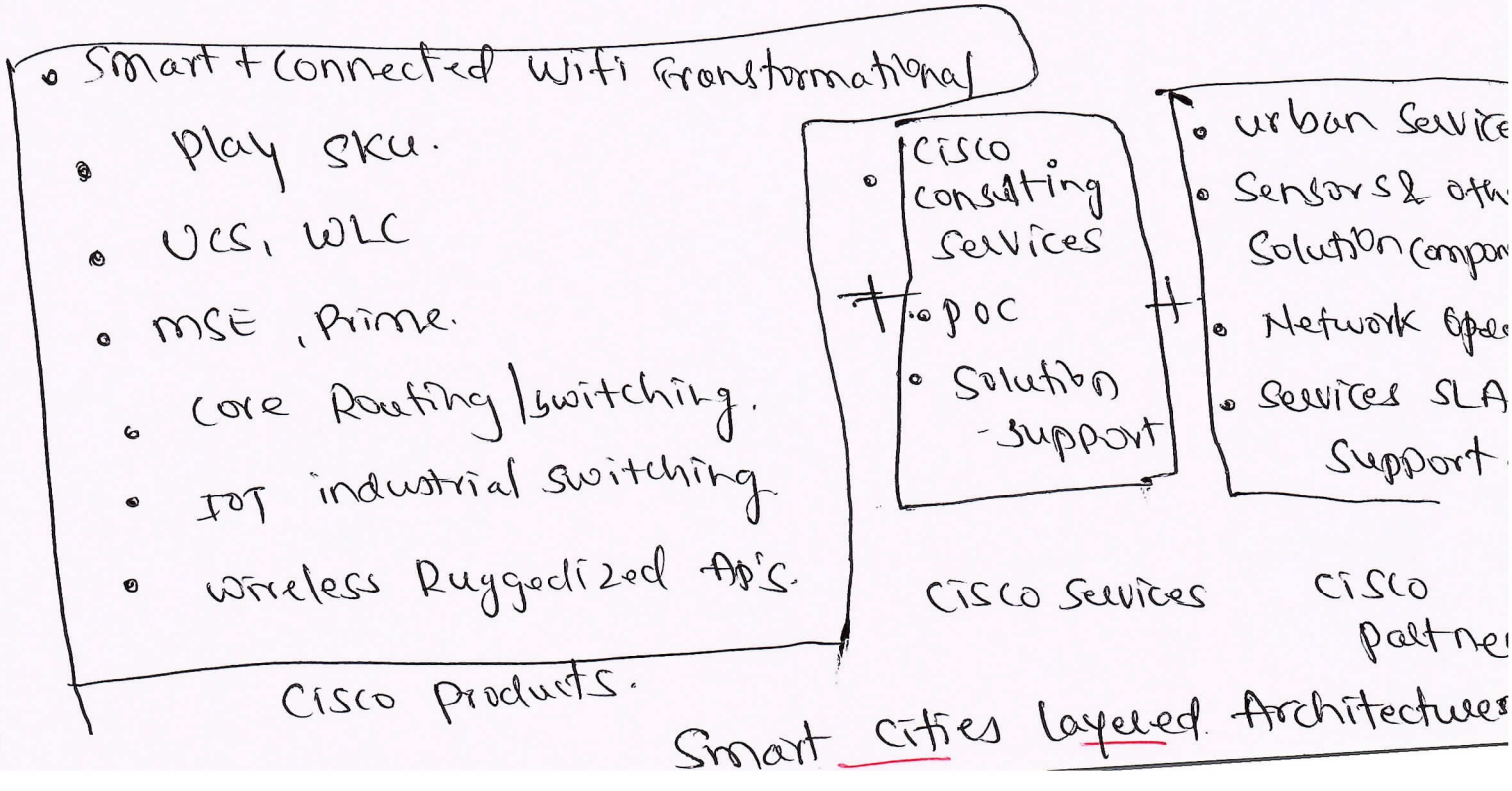
Here we created one field to monitor the temperature value, that can be reconfigueable to monitor a number of Sensor values in various field

This basic will teach you to how to work with a cloud by using LM35 as a temperature Sensor, to detect the temperature & to upload those values into the cloud.

10a. Explain in detail smart city IOT architecture? -8 marks.

A smart city IOT infrastructure is a four-layered architecture, as shown in fig.





1. Street layer.

The Street layer is composed of devices & sensors that collect data & take action based on instructions from the overall solution, as well as the networking components needed to aggregate & collect data.

2. City layer.

At the city layer, which is above the street layer, network routers & switches must be deployed to match the size of city data that needs to be transported.

3. Data Center layer.

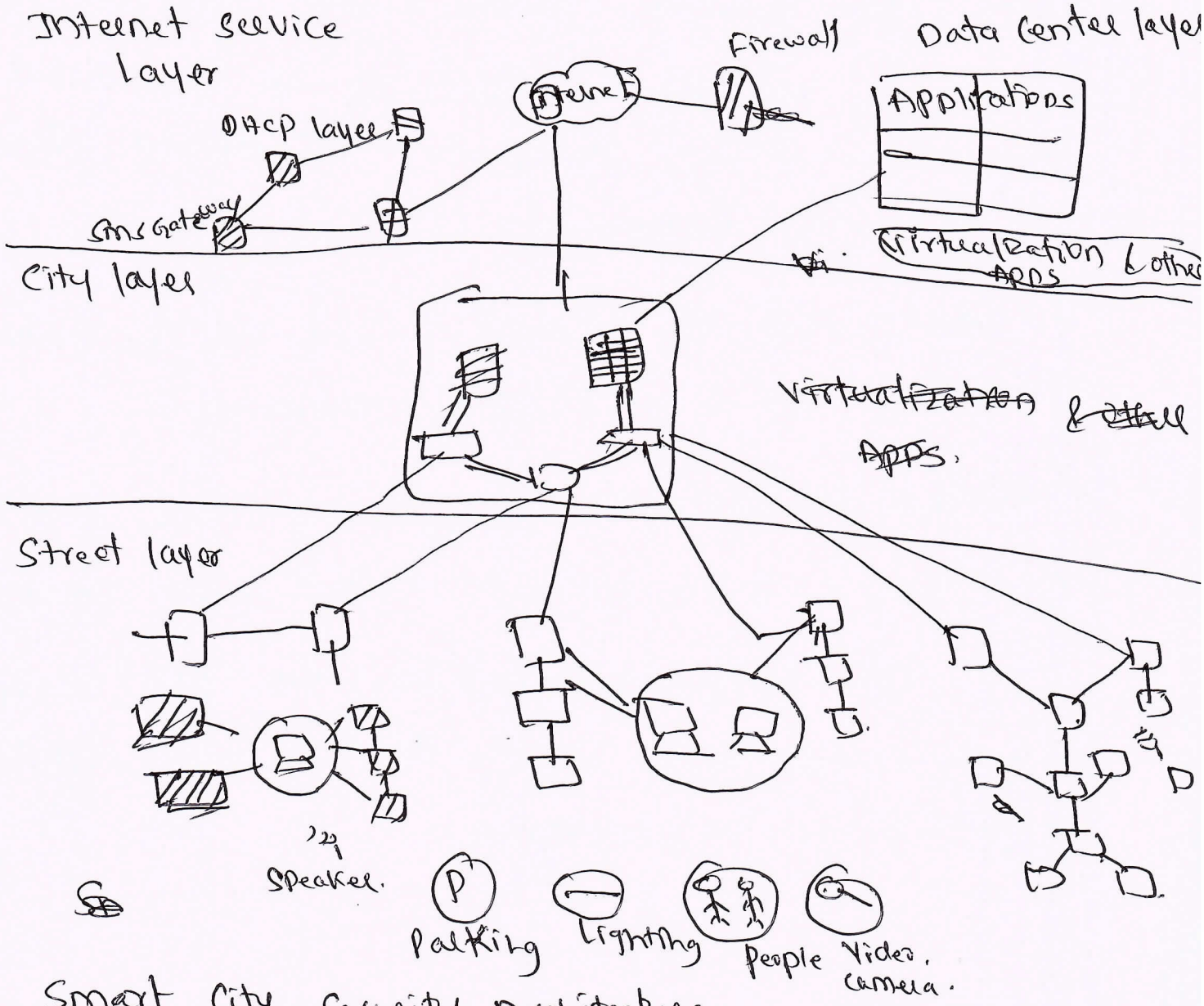
ultimately, data collected from the sensors is sent to a data center, where it can be processed & correlated.

4. Service layer.

ultimately, the ~~true~~ true value of ICT connectivity comes from the services that the measured data can provide to different users operating within a city.

10b. With the case study explain Smart & connected cities using Raspberry Pi. 08 marks.

Smart + connected city Reference Architecture



Smart City Security Architecture.

Starting from the street level, Sensors should have their own security protocols.

Some industry-standard security features include device/sensor identification & authorization; device/sensor data encryption; Trusted Platform module;

4. Service layer.

ultimately, the true value of ICT connecting comes from the services that the measured data can provide to different users operating within a city.

C. Write a short note on. 04marks.

i) IOT Challenges.

1. Safety.
2. Mobility.
3. Environment.
4. Privacy.
5. Big data & data analytics
6. Interopelability.

ii) Backhaul Technologies.

IOT devices & sensors often have constrained resources, however as compute capabilities increase.

Some new classes of IOT endpoints have enough compute capabilities to perform at least low-level analytics & filtering to make basic decisions.

PREPARED BY.

(Sandeep T.)

HOD.

Dean, Academics.