As Per New Syllabus of VTU 2015 Scheme
Choice Based Credit System(CBCS)

ALL IN ONE
SUNSTAR EXAM SCANNER
B.E.

8TH Sem CSE/ISE

- *As Per VTU CBCS Pattern*
- *Three CBCS Model Question Papers (With Answers)*

- Internet of Things Technology
- Big Data Analytics
- Network Management
- System Modeling and Simulation

AUTHORED BY A TEAM OF EXPERTS

SUNSTAR PUBLISHER
#4/1, Kuppaswamy Building, 19th Cross,
Cubbonpet, Bangalore - 560002
Phone : 080 22224143
E-mail: sunstar884@gmail.com

SUNSTAR EXAM SCANNER for 8th Sem B.E. CSE/ISE, V. T. U
Authored by A Team of Experts and Published by Sunstar Publisher, Bangalore - 2.

Pages : IV + 260	**No of Copies :** 1000
First Edition : 2019	**Paper used :** 11.2 kg (58 GSM) Sripathi
	Book Size : 1/4th Crown

Published By:
SUNSTAR PUBLISHER
#4/1, Kuppaswamy Building, 19th Cross,
Cubbonpet, Bangalore - 560002
Phone : 080 22224143
E-mail: sunstar884@gmail.com

Composed by
S.B. SOLUTIONS
Bangalore

Printed at:
Sri Manjunatha Printers
Bangalore

Dedicated
to
All Engineering Students

CONTENTS

As Per New VTU Syllabus w.e.f 2015-16
Choice Based Credit System(CBCS)

SUNSTAR

SUNSTAR EXAM SCANNER

INTERNET OF THINGS TECHNOLOGY

(VIII SEM. B.E. CSE / ISE)

SYLLABUS

INTERNET OF THINGS TECHNOLOGY			
[AS PER CHOICE BASED CREDIT SYSTEM (CBCS) SCHEME] (EFFECTIVE FROM THE ACADEMIC YEAR 2016 - 2017)			
Subject Code	15CS81	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

MODULE 1

What is IoT, Genesis of IoT, IoT and Digitization, IoT Impact, Convergence of IT and IoT, IoT Challenges, IoT Network Architecture and Design, Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack.

MODULE 2

Smart Objects: The "Things" in IoT, Sensors, Actuat ors, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access Technologies.

MODULE 3

IP as the IoT Network Layer, The Business Case for IP, The need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT, The Transport Layer, IoT Application Transport Methods.

MODULE 4

Data and Analytics for IoT, An Introduction to Data Analytics for IoT, Machine Learning, Big Data Analytics Tools and Technology, Edge Streaming Analytics, Network Analytics, Securing IoT, A Brief History of OT Security, Common Challenges in OT Security, How IT and OT Security Practices and Systems Vary, Formal Risk Analysis Structures: OCTAVE and FAIR, The Phased Application of Security in an Operational Environment

MODULE 5

IoT Physical Devices and Endpoints - Arduino UNO: Introduction to Arduino, Arduino UNO, Installing the Software, Fundamentals of Arduino Programming. IoT Physical Devices and Endpoints - RaspberryPi: Introduction to RaspberryPi, About the RaspberryPi Board: Hardware Layout, Operating Systems on RaspberryPi, Configuring RaspberryPi, Programming RaspberryPi with Python, Wireless Temperature Monitoring System Using Pi, DS18B20 Temperature Sensor, Connecting Raspberry Pi via SSH, Accessing Temperature from DS18B20 sensors, Remote access to RaspberryPi, Smart and Connected Cities, An IoT Strategy for Smarter Cities, Smart City IoT Architecture, Smart City Security Architecture, Smart City Use-Case Examples.

Eighth Semester B.E. Degree Examination,
CBCS - Model Question Paper - 1
INTERNET OF THINGS TECHNOLOGY

Time: 3 hrs. **Max. Marks:** 80

Note : ***Answer any FIVE full questions, selecting ONE full question from each module.***

Module - 1

1. a. What is IOT? Explain the features of IOT **(08 Marks)**

Ans. The most important features of IOT are

Connectivity: Connectivity refers to establish a proper connection between all the things of IOT to IvT platform it may be server or cloud. After connecting the IOT devices, it needs a high speed messaging between the devices and cloud to enable reliable, secure and bi-directional communication.

Analyzing: After connecting all the relevant things, it comes to real-time analyzing the data collected and use them to build effective business intelligence. If we have a good insight into data gathered from all these things, then we call our system has a smart system.

Integrating: IOT integrating the various models to improve the user experience as well.

Artificial Intelligence: IOT makes things smart and enhances life through the use of data. For example, if we have a coffee machine whose beans have going to end, then the coffee machine itself order the coffee beans of your choice from the retailer.

Sensing: The sensor devices used in IOT technologies detect and measure any change in the environment and report on their status. IOT technology brings passive networks to active networks. Without sensors, there could not hold an effective or true IOT environment.

Active Engagement: IOT makes the connected technology, product, or services to active engagement between each other.

Endpoint Management: It is important to be the endpoint management of all the IOT system otherwise; it makes the complete failure of the system. For example, if coffee machines itself order the coffee beans when it goes to end but what happens when it orders the beans from a retailer and we are not present at home for a few days, it leads to the failure of the IOT system. So, there must be a need for endpoint management.

b. Explain the IOT Applications **(08 Marks)**

Ans. The versatility of IOT has become very popular in recent years. There are many advantages to having a device based on IvT. **Mckinsey Global Institute reports that IOT business will reach 6.2 trillion in revenue by 2025.** There are lots of applications are available in the market in different areas.

1) Personal Home Automation System: Home Automation system is the major example in this area.

2)Wemo Switch Smart Plug: It is the most useful devices which connected home devices in the Switch, a smart plug. **It plugs into a regular outlet, accepts the power cable from any device, and can be used to turn it on and off on hit a button on your smartphone.**

3) Enterprise: In the enterprise area many applications are there Like environmental monitoring system, smart environment etc.

4) Nest Smart Thermostat: It is connected to the internet. **The Nest learns automatically your family's routines and will automatically adjust the temperature based on your activities, to make your house more efficient.** There is also a mobile app which allows the user to edit temperature and schedules.

5) Utilities: smart metering, smart grid, and water monitoring system are the most useful applications in the various utility area.

6) Energy Management: Advanced Metering Infrastructure is the major example in this area.

7) Medical and Health Care: Remote health monitoring and emergency notification system are examples of IOT in the medicalfield.

8) Health patch Health Monitor: It can be used for the patient who can't go to doctors, letting them get ECG, heart rate, respiratory rate, skin temperature, body posture, fall detection, and activity readings remotely.

9) Transportation: Electronic toll collection system is the most useful example in this area.

10) Large scale deployment: There are various large projects ongoing in the world. **Songdo (South Korea), the first of its kind fully wired Smart City, is near completion**. Everything in this city is planned to be wired, connected and turned into a data stream that would be monitored by an array of computers without any human interaction.

11) Another example is the Sino-Singapore Guangzhou Knowledge City work on improving air and water quality. French company Sigfox commenced building an ultra-narrowband wireless data network in the San Francisco Bay area in 2014. **Another example is the one completed by New York Waterways in New York City to connect all their vessels and being able to monitor them 24/7.**

So these are large applications are present in the market which is based on IoT. This world is going to become a better place to live with more communication with everyone. In near future large number of devices connected to the internet and provide great facilities to the world.

OR

2. a. Explain the IOT network architecture components. **(10 Marks)**

Ans. A "thing" is an object equipped with **sensors** that gather data which will be transferred over a network and **actuators** that allow things to act (for example, to switch on or off the light, to open or close a door, to increase or decrease engine rotation speed and more). This concept includes fridges, street lamps, buildings, vehicles, production machinery, rehabilitation equipment and everything else imaginable. Sensors are

not in all cases physically attached to the things: sensors may need to monitor, for example, what happens in the closest environment to a thing.

Gateways. Data goes from things to the cloud and vice versa through the gateways. A gateway provides connectivity between things and the cloud part of the IoT solution, enables data preprocessing and filtering before moving it to the cloud (to reduce the volume of data for detailed processing and storing) and transmits control commands going from the cloud to things. Things then execute commands using their actuators.

Cloud gateway facilitates data compression and secure data transmission between field gateways and cloud IoT servers. It also ensures compatibility with various protocols and communicates with field gateways using different protocols depending on what protocol is supported by gateways.

Streaming data processor ensures effective transition of input data to a data lake and control applications. No data can be occasionally lost or corrupted.

Data Lake. A data lake is used for storing the data generated by connected devices in its natural format. Big data comes in "batches" or in "streams". When the data is needed for meaningful insights it's extracted from a data lake and loaded to a big data warehouse.

Big data warehouse. Filtered and preprocessed data needed for meaningful insights is extracted from a data lake to a big data warehouse. A big data warehouse contains only cleaned, structured and matched data (compared to a data lake which contains all sorts of data generated by sensors). Also, data warehouse stores context information about things and sensors (for example, where sensors are installed) and the commands control applications send to things.

Data analytics. Data analysts can use data from the big data warehouse to find trends and gain actionable insights. When analyzed (and in many cases – visualized in schemes, diagrams, info graphics) big data show, for example, the performance of devices, help identify inefficiencies and work out the ways to improve an IoT system (make it more reliable, more customer-oriented). Also, the correlations and patterns found manually can further contribute to creating algorithms for control applications.

Machine learning and the models ML generates. With machine learning, there is an opportunity to create more precise and more efficient models for control applications. Models are regularly updated (for example, once in a week or once in a month) based on the historical data accumulated in a big data warehouse. When the applicability and efficiency of new models are tested and approved by data analysts, new models are used by control applications.

Control applications send automatic commands and alerts to actuators, for example:

- Windows of a smart home can receive an automatic command to open or close depending on the forecasts taken from the weather service.
- When sensors show that the soil is dry, watering systems get an automatic command to water plants.
- Sensors help monitor the state of industrial equipment, and in case of a pre-failure situation, an IoT system generates and sends automatic notifications to

field engineers.

The commands sent by control apps to actuators can be also additionally stored in a big data warehouse. This may help investigate problematic cases (for example, a control app sends commands, but they are not performed by actuators – then connectivity, gateways and actuators need to be checked). On the other side, storing commands from control apps may contribute to security, as an IoT system can identify that some commands are too strange or come in too big amounts which may evidence security breaches (as well as other problems which need investigation and corrective measures).

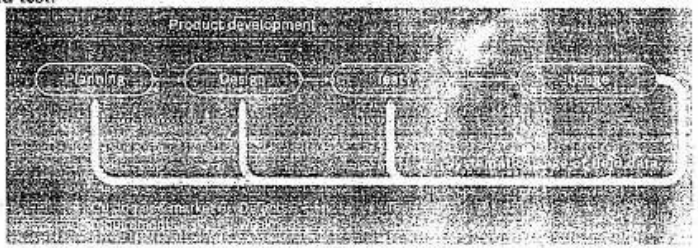
Control applications can be either rule-based or machine-learning based. In the first case, control apps work according to the rules stated by specialists. In the second case, control apps are using models which are regularly updated (once in a week, once in a month depending on the specifics of an IoT system) with the historical data stored in a big data warehouse.

Although control apps ensure better automation of an IoT system, there should be always an option for users to influence the behavior of such applications (for example, in cases of emergency or when it turns out that an IoT system is badly tuned to perform certain actions).

User applications: Are a software component of an IoT system which enables the connection of users to an IoT system and gives the options to monitor and control their smart things (while they are connected to a network of similar things, for example, homes or cars and controlled by a central system). With a mobile or web app, users can monitor the state of their things, send commands to control applications, set the options of automatic behavior (automatic notifications and actions when certain data comes from sensors).

b. Write explanatory note on IOT Data Management. (06 Marks)

Ans. IoT data management enables businesses to discover usage patterns. It also challenges assumptions made during design and development phases, identifying weaknesses in connected devices. In other words – it helps create the best connected products possible. Before the product is released, IoT data management allows to conduct a field test.



Source: Bosch Software Innovations

Armed with this data, we can improve design and create a higher-quality product that offers the best user experience. For example, an automated vehicle manufacturer can identify how various parts and components are used, and assess what conditions

they can with stand. When we consider that vehicle recall costs can run into millions in compensation claims (not to mention the cost to your reputation), this is a no-brainer. Collecting field data is also an important step post-launch. we can provide continuous product improvements with software updates and get important insights for your next version. Throughout the product lifetime, these insights will support the development process of new products and additional iterations.

Module - 2

3. a. What are Smart objects in IOT? Explain (06 Marks)

Ans. The concept of smart in IoT is used for physical objects that are active, digital, networked, can operate to some extent autonomously, reconfigurable and has local control of the resources. The smart objects need energy, data storage, etc. A **smart object** is an object that enhances the interaction with other smart objects as well as with people also. The world of IoT is the network of interconnected heterogeneous objects (such as smart devices, smart objects, sensors, actuators, RFID, embedded computers, etc.) uniquely addressable and based on standard communication protocols. In a day to day life, people have a lot of object with internet or wireless or wired connection. Such as:

- Smartphone
- Tablets
- TV computer

These objects can be interconnected among them and facilitate our daily life (smart home, smart cities) no matter the situation, localization, accessibility to a sensor, size, scenario or the risk of danger.

Smart objects are utilized widely to transform the physical environment around us to a digital world using the Internet of things (IoT) technologies. A smart object carries blocks of application logic that make sense for their local situation and interact with human users. A smart object sense, log, and interpret the occurrence within themselves and the environment, and intercommunicate with each other and exchange information with people.

The work of smart object has focused on technical aspects (such as software infrastructure, hardware platforms, etc.) and application scenarios. Application areas range from supply-chain management and enterprise applications (home and hospital) to healthcare and industrial workplace support. As for human interface aspects of smart-object technologies are just beginning to receive attention from the environment.

b. What are Sensor Networks in IOT? Mention the characteristics of IOT. (10 Marks)

Ans. A Wireless Sensor Network is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of

computing & processing. Nodes are the tiny computers, which work jointly to form the networks.

The sensor node is a multi-functional, energy efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives. The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor n/ws, Ad Hoc networks will have fewer nodes without any structure.

Wireless Sensor Network Architecture

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network.

Characteristics of Wireless Sensor Network

The characteristics of WSN include the following.

- The consumption of Power limits for nodes with batteries
- Capacity to handle with node failures
- Some mobility of nodes and Heterogeneity of nodes
- Scalability to large scale of distribution
- Capability to ensure strict environmental conditions
- Simple to use
- Cross-layer design

Advantages of Wireless Sensor Networks

The advantages of WSN include the following

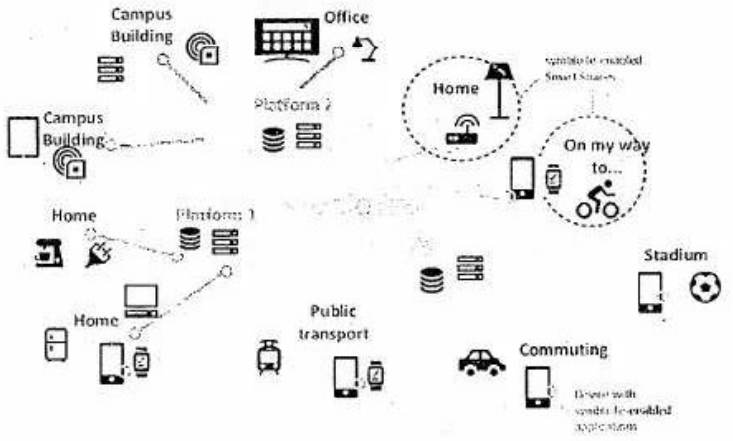
- Network arrangements can be carried out without immovable infrastructure.
- Apt for the non-reachable places like mountains, over the sea, rural areas and deep forests.
- Flexible if there is a casual situation when an additional workstation is required.
- Execution pricing is inexpensive.
- It avoids plenty of wiring.
- It might provide accommodations for the new devices at any time.
- It can be opened by using a centralized monitoring.

OR

4. a. How do we connect Smart Objects in IOT? Explain (08 Marks)

Ans. In a world of smart networked devices, wearables, sensors and actuators, transparent and secure access to and usage of the available resources across various IoT domains is crucial to satisfy the needs of an increasingly connected society. The current IoT ecosystem is however fragmented: a series of vertical solutions exist today which,

on the one hand, integrate connected objects within local environments using purpose-specific implementations and, on the other hand, connect smart spaces with a back-end cloud hosting dedicated often proprietary software components. **symbIoTe (symbiosis of smart objects across IoT environments)** comes to remedy this fragmented environment by providing an *abstraction layer* for a "unified view" on various platforms and their resources so that platform resources are transparent to application designers and developers. In addition, symbIoTe also chooses a challenging task to implement *IoT platform federations* so that they can securely interoperate, collaborate and share resources for the mutual benefit, and what is more, support the migration of smart objects between various IoT domains and platforms, i.e., *"smart object roaming"*. symbIoTe will achieve all of the above by designing and implementing an *Open Source mediation prototype*. In light of the above, symbIoTe opens up the potential for innovative business models that are incrementally deployable. This is especially important for SMEs who are symbIoTe's primary target group. Moreover, symbIoTe removes the strict separation between IoT islands to create an environment which i) has significant impact on the market since it bridges individual efforts and investments, ii) is attractive for a heterogeneous user group, iii) matches the dynamicity of modern life due to ease of use and iv) is helpful for various business, home and public infrastructure use cases.



b. What are the network technologies for IOT connectivity? (08 Marks)

Ans. The 3 main network technologies for IoT Connectivity are:

1. Standard Wireless Access – WiFi, 2G, 3G and standard LTE.
2. Private Long Range – LoRA based platform, Zigbee, and SigFox.
3. Mobile IoT Technologies – LTE-M, NB-IoT, and EC-GSM-IoT

There is no doubt that IoT is driving a lot of changes in connectivity (among many

other infrastructure technologies). The rule that connected devices impose over networking technologies is not the same as in our mobile phones..

Standard Wireless Access – WiFi, 2G, 3G and standard LTE

This is a no-brainer move. There are already plenty of devices that use this, such as:

- Smart-TVs
- Gaming consoles
- Panic buttons
- Video surveillance
- eHealth
- Fleet tracking
- Industrial IoT

It's an "obvious choice" for providers and consumers to continue using their current internet access (Wi-Fi, 2G, 3G, LTE, etc) as the primary network option for their home appliances. As always, there is a catch, the power consumption is quite a thing for cordless devices. Most devices using this network access are statically connected to a power outlet (or big batteries). In case of using a mobile network, another constraint is that their data plan acquired was thought for phones. This way it's quite expensive if you are thinking in multiples devices per user.

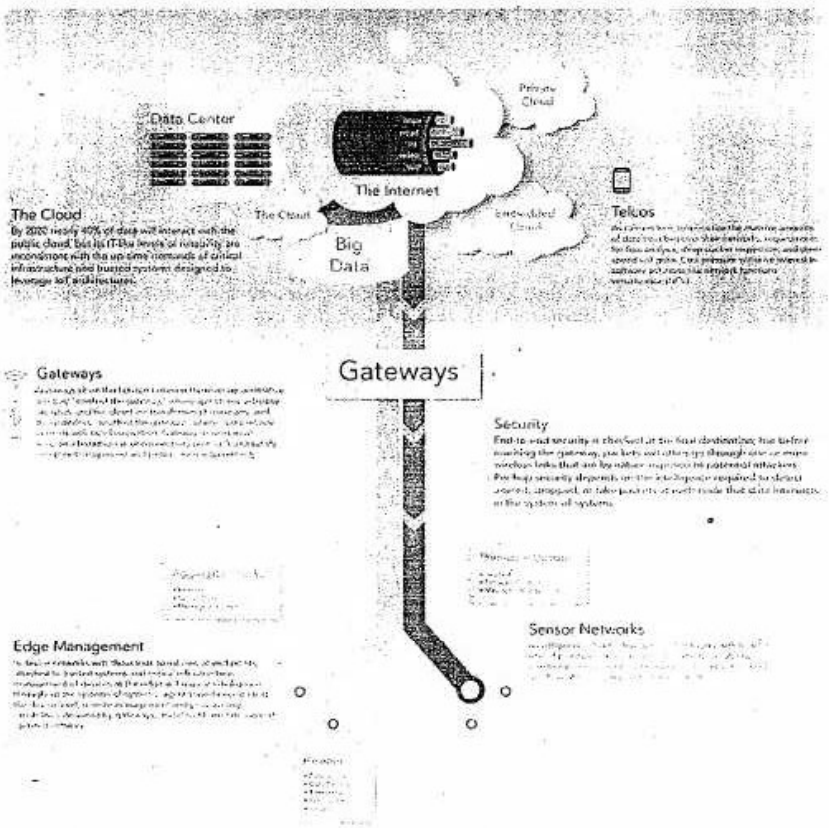
Private Long Range – LoRA based platform, Zigbee, and SigFox

The requirements of low power connectivity opened a window to private companies to develop new networks with that specific constraint at their core which are IoT native. These private wireless networks are used for the specific proprietary network. It's also to deploy a network which allows third-party devices to connect and build an ecosystem.The three leading technologies in this area are, LoRAWAN, Zigbee. and SigFox.

Module - 3

5. a. Explain the business case towards IP. (08 Marks)

Ans. Much of the technology needed for the Internet of Things (IoT) has been available for some time, but connecting a world's worth of devices to the cloud requires more than just an Internet connection. For IoT deployments to be successful, business models and pain points for players on both the device side and network side must be identified, followed by solutions that can collect and analyze data securely and efficiently.



b. What are Light Weight Application Layer protocols (08 Marks)

Ans. Along with physical and MAC layer protocols, we also need application layer protocols for IoT networks. These lightweight protocols need to be able to carry application messages, while simultaneously reducing power as far as possible. OMA Lightweight M2M (LWM2M) is one such protocol. It defines the communication protocol between a server and a device. The devices often have limited capabilities and are thus referred to as constrained devices. The main aims of the OMA protocol are as follows:(1)Remote device management.(2)Transferring service data/ information between different nodes in the LWM2M network. All the protocols in this class treat all the network resources as objects. Such resources can be created, deleted, and remotely configured. These devices have their unique limitations and can use different kinds of protocols for internally representing information. The LWM2M protocol abstracts all of this away and provides a convenient interface to send messages between a generic LWM2M server and a distributed set of LWM2M

clients. This protocol is often used along with CoAP (Constrained Application Protocol). It is an application layer protocol that allows constrained nodes such as sensor motes or small embedded devices to communicate across the Internet. CoAP seamlessly integrates with HTTP, yet it provides additional facilities such as support for multicast operations. It is ideally suited for small devices because of its low overhead and parsing complexity and reliance on UDP rather than TCP.

OR

6. a. Explain the application protocols for IP. (12 Marks)

Ans. Application layer protocols founded on TCP and UDP solve the communication challenges faced in an IoT project. The TCP protocol enables the XMPP, MQTT and REST/HTTP communication protocols. The UDP protocol enables DDSI and there are DDSI implementations on TCP/IP. Device and data storage server communication is enabled by XMPP and MQTT protocols that are enabled by TCP/IP. The RESTful API supported by HTTP enables client/server communication. In subsequent sections, the communication protocols will be discussed in detail.

The message queue telemetry transport (MQTT): – is a machine to machine architecture developed to enable lightweight connectivity. MQTT supports publish/subscribe over TCP. TCP minimizes the risk of data loss and brings in stream simplicity and reliability. The publish/service protocol is advantageous in an IoT environment because there is no requirement on clients to request updates which minimizes bandwidth, battery and computational requirements. Due to the advantages identified MQTT is suitable for home automation and mobile communication. MQTT is laid out in a star architecture where all devices connect to a common server. The server is referred to as a broker and TCP enables communication between a server and a client. Security is enforced through a user name and a password in a similar way to HTTPS.

MQTT offers flexibility in quality by allowing three levels of quality enforcement which are listedbelow:

- The first option is sending a message without an acknowledgment requirement
- The second option is sending a message once and requiring an acknowledgment
- The third option is requiring only one delivery through a handshake mechanism

The constrained application protocol (CoAP): – uses request/response to enable communication in recourse-constrained environments. Because the design of CoAP is a subset of HTTP interoperability between CoAP and HTTP is possible. CoAP is implemented over UDP to minimize its footprint. UDP is preferable over TCP because UDP minimizes bandwidth and overhead as compared to TCP. Because of the unreliability of UDP the design of CoAP included reliability. Every packet has a header that specifies message type and quality level required. The message types that can be specified are listed below.

- A confirmable message type is sent synchronously or asynchronously and an acknowledgment isrequired.
- A non-confirmable message does not require acknowledgment.
- An acknowledgment message type requires confirmation of a processed message.

- In a reset message type confirmation of a message that has not been processed is needed.

CoAP lacks security and the solution to this limitation is the datagram transport layer security (DTLS) which is the equivalent of TLS securing TCP. DTLS has limitations that reduce its suitability in an IoT environment. DTLS lacks support for multicast which is a key advantage of CoAP relative to other protocols. DTLS handshakes place a heavy burden on network and device battery which reduces usefulness of battery powered devices that are central to success of IoT.

Another application layer protocol is extensible messaging and presence protocol (XMPP). The protocol was designed to facilitate chat and messaging. Although XMPP is not suitable in other areas IoT is one area that would benefit from XMPP. Asynchronous and synchronous publish/subscribe over TCP. It is the publish/subscribe approach that makes XMPP better that CoAP in IoT applications. The disadvantage of XMPP is use of XML which increases computational and power use because of XML parsing. XMPP is excellent in supporting near real time because of low latency and small footprint in messaging.

Representational state transfer (REST): – enables synchronous request/response over HTTP. Caching and authentication among other HTTP features can be used in REST. The accept HTTP header specifies the data format as XML or JSON. REST can be implemented in machine to machine, smartphone and tablet environments which have made it important in IoT. The disadvantage of REST is difficulty in implementation.

The advanced message queuing protocol (AMQP): – enables asynchronous publish/subscribe approach to communication over TCP but other transport protocols can be used. Reliability is flexible with three delivery levels which are listed below.

- A message is sent only once when a delivery or failure happens.
- There is a guarantee of one or more message delivery.
- There is a guarantee a message will only be delivered once.

Security in AMQQ is implemented using TLS/SSL over TCP.

When selecting the application layer protocol to use in an IoT, the following factors need to be considered:

- Bandwidth requirement
- Data latency
- Reliability
- Memory and code footprint

b. Briefly describe the IOT Application transport methods. (04 Marks)

Ans. IOT Application Transport methods are HTTP(s) and Websockets which are some of the common existing standards, which can be used to deliver XML or JavaScript Object Notation (JSON) in the payload. JSON provides an abstraction layer for Web developers to create a stateful Web application with a persistent connection to a Web server.

1) HTTP : HTTP is the foundation of the client-server model used for the Web. The more secure method to implement HTTP is to include only a client in your IoT device, not a server.

2) WebSocket: WebSocket is a protocol that provides full-duplex communication over a single TCP connection between client and server. It is part of the HTML 5 specification. The WebSocket standard simplifies much of the complexity around bi-directional Web communication and connection management.

3) XMPP: XMPP is a good example of an existing Web technology finding new use in the IoT space. XMPP has its roots in instant messaging and presence information. It has expanded into signaling for VoIP, collaboration, lightweight middleware, content syndication, and generalized routing of XML data. It is a contender for mass scale management of consumer white goods such as washers, dryers, refrigerators, and so on.

4) CoAP: The Constrained Application Protocol (CoAP) was designed by the IETF for use with low-power and constrained networks. CoAP is a RESTful protocol. It is semantically aligned with HTTP, and even has a one-to-one mapping to and from HTTP. CoAP is a good choice of protocol for devices operating on battery or energy harvesting.

5) MQTT: MQ Telemetry Transport (MQTT) is an open source protocol for constrained devices and low-bandwidth, high-latency networks. It is a publish/subscribe messaging transport that is extremely lightweight and ideal for connecting small devices to constrained networks.

Module - 4

7. a. Explain briefly Big data analytics tools and technology (12 Marks)

Ans. Big data analytics is the process of extracting useful information by analysing different types of big data sets. Big data analytics is used to discover hidden patterns, market trends and consumer preferences, for the benefit of organizational decision making. There are several steps and technologies involved in big data analytics.

Data Acquisition

Data acquisition has two components: identification and collection of big data. Identification of big data is done by analyzing the two natural formats of data—born digital and born analogue.

Born Digital Data

It is the information which has been captured through a digital medium, e.g. a computer or smartphone app, etc. This type of data has an ever expanding range since systems keep on collecting different kinds of information from users. Born digital data is traceable and can provide both personal and demographic business insights. Examples include Cookies, Web Analytics and GPS tracking.

Born Analogue Data

When information is in the form of pictures, videos and other such formats which relate to physical elements of our world, it is termed as analogue data. This data requires conversion into digital format by using sensors, such as cameras, voice recording, digital assistants, etc. The increasing reach of technology has also raised the rate at which traditionally analogue data is being converted or captured through digital mediums.

The second step in the data acquisition process is collection and storage of data sets identified as big data. Since the archaic DBMS techniques were inadequate for managing big data, a new method is used for collecting and storing big data. The process is called MAD—magnetic, agile and deep. Since, managing big data requires a significant amount of processing and storage capacity, creating such systems is out-of-reach for most entities which rely on big data analytics. Thus, the most common solutions for big data processing today are based on two principles—distributed storage and Massive Parallel Processing a.k.a. MPP. Most of the high-end Hadoop platforms and specialty appliances use MPP configurations in their system.

Non-relational Databases

The databases that store these massive data sets have also evolved in how and where the data is stored. JavaScript Object Notation or JSON is the preferred protocol for saving big data nowadays. Using JSON, the tasks can be written in the application layer and allow better cross-platform functionalities. Thus enabling, agile development of scalable and flexible data solutions for the devs. Many companies are using it as a replacement of XML as a way of transmitting structured data between the server and web application.

In-memory Database Systems

These database storage systems are designed to overcome one of the major hurdles in the way of big data processing—the time taken by traditional databases to access and process information. IMDB systems store the data in the RAM of big data servers, therefore, drastically reducing the storage I/O gap. Apache Spark is an example of IMDB systems. VoltDB, NuoDB and IBM solidDB are some more examples of the same.

Hybrid Data Storage and Processing Systems—Apache Hadoop

Apache Hadoop is a hybrid data storage and processing system which provides scalability and speed at reasonable costs for mid and small-scale businesses. It uses a Hadoop Distributed File System (HDFS) for storing large files across multiple systems known as cluster nodes. Hadoop has a replication mechanism to ensure smooth operation even during instances of individual node failures. Hadoop uses Google's MapReduce parallel programming as its core. The name originates from 'Mapping' and 'Reduction' of functional programming languages in its algorithm for big data processing. MapReduce works on the premise of increasing the number of functional nodes over increasing processing power of individual nodes. Moreover, Hadoop can be run using readily available hardware which has sped up its development and popularity, significantly.

Data Mining

It is a recent concept which is based on contextual analysing of big data sets to discover the relationship between separate data items. The objective is to use a single data set for different purposes by different users. Data mining can be used for reducing costs and increasing revenues.

b. **What do you mean by Edge streaming analytics? Explain** **(04 Marks)**

Ans. Azure Stream Analytics (ASA) on IoT Edge empowers developers to deploy near-real-time analytical intelligence closer to IoT devices so that they can unlock the full value of device-generated data. Azure Stream Analytics is designed for low latency, resiliency, efficient use of bandwidth, and compliance. Enterprises can now deploy control logic close to the industrial operations and complement Big Data analytics done in the cloud.

Azure Stream Analytics on IoT Edge runs within the Azure IoT Edge framework. Once the job is created in ASA, you can deploy and manage it using IoT Hub.

OR

8. a. **How IOT Security is different from Physical and conventional IT Security? Explain.** **(06 Marks)**

Ans. **1. Lifecycle mismatch**

Many types of physical objects — buildings, automobiles, refrigerators, light switches — last a long time, decades even. They typically require maintenance, but they're often not replaced until the repair bills get too high or they just don't work. We certainly don't expect to replace them because a manufacturer decided not to support them after five years.

Yet much of the software involved in IoT is intended to be disposable. There may be no provisions for upgrading client devices at all. Software support for even relatively expensive consumer devices is usually just on the order of a few years.

From a security perspective, this means otherwise functional devices are likely to be exposed to unpatched vulnerabilities as they get older.

2. General-purpose extensible devices

If these network-connected systems used specialized hardware and software to operate and communicate, outdated software wouldn't necessarily be a major issue. It would likely be hard to force such devices to take actions they weren't originally designed to do.

However, in practice, it's very common for IoT devices to effectively be general-purpose computers running open source operating systems and network stacks. There are good reasons for this; among other things, it's easier (at least in principle) to update them and add new capabilities over time. However, it also means that an attacker who gains control of a device has more options to wreak havoc.

3. Bad economic incentives

None of the above is unfixable. We keep industrial equipment running for decades. Software vendors, including my employer, offer a variety of extended life support options for subscription products. These models work because customers are willing to pay for ongoing maintenance and support at levels where it's profitable for vendors to supply them.

Those same incentives aren't in place when you buy a light switch, or perhaps even a vehicle. No consumer is likely to pay for an ongoing light switch contract. Some may do so for cars, but it's not common after the initial warranty period. As a result, there are no incentives for most device makers to continue supporting what they've

sold beyond a fairly short window.

4. Connected by default

Vulnerability to attackers who connect to an IoT device or gateway wouldn't matter so much if making that connection were difficult or impossible. But increasingly it is not. The norm is to connect to networks, usually wireless networks, and often public networks. Even when there's no compelling reason to do so.

It's long been recognized that protecting computer systems against intruders who have gained physical access can be extremely challenging. (Witness breaches at the NSA and elsewhere.) However, pervasive and routine network access introduces many of the same threat vectors. Certainly it creates a far greater attack surface than physically isolated systems.

5. Ecosystem effects

When general-purpose, network-connected computers are breached, it doesn't just affect the target of the attack.

Data breaches can affect millions of customers when sensitive information is stolen; this applies whether we're talking IoT or more conventional IT systems. IoT multiplies the issue by collecting more and more ambient data that people may not even be aware is being collected.

Ecosystem damage can go beyond data. The Mirai botnet's DDoS attackcaused significant disruption to the internet as a whole. It resulted from outdated versions of Linux on webcams being turned into remote-controlled bots for large-scale network attacks.

6. Common widespread failure modes

Speaking at the Open Source Leadership Summit earlier this year, security expert Bruce Schneier noted that computers and networks fail in a different way than non-computerized systems. "You worry about crashing all the cars. You're concerned about the five sigma guy, not the average guy. It doesn't happen in lock picking in the same way," he said, because no matter how skilled, one person can only break into one physical building at a time.

I mentioned the Mirai botnet earlier. But it's the nature of IoT and connected systems more broadly that vulnerabilities and attacks usually affect many systems. Of course, individual attacks can still lead to data breaches or the shutdown of a critical system. But even breaches that would be relatively innocuous in isolation can cause serious failures in systems like the power grid if multiplied by a thousand or a million. Scale matters.

7. Actuators can affect our environment

We've seen how IoT can differ in scale, connectedness and vendor support from more conventional IT systems. But if I had to pick one aspect of IoT that's fundamentally different, it's this one: IoT is not read-only.

Schneier calls it "an internet that affects the world."

Software already controls many critical systems or directly tells humans what to do. But the degree to which IoT is replacing manual and disconnected controls pervasively and by default is striking.

That IoT can take physical actions may not really change its security model, but it certainly raises the stakes.

We prioritize features. We prioritize low prices. We prioritize today. We do notprioritize security over a product lifecycle that may span decades. In devices that have the power to affect the physical world.

All IoT Agenda network contributors are responsible for the content and accuracy of their posts. Opinions are of the writers and do not necessarily convey the thoughts of IoT Agenda.

b. What is OCTAVE and FAIR explain? (10 Marks)

Ans. Within the industrial environment, there are a number of standards, guidelines, and best practices available to help understand risk and how to mitigate it. IEC 62443 is the most commonly used standard globally across industrial verticals. It consists of a number of parts, including 62443-3-2 for risk assessments, and 62443-3-3 for foundational requirements used to secure the industrial environment from a networking and communications perspective. Also, ISO 27001 is widely used for organizational people, process, and information security management. In addition, the National Institute of Standards and Technology (NIST) provides a series of documents for critical infrastructure, such as the NIST Cybersecurity Framework (CSF). In the utilities domain, the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) has legally binding guidelines for North American utilities, and IEC 62351 is the cybersecurity standard for power utilities.

The key for any industrial environment is that it needs to address security holistically and not just focus on technology. It must include people and processes, and it should include all the vendor ecosystem components that make up a control system.

In this section, we present a brief review of two such risk assessment frameworks:

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) from the Software Engineering Institute at Carnegie Mellon University
- FAIR (Factor Analysis of Information Risk) from The Open Group

These two systems work toward establishing a more secure environment but with two different approaches and sets of priorities. Knowledge of the environment is key to determining security risks and plays a key role in driving priorities.

OCTAVE

OCTAVE has undergone multiple iterations. The version this section focuses on is OCTAVE Allegro, which is intended to be a lightweight and less burdensome process to implement. Allegro assumes that a robust security team is not on standby or immediately at the ready to initiate a comprehensive security review. This approach and the assumptions it makes are quite appropriate, given that many operational technology areas are similarly lacking in security-focused human assets. Figure 8 illustrates the OCTAVE Allegro steps and phases.

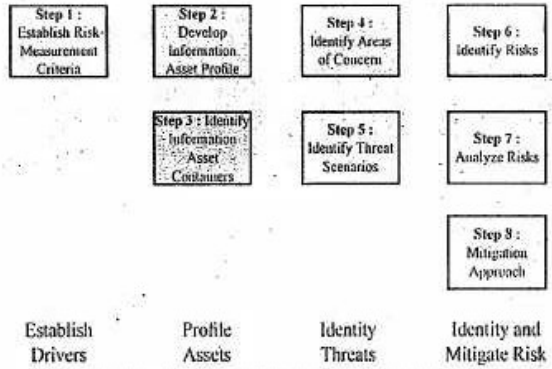


Figure 8 *OCTAVE Allegro Steps and Phases*

The first step of the OCTAVE Allegro methodology is to establish a risk measurement criterion. OCTAVE provides a fairly simple means of doing this with an emphasis on impact, value, and measurement. The point of having a risk measurement criterion is that at any point in the later stages, prioritization can take place against the reference model. (While OCTAVE has more details to contribute, we suggest using the FAIR model, described next, for risk assessment.)

The second step is to develop an information asset profile. This profile is populated with assets, a prioritization of assets, attributes associated with each asset, including owners, custodians, people, explicit security requirements, and technology assets. It is important to stress the importance of process. Certainly, the need to protect information does not disappear, but operational safety and continuity are more critical.

Within this asset profile, process are multiple substages that complete the definition of the assets. Some of these are simply survey and reporting activities, such as identifying the asset and attributes associated with it, such as its owners, custodians, human actors with which it interacts, and the composition of its technology assets. There are, however, judgment-based attributes such as prioritization. Rather than simply assigning an arbitrary ranking, the system calls for a justification of the prioritization. With an understanding of the asset attributes, particularly the technical components, appropriate threat mitigation methods can be applied. With the application of risk assessment, the level of security investment can be aligned with that individual asset.

The third step is to identify information asset containers. Roughly speaking, this is the range of transports and possible locations where the information might reside. This references the compute elements and the networks by which they communicate. However, it can also mean physical manifestations such as hard copy documents or even the people who know the information. Note that the operable target here is information, which includes data from which the information is derived.

In OCTAVE, the emphasis is on the container level rather than the asset level. The value is to reduce potential inhibitors within the container for information operation. In the OT world, the emphasis is on reducing potential inhibitors in the containerized operational space. If there is some attribute of the information that is endemic to it, then the entire container operates with that attribute because the information is the defining element. In some cases this may not be true, even in IT environments. Discrete atomic-level data may become actionable information only if it is seen in the context of the rest of the data. Similarly, operational data taken without knowledge of the rest of the elements may not be of particular value either.

The fourth step is to identify areas of concern. At this point, we depart from a data flow, touch, and attribute focus to one where judgments are made through a mapping of security-related attributes to more business-focused use cases. At this stage, the analyst looks to risk profiles and delves into the previously mentioned risk analysis. It is no longer just facts, but there is also an element of creativity that can factor into the evaluation. History both within and outside the organization can contribute. References to similar operational use cases and incidents of security failures are reasonable associations.

Closely related is the fifth step, where threat scenarios are identified. Threats are broadly (and properly) identified as potential undesirable events. This definition means that results from both malevolent and accidental causes are viable threats. In the context of operational focus, this is a valuable consideration. It is at this point that an explicit identification of actors, motives, and outcomes occurs. These scenarios are described in threat trees to trace the path to undesired outcomes, which, in turn, can be associated with risk metrics.

At the sixth step risks are identified. Within OCTAVE, risk is the possibility of an undesired outcome. This is extended to focus on how the organization is impacted. For more focused analysis, this can be localized, but the potential impact to the organization could extend outside the boundaries of the operation.

The seventh step is risk analysis, with the effort placed on qualitative evaluation of the impacts of the risk. Here the risk measurement criteria defined in the first step are explicitly brought into the process.

Finally, mitigation is applied at the eighth step. There are three outputs or decisions to be taken at this stage. One may be to accept a risk and do nothing, other than document the situation, potential outcomes, and reasons for accepting the risk. The second is to mitigate the risk with whatever control effort is required. By walking back through the threat scenarios to asset profiles, a pairing of compensating controls to mitigate those threat/risk pairings should be discoverable and then implemented. The final possible action is to defer a decision, meaning risk is neither accepted nor mitigated. This may imply further research or activity, but it is not required by the process.

OCTAVE is a balanced information-focused process. What it offers in terms of discipline and largely unconstrained breadth, however, is offset by its lack of security specificity. There is an assumption that beyond these steps are seemingly means of

identifying specific mitigations that can be mapped to the threats and risks exposed during the analysis process.

FAIR

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. For many operational groups, it is a welcome acknowledgement of existing contingency planning. Unlike with OCTAVE, there is a significant emphasis on naming, with risk taxonomy definition as a very specific target.

FAIR places emphasis on both unambiguous definitions and the idea that risk and associated attributes are measurable. Measurable, quantifiable metrics are a key area of emphasis, which should lend itself well to an operational world with a richness of operational data.

At its base, FAIR has a definition of risk as the probable frequency and probable magnitude of loss. With this definition, a clear hierarchy of sub-elements emerges, with one side of the taxonomy focused on frequency and the other on magnitude.

Loss even frequency is the result of a threat agent acting on an asset with a resulting loss to the organization. This happens with a given frequency called the threat event frequency (TEF), in which a specified time window becomes a probability. There are multiple sub-attributes that define frequency of events, all of which can be understood with some form of measurable metric. Threat event frequencies are applied to a vulnerability. *Vulnerability* here is not necessarily some compute asset weakness, but is more broadly defined as the probability that the targeted asset will fail as a result of the actions applied. There are further sub-attributes here as well.

The other side of the risk taxonomy is the probable loss magnitude (PLM), which begins to quantify the impacts, with the emphasis again being on measurable metrics. The FAIR specification makes it a point to emphasize how ephemeral some of these cost estimates can be, and this may indeed be the case when information security is the target of the discussion. Fortunately for the OT operator, a significant emphasis on operational efficiency and analysis makes understanding and quantifying costs much easier.

FAIR defines six forms of loss, four of them externally focused and two internally focused. Of particular value for operational teams are productivity and replacement loss. Response loss is also reasonably measured, with fines and judgments easy to measure but difficult to predict. Finally, competitive advantage and reputation are the least measurable.

Module - 5

9. a. What do you setup Arduino UNO? (06 Marks)

Ans. setup() - The setup() function is called when a sketch starts. Use it to initialize variables, pin modes, start using libraries, etc. The setup function will only run once.

after each powerup or reset of the Arduino board.

Example

```
int buttonPin = 3;
void setup()
{
Serial.begin(9600);
pinMode(buttonPin, INPUT);
}
void loop()
{
// ...
}
```

b. Explain the IOT network protocol stack **(10 Marks)**

Ans. The Internet Engineering Task Force (IETF) has developed alternative protocols for communication between IoT devices using IP because IP is a flexible and reliable standard. The Internet Protocol for Smart Objects (IPSO) Alliance has published various white papers describing alternative protocols and standards for the layers of the IP stack and an additional adaptation layer, which is used for communication between smart objects.

(1) Physical and MAC Layer (IEEE 802.15.4). The IEEE 802.15.4 protocol is designed for enabling communication between compact and inexpensive low power embedded devices that need a long battery life. It defines standards and protocols for the physical and link (MAC) layer of the IP stack. It supports low power communication along with low cost and short range communication. In the case of such resource constrained environments, we need a small frame size, low bandwidth, and low transmit power.

Transmission requires very little power (maximum one milliwatt), which is only one percent of that used in WiFi or cellular networks. This limits the range of communication. Because of the limited range, the devices have to operate cooperatively in order to enable multihop routing over longer distances. As a result, the packet size is limited to 127 bytes only, and the rate of communication is limited to 250 kbps. The coding scheme in IEEE 802.15.4 has built in redundancy, which makes the communication robust, allows us to detect losses, and enables the retransmission of lost packets. The protocol also supports short 16-bit link addresses to decrease the size of the header, communication overheads, and memory requirements.

(2) Adaptation Layer. IPv6 is considered the best protocol for communication in the IoT domain because of its scalability and stability. Such bulky IP protocols were initially not thought to be suitable for communication in scenarios with low power wireless links such as IEEE 802.15.4.

6LoWPAN, an acronym for IPv6 over low power wireless personal area networks, is a very popular standard for wireless communication. It enables communication using IPv6 over the IEEE 802.15.4 protocol. This standard defines an adaptation layer between the 802.15.4 link layer and the transport layer. 6LoWPAN devices can

communicate with all other IP based devices on the Internet. The choice of IPv6 is because of the large addressing space available in IPv6. 6LoWPAN networks connect to the Internet via a gateway (WiFi or Ethernet), which also has protocol support for conversion between IPv4 and IPv6 as today's deployed Internet is mostly IPv4. IPv6 headers are not small enough to fit within the small 127 byte MTU of the 802.15.4 standard. Hence, squeezing and fragmenting the packets to carry only the essential information is an optimization that the adaptation layer performs.

Specifically, the adaptation layer performs the following three optimizations in order to reduce communication overhead:(i)Header compression 6loWPAN defines header compression of IPv6 packets for decreasing the overhead of IPv6. Some of the fields are deleted because they can be derived from link level information or can be shared across packets.(ii)Fragmentation: the minimum MTU size (maximum transmission unit) of IPv6 is 1280 bytes. On the other hand, the maximum size of a frame in IEEE 802.15.4 is 127 bytes. Therefore, we need to fragment the IPv6 packet. This is done by the adaptation layer.(iii)Link layer forwarding 6LoWPAN also supports mesh under routing, which is done at the link layer using link level short addresses instead of in the network layer. This feature can be used to communicate within a 6LoWPAN network.

(3) Network Layer. The network layer is responsible for routing the packets received from the transport layer. The IETF Routing over Low Power and Lossy Networks (ROLL) working group has developed a routing protocol (RPL) for Low Power and Lossy Networks (LLNs).

For such networks, RPL is an open routing protocol, based on distance vectors. It describes how a destination oriented directed acyclic graph (DODAG) is built with the nodes after they exchange distance vectors. A set of constraints and an objective function is used to build the graph with the best path. The objective function and constraints may differ with respect to their requirements. For example, constraints can be to avoid battery powered nodes or to prefer encrypted links. The objective function can aim to minimize the latency or the expected number of packets that need to be sent.

The making of this graph starts from the root node. The root starts sending messages to neighboring nodes, which then process the message and decide whether to join or not depending upon the constraints and the objective function. Subsequently, they forward the message to their neighbors. In this manner, the message travels till the leaf nodes and a graph is formed. Now all the nodes in the graph can send packets upwards hop by hop to the root. We can realize a point to point routing algorithm as follows. We send packets to a common ancestor, from which it travels downwards (towards leaves) to reach the destination.

To manage the memory requirements of nodes, nodes are classified into storing and nonstoring nodes depending upon their ability to store routing information. When nodes are in a nonstoring mode and a downward path is being constructed, the route information is attached to the incoming message and forwarded further till the root. The root receives the whole path in the message and sends a data packet along

with the path message to the destination hop by hop. But there is a trade-off here because nonstoring nodes need more power and bandwidth to send additional route information as they do not have the memory to store routing tables.

(4) Transport Layer. TCP is not a good option for communication in low power environments as it has a large overhead owing to the fact that it is a connection oriented protocol. Therefore, UDP is preferred because it is a connectionless protocol and has low overhead.

(5) Application Layer. The application layer is responsible for data formatting and presentation. The application layer in the Internet is typically based on HTTP. However, HTTP is not suitable in resource constrained environments because it is fairly verbose in nature and thus incurs a large parsing overhead. Many alternate protocols have been developed for IoT environments such as CoAP (Constrained Application Protocol) and MQTT (Message Queue Telemetry Transport).(a) Constrained Application Protocol: CoAP can be thought of as an alternative to HTTP. It is used in most IoT applications. Unlike HTTP, it incorporates optimizations for constrained application environments. It uses the EXI (Efficient XML Interchanges) data format, which is a binary data format and is far more efficient in terms of space as compared to plain text HTML/XML. Other supported features are built in header compression, resource discovery, autoconfiguration, asynchronous message exchange, congestion control, and support for multicast messages. There are four types of messages in CoAP: nonconfirmable, confirmable, reset (nack), and acknowledgement. For reliable transmission over UDP, confirmable messages are used. The response can be piggybacked in the acknowledgement itself. Furthermore, it uses DTLS (Datagram Transport Layer Security) for security purposes.(b)Message Queue Telemetry Transport: MQTT is a publish/subscribe protocol that runs over TCP. It was developed by IBM primarily as a client/server protocol. The clients are publishers/subscribers and the server acts as a broker to which clients connect through TCP. Clients can publish or subscribe to a topic. This communication takes place through the broker whose job is to coordinate subscriptions and also authenticate the client for security. MQTT is a lightweight protocol, which makes it suitable for IoT applications. But because of the fact that it runs over TCP, it cannot be used with all types of IoT applications. Moreover, it uses text for topic names, which increases its overhead.

MQTT-S/MQTT-SN is an extension of MQTT, which is designed for low power and low cost devices. It is based on MQTT but has some optimizations for WSNs as follows. The topic names are replaced by topic IDs, which reduce the overheads of transmission. Topics do not need registration as they are preregistered. Messages are also split so that only the necessary information is sent. Further, for power conservation, there is an offline procedure for clients who are in a sleep state. Messages can be buffered and later read by clients when they wake up. Clients connect to the broker through a gateway device, which resides within the sensor network and connects to the broker.

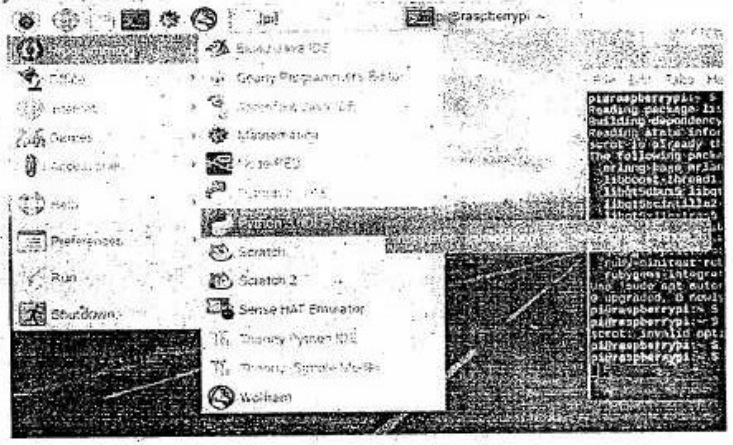
OR

10. a. How do you program raspberry pi with python? **(10 Marks)**

Ans. Python is a programming language that has recently become very popular—so popular, in fact, that it is now the fourth most popular language (according to the TIOBE index).Unlike other languages (C, C++, etc.), Python is an interpreted language, which means when a Python program is executed, an interpreter reads the Python instructions and then performs the desired action. The interpreter itself is written in CPU native instructions, but the Python program is not. This means Python programs can, in theory, run on ANY computer, so long as that computer has a Python interpreter. This makes Python a cross-platform language, which is one of the main reasons why it has become so popular. A program written on Windows does not need to be rewritten to work on a Mac or a Linux machine. It's also incredibly simple, easy to read, and powerful. It can write advanced programs, including graphical interfaces, networking, parallelism, and much more. Python is a productive language, resulting in faster program production and requiring less code and time. Since Linux has been written for the Pi (ARM core), the Python interpreter can run on it and, therefore, so can Python programs. So, how do we start with this wonderful programming language on the Pi?

Installing and Loading the IDE

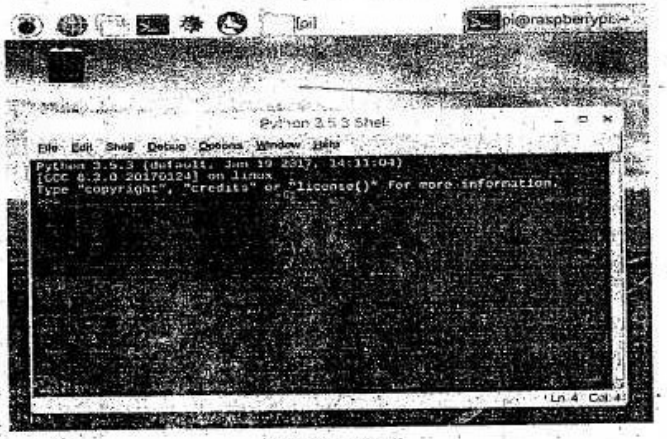
Raspbian, the default OS choice for the Raspberry Pi, should contain both Python 2 and 3, so loading Python should be easy to navigate through menu options. Firstly, click the top left Pi icon on the menu bar. Then navigate to "Programming" and click "Python 3 (IDEL)".



Loading Python 3 IDE

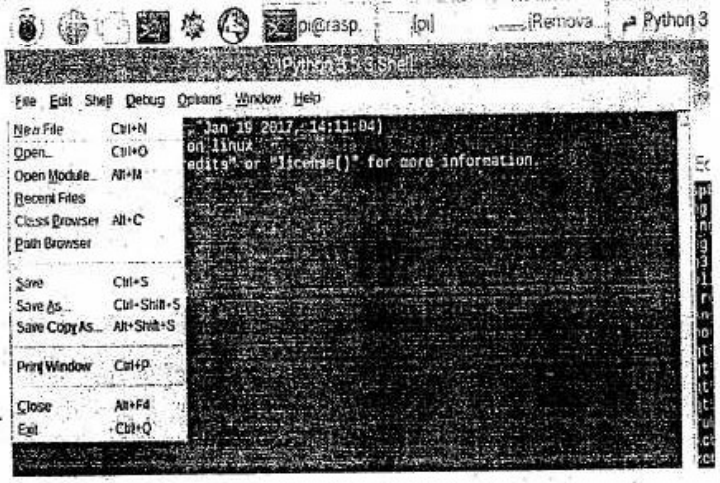
When Python 3 loads, the visible window is the shell, which has two main purposes:

1. **Entering Python commands:** some quick calculations
2. **Input/output for programs:** getting data from a user and displaying information



The main shell

The IDE also has a menu bar with many options, including file operations, editing, shell specific options ("Interrupt program" for example), program debugging, IDE options, and "Help". For now, we will only concern ourselves with creating a new file, which is done by clicking File > New File.



Creating a new file

CreatingFirst Program

Once the new window loads, we can finally enter our first Python program. To do this, enter the code as shown below into the window. Then, save the file.

```
name = ""
age = 0
currentYear = 0
```



```
yearBorn = 0
name = input("Enter your name: ")
age = int(input("Enter your max age this year: "))
currentYear = int(input("What is the current year? : "))
yearBorn = currentYear - age
print("You were born in the year " + str(yearBorn))
```

Running Our Program

With the code entered and the file saved, it's time to run the program. Running a Python program can be done in one of three ways: press F5 in the window with the program to run, go to the menu bar and click Run > Python Shell, or run the file via a terminal window as an argument for Python. For now, the easiest way is to simply press F5 in the window with the code. Once pressed, the code should return no errors, and the shell window should prompt for data.

b. Justify the statement "An IOT strategy for smarter cities". (06 Marks)

Ans. Smart transport applications can manage daily traffic in cities using sensors and intelligent information processing systems. The main aim of intelligent transport systems is to minimize traffic congestion, ensure easy and hassle-free parking, and avoid accidents by properly routing traffic and spotting drunk drivers. The sensor technologies governing these types of applications are GPS sensors for location, accelerometers for speed, gyroscopes for direction, RFIDs for vehicle identification, infrared sensors for counting passengers and vehicles, and cameras for recording vehicle movement and traffic. There are many types of applications in this area:(1) Traffic surveillance and management applications: vehicles are connected by a network to each other, the cloud, and to a host of IoT devices such as GPS sensors, RFID devices, and cameras. These devices can estimate traffic conditions in different parts of the city. Custom applications can analyze traffic patterns so that future traffic conditions can be estimated. They implemented a vehicle tracking system for traffic surveillance using video sequences captured on the roads. Traffic congestion detection can also be implemented using smartphone sensors such as accelerometers and GPS sensors. These applications can detect movement patterns of the vehicle while the user is driving. Such kind of information is already being collected by Google maps and users are using it to route around potentially congested areas of the city.(2) Applications to ensure safety: smart transport does not only imply managing traffic conditions. It also includes safety of people travelling in their vehicles, which up till now was mainly in the hands of drivers. There are many IoT applications developed to help drivers become safer drivers. Such applications monitor driving behavior of drivers and help them drive safely by detecting when they are feeling drowsy or tired and helping them to cope with it or suggesting rest. Technologies used in such applications are face detection, eye movement detection, and pressure detection on the steering (to measure the grip of the driver's hands on the steering). A smartphone application, which estimates the driver's driving behavior using smartphone sensors such as the accelerometer, gyroscope, GPS, and camera, has been proposed by Eren

et al. It can decide whether the driving is safe or rash by analyzing the sensor data. (3)Intelligent parking management: in a smart transportation system, parking is completely hassle free as one can easily check on the Internet to find out which parking lot has free spaces. Such lots use sensors to detect if the slots are free or occupied by vehicles. This data is then uploaded to a central server.(4)Smart traffic lights: traffic lights equipped with sensing, processing, and communication capabilities are called smart traffic lights. These lights sense the traffic congestion at the intersection and the amount of traffic going each way. This information can be analyzed and then sent to neighboring traffic lights or a central controller. It is possible to use this information creatively. For example, in an emergency situation the traffic lights can preferentially give way to an ambulance. When the smart traffic light senses an ambulance coming, it clears the path for it and also informs neighboring lights about it. Technologies used in these lights are cameras, communication technologies, and data analysis modules. Such systems have already been deployed in Rio De Janeiro. (5)Accident detection applications: a smartphone application designed by White detects the occurrence of an accident with the help of an accelerometer and acoustic data. It immediately sends this information along with the location to the nearest hospital. Some additional situational information such as on-site photographs is also sent so that the first responders know about the whole scenario-and the degree of medical help that is required.

Eighth Semester B.E. Degree Examination,
CBCS - Model Question Paper - 2
INTERNET OF THINGS TECHNOLOGY

Time: 3 hrs. **Max. Marks:** 80

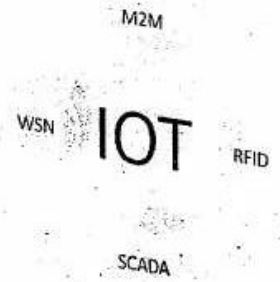
Note : ***Answer any FIVE full questions, selecting ONE full question from each module.***

Module - 1

1. a. Explain the four pillars of IOT &how are they interconnected with each other (10 Marks)

Ans. The four pillars of IoT are M2M, RFID, WSNs and SCADA (Supervisory Control and Data Acquisition).

- **M2M** uses devices to capture events, via a network connection to a central server, that translates the captured events into meaningful information.
- **RFID** uses radio waves to transfer data from an electronic tag attached to an object to a central system through a reader for the purpose of identifying and tracking the object.
- A **WSN** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions.
- **SCADA** is an autonomous system based on closed-loop control theory or a smart system or a CPS data connects, monitors, and controls equipment via network in a facility such as a plant or a building.



One of the common characteristics of the Internet of Things is that objects in a IoT world have to be **instrumented**, **interconnected**, before **anything** can be **intelligently** processed and used **anywhere**, **anytime**, **anyway**, and **anyhow**, which are the 5A and 3I characteristics.

Four Pillars and Their Relevance to the Network:

RFID	Yes	Some	No	Some
WSN	Yes	Some	No	Some
M2M	Some	Yes	No	Some
SCADA	Some	Some	Yes	Yes

1. Machine-to-Machine (M2M) communication:

Machine-to-Machine (M2M) communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. M2M is also named as Machine Type Communication (MTC) in 3GPP. It is different from the current communication models in the ways that it involves:

– new or different market scenarios
– lower costs and effort
– a potentially very large number of communicating terminals
– little traffic per terminal, in general

M2M communication could be carried over mobile networks (e.g. GSM-GPRS, CDMA EVDO networks). In the M2M communication, the role of mobile network is largely confined to serve as a transport network.

Some of the key features of M2M communication system are given below:

a. Low Mobility : M2M Devices do not move, move infrequently, or move only within a certain region

b. Time Controlled : Send or receive data only at certain pre-defined periods

c. Time Tolerant : Data transfer can be delayed

d. Packet Switched : Network operator to provide packet switched service with or without an MSISDN

e. Online small Data Transmissions: MTC Devices frequently send or receive small amounts of data.

f. Monitoring: Not intend to prevent theft or vandalism but provide functionality to detect the events

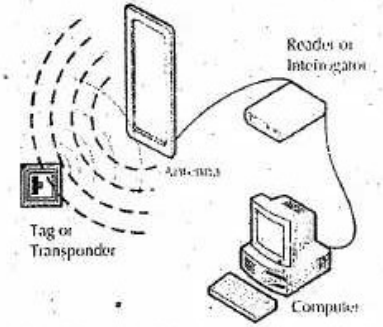
g. Low Power Consumption : To improve the ability of the system to efficiently service M2M applications

h. Location Specific Trigger : Intending to trigger M2M device in a particular area e.g. wake up the device

2. RFID : is the 2nd pillar of IOT.

RFID stands for **Radio Frequency IDentification** and it's a non-contact technology that's broadly used in many industries for tasks such as personnel tracking, access control, supply chain management, books tracking in libraries, tollgate systems and so on.

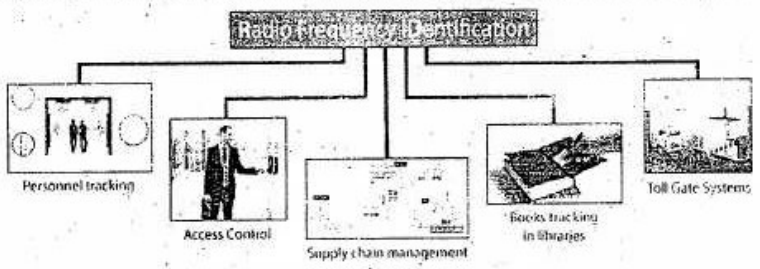
RFID uses radio waves produced by a **reader** to detect the presence of (then read the data stored on) an RFID **tag**. Tags are embedded in small items like cards, buttons, or tiny capsules.



The RFID reader consist of a radio frequency module, a control unit and an antenna coil which generates high frequency electromagnetic field. On the other hand, the tag is usually a passive component, which consist of just an antenna and an electronic microchip, so when it gets near the electromagnetic field of the transceiver, due to induction, a voltage is generated in its antenna coil and this voltage serves as power for the microchip. RFID Frequencies

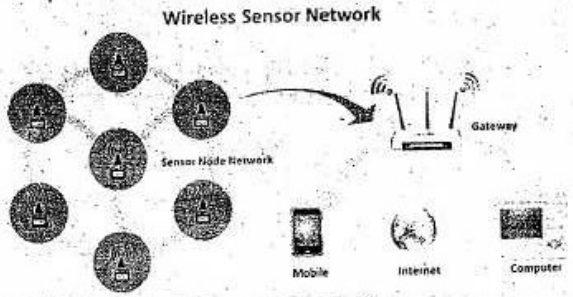
As well as active and passive systems, RFID systems can also be broken out into different frequencies.

Some frequencies and systems are designed to only read one tag at a time, while others can read multiple. Cost of readers can also vary wildly based the frequency rating of the modules. In prior years a reader capable of reading multiple tags was in the thousands of dollars, sometimes tens of thousands. These systems were unattainable for most hobbyists and prototypers. However, this is finally beginning to change, and multi-read capable readers are becoming much more affordable.



3. Wireless Sensor Network (Wsn):

WSN is the third pillar of IOT.



It's a collection of devices " sensor nodes" . They are small, inexpensive, with constrained power . They are organized in a cooperative network .They communicate wirelessly in multi hop routing . Heavily deployment. Changing network topology

WSN Definition

A sensor network is composed of a large number of sensor nodes that are densely deployed inside or very close to the phenomenonθ

random deploymentθ

self-organizing capabilitiesθ

Each node of the sensor networks consist of three subsystem:θ

Sensor subsystem: senses the environmentθ

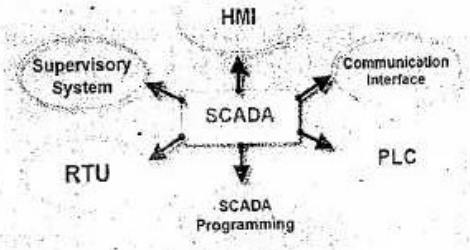
Processing subsystem: performs local computations on the sensed dataθ

Communication subsystem: responsible for message exchange with neighboring sensor nodesθ

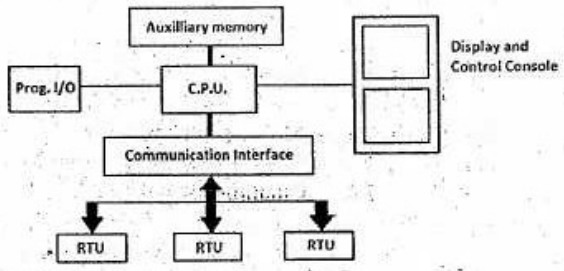
The features of sensor nodesθ

Limited sensing region, processing power, energyθ

4. Scada (Supervisory Control and Data Acquisition):



It is impossible to keep control and supervision on all industrial activities manually. Some automated tool is required which can control, supervise, collect data, analyses data and generate reports. A unique solution is introduced to meet all this demand is SCADA system.



(i) Human Machine Interface (HMI)

It is an interface which presents ***process data to a human operator***, and through this, the human operator monitors and controls the process.

(ii) Supervisory (computer) system

It gathers data on the process and sending commands (*or control*) to the process.

(iii) Remote Terminal Units (RTUs)

It connect to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.

(iv) Programmable Logic Controller (PLCs)

It is used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

(v) Communication infrastructure

It provides connectivity to the supervisory system to the Remote Terminal Units.

b. Explain the applications of IOT. **(06 Marks)**

Ans. Smart Home :

Whenever we think of IoT systems, the most important and efficient application that stands out is the smart home, ranking the highest IoT application on all channels. The number of people searching for smart homes increases every month by about 60,000 people. Another interesting thing is that the database of smart homes for IoT analytics includes 256 companies and startups. More companies are now actively involved in smart homes, as well as similar applications in the field. The estimated amount of funding for smart home startups exceeds $2.5 billion and growing at a rapid rate. The list of startups includes prominent startup company names, such as AlertMe or Nest, as well as a number of multinational corporations, like Philips, Haier, or Belkin.

Wearables

Just like smart homes, wearables remain a hot topic among potential IoT. Every year, consumers all across the globe await the release of the latest Apple smartwatch. Apart from this, there are plenty of other wearable devices that make our life easy, such as the Sony Smart B Trainer, LookSee bracelet, or the Myo gesture control.

Smart City

Smart cities, like its name suggests, is a big innovation and spans a wide variety of use cases, from water distribution and traffic management to waste management and environmental monitoring. The reason why it is so popular is that it tries to remove the discomfort and problems of people who live in cities. IoT solutions offered in the smart city sector solve various city-related problems, comprising of traffic, reducing air and noise pollution, and helping to make cities safer.

Smart Grids

Smart grids are another area of IoT technology that stands out. A smart grid basically promises to extract information on the behaviors of consumers and electricity suppliers in an automated fashion to improve the efficiency, economics, and reliability of electricity distribution. 41,000 monthly Google searches is a testament to this concept's popularity.

Industrial Internet

One way to think of the Industrial Internet is by looking at connected machines and devices in industries such as power generation, oil, gas, and healthcare. It also makes use of situations where unplanned downtime and system failures can result in life-threatening situations. A system embedded with the IoT tends to include devices such as fitness bands for heart monitoring or smart home appliances. These systems are functional and can provide ease of use but are not reliable because they do not typically create emergency situations if a downtime was to occur.

Connected Car

Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in communication to navigate in our complex world. It has the responsibility of making decisions with consistency, accuracy, and speed. It also has to be reliable. These requirements will become even more critical when humans give up control of the steering wheel and brakes to the autonomous vehicles that are being tested on our highways right now.

Connected Health (Digital Health/Telehealth/Telemedicine)

IoT has various applications in healthcare, which are from remote monitoring equipment to advance and smart sensors to equipment integration. It has the potential to improve how physicians deliver care and also keep patients safe and healthy. Healthcare IoT can allow patients to spend more time interacting with their doctors, which can boost patient engagement and satisfaction. From personal fitness sensors to surgical robots, IoT in healthcare brings new tools updated with the latest technology in the ecosystem that helps in developing better healthcare. IoT helps to revolutionize healthcare and provide pocket-friendly solutions for both the patient and healthcare professional.

Smart Retail

Retailers have started adopting IoT solutions and using IoT embedded systems across a number of applications that improve store operations, increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience. Through IoT physical retailers can compete against online

challengers more strongly. They can regain their lost market share and attract consumers into the store, thus making it easier for them to buy more while saving money.

Smart Supply Chain

Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit or helping suppliers exchange inventory information are some of the popular offerings. With an IoT enabled system, factory equipment that contains embedded sensors communicate data about different parameters, such as pressure, temperature, and utilization of the machine. The IoT system can also process workflow and change equipment settings to optimize performance.

Smart Farming

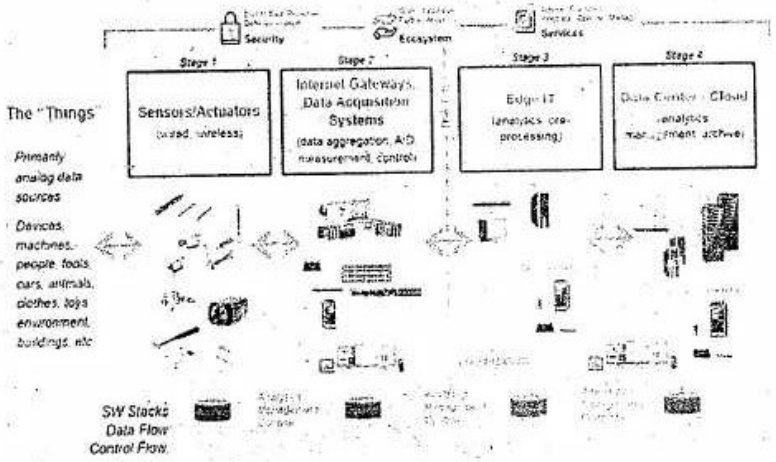
Smart farming is an often overlooked in IoT applications. However, because the number of farming operations is usually remote and the large number of livestock that farmers work on, all of this can be monitored by the Internet of Things and can revolutionize the way farmers operate day to day. But, this idea is yet to reach a large-scale attention. Nevertheless, it still remains one of the IoT applications that should not be underestimated. Smart farming has the potential to become an important application field, specifically in the agricultural-product exporting countries.

OR

2. a. Explain the IOT network architecture and design **(10 Marks)**

Ans. An Overview of the Main Stages in the IoT Architecture Diagram. In simple terms, the4 Stage IoT architecture consists of Sensors and actuators, Internet getaways and Data Acquisition Systems, Edge IT, Data center and cloud. The detailed presentation ofthesestages can be found on the diagram below.

The 4 Stage IoT Solutions Architecture



To get the proper understanding of the main actions and the importance of each stage in this process, refer to the detailed reviews presented below.

Stage 1: Networked things (wireless sensors and actuators)

The outstanding feature about sensors is their ability to convert the information obtained in the outer world into data for analysis. In other words, it's important to start with the inclusion of sensors in the 4 stages of an IoT architecture framework to get information in an appearance that can be actually processed. For actuators, the process goes even further—these devices are able to intervene the physical reality. For example, they can switch off the light and adjust the temperature in a room. Because of this, sensing and actuating stage covers and adjusts everything needed in the physical world to gain the necessary insights for further analysis.

Stage 2: Sensor data aggregation systems and analog-to-digital data conversion

Even though this stage of IoT architecture still means working in a close proximity with sensors and actuators, Internet getaways and data acquisition systems (DAS) appear here too. Specifically, the later connect to the sensor network and aggregate output, while Internet getaways work through Wi-Fi, wired LANs and perform further processing. The vital importance of this stage is to process the enormous amount of information collected on the previous stage and squeeze it to the optimal size for further analysis. Besides, the necessary conversion in terms of timing and structure happens here. In short, Stage 2 makes data both digitalized and aggregated.

Stage 3. The appearance of edge IT systems

During this moment among the stages of IoT architecture, the prepared data is transferred to the IT world. In particular, edge IT systems perform enhanced analytics and pre-processing here. For example, it refers to machine learning and visualization technologies. At the same time, some additional processing may happen here, prior to the stage of entering the data center. Likewise, Stage 3 is closely linked to the previous phases in the building of anarchitecture ofIoT. Because of this, the location of edge IT systems is close to the one where sensors and actuators are situated, creating a wiring closet. At the same time, the residing in remote offices is also possible

Stage 4. Analysis, management, and storage of data

The main processes on the last stage of IoT architecture happen in data center or cloud. Precisely, it enables in-depth processing, along with a follow-up revision for feedback. Here, the skills of both IT and OT (operational technology) professionals are needed. In other words, the phase already includes the analytical skills of the highest rank, both in digital and human worlds. Therefore, the data from other sources may be included here to ensure an in-depth analysis. After meeting all the quality standards and requirements, the information is brought back to the physical world—but in a processed and precisely analyzed appearance.

Stage 5. IoT Architecture

In fact, there is an option to extend the process of building a sustainable IoT architecture by introducing an extra stage in it. It refers to initiating a user's control over the structure if only your result doesn't include full automation, of course.

The main tasks here are visualization and management. After including Stage 5, the system turns into a circle where a user sends commands to sensors/actuators (Stage 1) to perform some actions. And the process starts all over again.

b. Explain the layered IOT Stack. **(06 Marks)**

Ans. The IoT stack is rapidly developing and maturing into the Thing Stack. This Thing Stack consists of three technology layers: sensors, microcontrollers and internet connectivity, and service platforms.

- **Layer One** - Sensors are embedded in objects or the physical environment to capture information and events for your company.
- **Layer Two** - Microcontrollers and internet connectivity share information captured by sensors within your IoT objects and act based on this information to change the environment.
- **Layer Three** - Through the aggregation and analysis of data, service platforms cater to your customers. Service platforms also control your IoT product's end-to-end experience and enable your customers to define system rules and update firmware.

Layer 1: Sensors

Sensors have been used for years in a number of different industry contexts like healthcare, aviation, manufacturing and automotive. Now, sensors are so tiny and inexpensive they can be embedded in all the devices you use personally and professionally. The sensor layer of the IoT tech stack continues to expand as internet connected sensors are added to new products and services.

Layer 2: Microcontrollers and internet connectivity

The second layer in the Internet of Things technology stack allows for local storage, data processing and internet connectivity. The Internet of Things needs internet connectivity to send collected data to your cloud database. Because some sensors generate over 10,000 data points per second, it makes sense to pre-process data locally before sending it to your cloud database. By analyzing, extracting and summarizing your collected data before you send it to your cloud database, you reduce the volume of unnecessary data you send to and store on your cloud database, saving you money on data transfer and storage costs.

Your microcontroller is a small computer embedded within a chip and it helps your IoT device store and pre-process collected data before it's synced to your cloud database. Your microcontroller possesses a processor, a small amount of RAM to hold data, some kilobytes of EPROM or flash memory to hold embedded software, and solid-date memory to cache data.

In some cases, your IoT device may need to use programmable microcontrollers to take action and turn something on or off. In most cases, these decisions are made via a cloud application, but it makes sense to use programmable microcontrollers when a sensor detects something that could affect the health and safety of your end customers.

The main and most important capability of this layer is networking, which is either wireless or wired. If a device is stationary and can access an external power source, a wired network is sufficient, but a wired network doesn't make sense for many IoT use cases because physical cables are needed to connect to the network. WiFi, wireless modems, and wireless mesh networks are the most common ways IoT devices are connected to the internet.

If you plan to manufacture an IoT device you must keep in mind dependencies for your use cases. Is your device mobile or fixed? Does your device need a battery or is it connected to a fixed power supply? How much data do you need to transfer to your cloud database per hour? Should your device's connectivity be episodic or continuous?

Devices you use to track your health and fitness while bicycling, running, and exercising store data while you're active, and these devices use episodic connectivity. Your device then syncs with the cloud when it's close to your smartphone or tablet. Compare this to the continuous connectivity needed by Amazon Echo's voice based digital assistant who is always listening for your commands, fetching answers from the internet the instant you ask a question. Depending on your IoT product's use cases, you may need continuous connectivity.

When you research Think Stack vendors, you'll notice a wide range of different networking protocols, hardware, software, and architectures are used to build IoT products. Due to the variation in use cases and environments, you have many choices when it comes to adding networking and computing capabilities your IoT device. While some vendors focus more on hardware components, other vendors provide a system of integrated software and hardware. Sometimes, IoT software solutions spill into the third layer of the Thing Stack, which is referred to as the service platform.

Layer 3: Service platforms

The first two layers for the Thing Stack embed sensor and microcomputers in your IoT device, but your IoT product profits from the service platform layer. This layer delivers value to your customers by automating processes and delivering rich data analytics. Your cloud application combines data collected from numerous IoT sensors with your (or your customers) other business data to produce insights that generate business value.

It's important for your service platform to create a feedback loop between your IoT devices and you device management software, so you and your customers can upgrade, monitor, and maintain the firmware on each the device. In most cases, service platforms operate on cloud infrastructure and utilize a multi-tenant software architecture to deliver a seamless software-as-a-service (SaaS) experience.

The convergence between our digital and physical worlds stresses your IT operations by increasing demand for data management, storage, tagging and analysis. It's in your company's best interests to build your IoT service platform on robust cloud infrastructure, so you can scale infinitely as your business grows with your new IoT product.

While "software is eating the world" as Marc Andreessen said, consumers and companies still purchase a lot of physical things. If you build a robust IoT service platform, you obtain insights about how your customers use your IoT products and services. With a great IoT service platform you can manage post-transaction relationships in new and engaging ways.

Because service platforms store and make decisions based on data collected from all types of IoT devices, they are often considered the backbone of post-transactions relationships. What if you reached out to customers who never powered on your IoT device and proactively on-boarded them? What if you used anonymized data from customers getting the most value out of your product to help other customers unlock more business value?

Now is the time to build your IoT product because sensors keep getting smaller and network connectivity solutions keep getting better. Create a plan to engage with your customers and facilitate goal-oriented post-transaction relationships, leading to new opportunities to turn a single transaction into a strong relationship.

Module - 2

3. a. What are sensors , actuators and smart objects in IOT? (04 Marks)

Ans.

BASIS FOR COMPARISON	SENSORS	ACTUATORS
Basic	Used to measure the continuous and discrete process variables.	Impel continuous and discrete processes parameters.
Placed at	Input port	Output port
Outcome	Electrical signal	Heat or motion
Example	Magnetometer, Cameras, Accelerometer, microphones.	LED, Laser, Loudspeaker, Solenoid, motor controllers.

b. What are smart physical objects in IOT ? (06 Marks)

Ans. The concept smart for a smart physical object simply means that it is active, digital, networked, can operate to some extent autonomously, is reconfigurable and has local control of the resources it needs such as energy, data storage, etc. Note, a smart object does not necessarily need to be intelligent as in exhibiting a strong essence of artificial intelligence although it can be designed to also be intelligent.

Physical world smart objects can be described in terms of three properties:

- ***Awareness***: is a smart object's ability to understand (that is, sense, interpret, and react to) events and human activities occurring in the physical world.
- ***Representation***: refers to a smart object's application and programming model—in particular, programming abstractions.
- ***Interaction***: denotes the object's ability to converse with the user in terms of input, output, control, and feedback.

Based upon these properties, these have been classified into three types:

- ***Activity-Aware Smart Objects***: Are objects that can record information about work activities and its own use.
- ***Policy-Aware Smart Objects***: Are objects that are activity-aware Objects can interpret events and activities with respect to predefined organizational policies.
- ***Process-Aware Smart Objects***: Processes play a fundamental role in industrial work management and operation. A process is a collection of related activities or tasks that are ordered according to their position in time and space.

c. What are the primary components of smart connected products ? (06 Marks)

Ans. Smart, connected products have three primary components

- Physical – made up of the product's mechanical and electrical parts.
- Smart – made up of sensors, microprocessors, data storage, controls, software, and an embedded operating system with enhanced user interface.
- Connectivity – made up of ports, antennae, and protocols enabling wired/wireless connections that serve two purposes, it allows data to be exchanged with the product and enables some functions of the product to exist outside the physical device.

Each component expands the capabilities of one another resulting in "a virtuous cycle of value improvement". First, the smart components of a product amplify the value and capabilities of the physical components. Then, connectivity amplifies the value and capabilities of the smart components. These improvements include:

- Monitoring of the product's conditions, its external environment, and its operations and usage.
- Control of various product functions to better respond to changes in its environment, as well as to personalize the user experience.
- Optimization of the product's overall operations based on actual performance data, and reduction of downtimes through predictive maintenance and remote service.
- Autonomous product operation, including learning from their environment, adapting to users' preferences and self-diagnosing and service.

OR

4. a. What are actuators in IOT ? Explain (04 Marks)

Ans. An actuator is a mechanism for turning energy into motion.

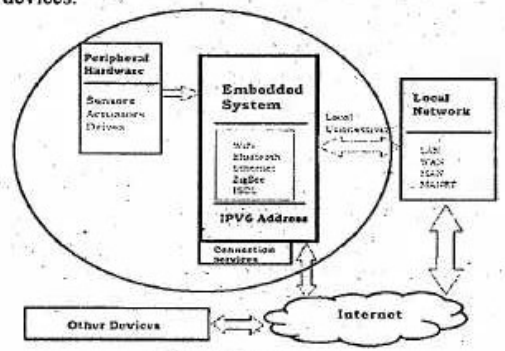
Actuators can be categorized by the energy source they require to generate motion. For example:

- Pneumatic actuators use compressed air to generate motion.
- Hydrolic actuators use liquid to generate motion.
- Electric actuators use an external power source, such as a battery, to generate motion.
- Thermal actuators use a heat source to generate motion.

b. What are embedded systems in IOT? Explain (12 Marks)

Ans. It is essential to know about the embedded devices while learning the IoT or building the projects on IoT. The embedded devices are the objects that build the unique computing system. These systems may or may not connect to the Internet.

An embedded device system generally runs as a single application. However, these devices can connect through the internet connection, and able communicate through other network devices.



Internet of Things (IoT)

Embedded System Hardware

The embedded system can be of type microcontroller or type microprocessor. Both of these types contain an integrated circuit (IC).

The essential component of the embedded system is a RISC family microcontroller like Motorola 68HC11, PIC 16F84, Atmel 8051 and many more. The most important factor that differentiates these microcontrollers with the microprocessor like 8085 is their internal read and writable memory. The essential embedded device components and system architecture are specified below.

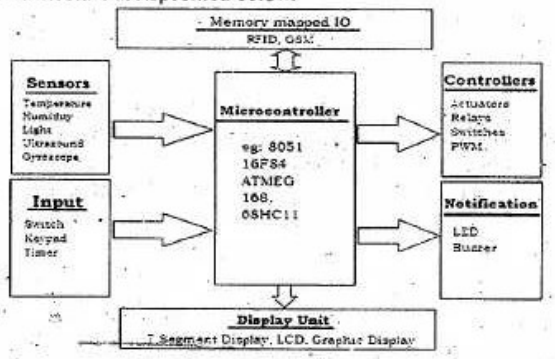


Fig: Basic Embedded System

OR

5. a. List the business case for IT and IOT **(05 Marks)**

Ans. 1) Recognise the need for a business case
2) Start on the shop floor
3) Identify meaningful data
4) Employ predictive analytics
5) Track your products and assests
6) Create a new revenue modela
7) Move from drawing board to reality
8) Choose the right IOT platforms and partners
9) Build a proof of concept
10) Roll out at scale

b. What is meant by device management in IOT **(05 Marks)**

Ans. Device management (DM) is an essential part of the IoT and provides efficient means to perform many of the management tasks for devices:

- **Provisioning**: Initialization (or activation) of devices in regards toconfiguration and features to be enabled.
- **Device Configuration**: Management of device settings and parameters.
- **Software Upgrades**: Installation of firmware, system software, and applications on the device.
- **Fault Management**: Enables error reporting and access to device status

In the simplest deployment, the devices communicate directly with the DM server. This is, however, not always optimal or even possible due to network or protocol constraints, e.g. due to a firewall or mismatching protocols.

In these cases, the gateway functions as mediator between the server and the devices, and can operate in three different ways:

- If the devices are visible to the DM server, the gateway can simply forward the messages between the device and the server and is not a visible participant in the session.
- In case the devices are not visible but understand the DM protocol in use, the gateway can act as a proxy, essentially acting as a DM server towards the device and a DM client towards the server.
- For deployments where the devices use a different DM protocol from the server, the gateway can represent the devices and translate between the different protocols (e.g. TR-069, OMA-DM, or CoAP). The devices can be represented either as virtual devices or as part of the gateway.

c. What are the networking technologies adopted with IOT **(06 Marks)**

Ans. 1. Power Line Communication

(PLC) refers to communicating over power (or phone, coax, etc.) lines.

This amounts to pulsing, with various degrees of power and frequency, the electrical lines used for power distribution. PLC comes in numerous flavors. At low frequencies

(tens to hundreds of Hertz) it is possible to communicate over kilometers with low bit rates (hundreds of bits per second).

Typically, this type of communication was used for remote metering, and was seen as potentially useful for the smart grid. Enhancements to allow higher bit rates have led to the possibility of delivering broadband connectivity over power lines.

1. LAN (and WLAN)

Continues to be important technology for M2M and IoT applications.

This is due to the high bandwidth, reliability, and legacy of the technologies. Where power is not a limiting factor, and high bandwidth is required, devices may connect seamlessly to the Internet via Ethernet (IEEE 802.3) or Wi-Fi (IEEE 802.11). The utility of existing (W) LAN infrastructure is evident in a number of early IoT applications targeted at the consumer market, particularly where integration and control with smart phones is required.

2. Bluetooth Low Energy

(BLE; "Bluetooth Smart") is a recent integration of Nokia's Wibree standard with the main Bluetooth standard. It is designed for short-range(.50 m) applications in healthcare, fitness, security, etc., where high data rates (millions of bits per second) are required to enable application functionality. It is deliberately low cost and energy efficient by design, and has been integrated into the majority of recent smart phones.

3. Low-Rate, Low-Power Networks

are another key technology that form the basis of the IoT.

4. IPv6 Networking

making the fact that devices are networked, with or without wires, with variouscapabilities in terms of range and bandwidth, essentially seamless.

It is foreseeable that the only hard requirement for an embedded device will be that it can somehow connect with a compatible gateway device.

5. 6LoWPAN

(IPv6 Over Low Power Wireless Personal Area Networks) was developed initially by the 6LoWPAN Working Group (WG) of the IETF

The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices", and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things

6. RPL

IPv6 Routing Protocol for Low-Power and Lossy Networks. Abstract

Low-Power and Lossy Networks (LLNs) are a class of network in which both the routers and their interconnect are constrained. LLN routers typically operate with constraints on processing power, memory, and energy (battery power).

7. CoAP

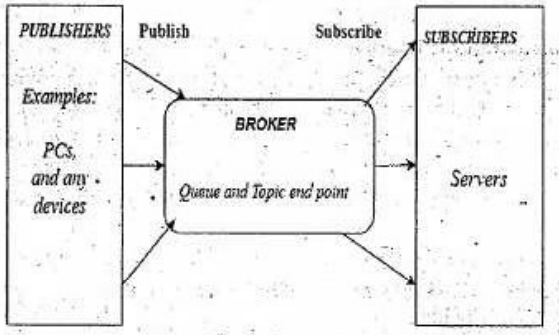
Constrained Application Protocol (CoAP) is a protocol that specifies how low-power compute-constrained devices can operate in the internet of things (IoT).

OR

6. a. Explainany threeIOT application layer transport methods with suitable illustrations. (12 Marks)

Ans. A. MQTT

MQTT (Message Queue Telemetry Transport) was develop by or introduce by IBM in 1999 and standardized by OASIS in 2013 to target come up with lightweight M2M communication. It is publish/subscribe protocol architecture similar to client/server protocol show in figure below. The importance of MQTT protocol is due to its simplicity and the no need of high CPU and memory usage (reason is the lightweight protocol). MQTT supports a wide range of different devices and mobile platforms. At transport layer TLS/SSL security provide to MQTT.



Show above figure there three component are there publishers, a broker and subscribers. Publishers are generally lightweight sensors that connect with a broker and send data to a broker and go back to sleep. Subscribers are IoT applications that interested in data send by sensors and also connect with a broker. so broker send interested data to subscribers. The brokers classify sensory data in topics and send them to subscribers interested in the topics. This all thing is on IoT point of view.

MQTT provide 3 option to achieve message in

Quality of Services (QoS):

1. One delivery (at most):

Deliver message according to best try of the network.

An acknowledgment is not required. Lowest level of QoS.

2. One delivery (at least):

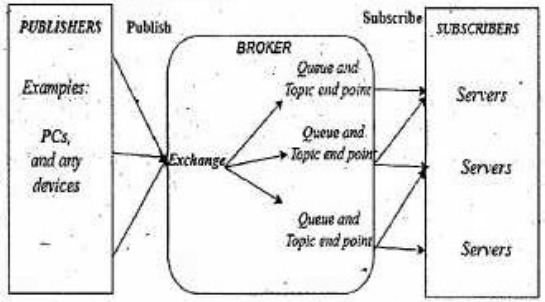
At least one message can be send and some duplicate message are there. An acknowledgment is required

3. On delivery:

Additional protocol required to ensure that one and only one message send. It is highest level of QoS.

B. AMQP

The Advanced Message Queuing Protocol (AMQP) is a protocol that across from the financial industry. Security is manage with the use of the TLS/SSL protocols. Its run over TCP. AMQT is follow publish/subscribe communication protocol for messaging. AMQP is same like MQTT but AMQT have advantage its store data then forward it, and this feature used at when network disruptions that time ensures reliability. Show in figure below a broker divide into two part exchange and queue. Exchange responsibility to receive publishers messages and distribute to queue. Queues is based on pre-define roles and condition and it's basically send message to subscribers who subscribe those data.



C. COAP

CoAP (constrained application protocol) is used for low power and low memory embedded devices where it can be used for communication instead of HTTP. Currently there is HTTP protocol available with request/response paradigm but HTTP has many features and more footprint [5]. HTTP runs over TCP where TCP will need more resources due to three way handshake and many more complex mechanism. Now for low power embedded devices, there is no need of this heavy protocols and we can optimize it to run over TCP.

As CoAP is a Restful web transfer protocol for use with constrained networks. CoAP uses client/server model of approach same as HTTP. It is designed for constrained networks with low overhead and lower footprint. Some points for CoAP that makes better protocol compared to HTTP is:

- CoAP runs over UDP (User data-gram protocol) that helps to avoid costly TCP handshake before data transmission
- CoAP protocol is only 4-byte header and provides reliable transfer and no reliable transfer as it uses four types of messages.
- It support four types of message

1) Confirmable, 2) Non-Confirmable, 3) Acknowledgement and 4) Reset. Request/Response layer used those message and classified in 1) Piggy-backed, 2) Separate response, 3) Non confirmable request and response, and communicate with each other .

b. Write explanatory notes on network optimization in IOT. (04 Marks)

Ans. Generally, network optimization is defined as the technology used to improve the performance of the network for any environment. This plays an important role in IT, as day by day large amount of data from various kinds of devices and applications are being populated into the network. Network optimization offers various benefits such as faster data rate, data recovery, eliminating redundant data and to increase the response time of application and network. Network optimization in IoT is gaining increased attention due to the expectation of a high increase in traffic from IoT things and objects, as billions of IoT devices are expected to connect global network in the coming years. Due to this, it is obvious for researchers and operators to provide efficient solution to optimize IoT networks to reduce the IoT generated traffic impacting other services in the network and to utilize network resourceefficiently. The traffic generated by IoT devices is different from the cellular network due to heterogeneity in applications and device types. Additionally, IoT traffic needs to be regulated to monitor the working of IoT devices and its services. IoT application generates fewer amount of data, however integration of devices to the application generates the higher volume of traffic because of control plane messages. Hence this non-application traffic puts a significant additional burden on the network. So to overcome from this burden, efficient mechanism is required to address and optimize the control plane messaging from IoT devices.

OR

7. a. Justify the statement" Merging Data Analytcs and IOT will positively impact business. (08 Marks)

Ans. Network optimization in IoT is gaining increased attention due to the expectation of a high increase in traffic from IoT things and objects, as billions of IoT devices are expected to connect global network in the coming years. Due to this, it is obvious for researchers and operators to provide efficient solution to optimize IoT networks to reduce the IoT generated traffic impacting other services in the network and to utilize network resourceefficiently. The traffic generated by IoT devices is different from the cellular network due to heterogeneity in applications and device types. Additionally, IoT traffic needs to be regulated to monitor the working of IoT devices and its services. IoT application generates fewer amount of data, however integration of devices to the application generates the higher volume of traffic because of control plane messages. Hence this non-application traffic puts a significant additional burden on the network. So to overcome from this burden, efficient mechanism is required to address and optimize the control plane messaging from IoT devices.

- **Competitive Edge:** IoT is a buzzword in the current era of technology and there are numerous IoT application developers and providers present in the market. The use of data analytics in IoT investments will provide a business unit to offer better services and will, therefore, provide the ability to gain a competitive edge in the market.

There are different types of data analytics that can be used and applied in the IoT investments to gain advantages. Some of these types have been listed and described below.

- **Streaming Analytics:** This form of data analytics is also referred as event stream processing and it analyzes huge in-motion data sets. Real-time data streams are analyzed in this process to detect urgent situations and immediate actions. IoT applications based on financial transactions, air fleet tracking, traffic analysis etc. can benefit from this method.
- **Spatial Analytics:** This is the data analytics method that is used to analyze geographic patterns to determine the spatial relationship between the physical objects. Location-based IoT applications, such as smart parking applications can benefit from this form of data analytics.
- **Time Series Analytics:** As the name suggests, this form of data analytics is based upon the time-based data which is analyzed to reveal associated trends and patterns. IoT applications, such as weather forecasting applications and health monitoring systems can benefit from this form of data analytics method.
- **Prescriptive Analysis:** This form of data analytics is the combination of descriptive and predictive analysis. It is applied to understand the best steps of action that can be taken in a particular situation. Commercial IoT applications can make use of this form of data analytics to gain better conclusions.

b. Explain the common challenges in OT security (08 Marks)

Ans. 1) Erosion of Network Architecture

Two of the major challenges in securing industrial environments have been initial design and ongoing maintenance. The initial design challenges arose from the concept that networks were safe due to physical separation from the enterprise with minimal or no connectivity to the outside world, and the assumption that attackers lacked sufficient knowledge to carry out security attacks. The challenge, and the biggest threat to network security, is standards and best practices either being misunderstood or the network being poorly maintained. In fact, from a security design perspective, it is better to know that communication paths are insecure than to not know the actual communication paths. It is more common that, over time, what may have been a solid design to begin with is eroded through ad hoc updates and individual changes to hardware and machinery without consideration for the broader network impact. This kind of organic growth has led to miscalculations of expanding networks and the introduction of wireless communication in a standalone fashion, without consideration of the impact to the original security design. These uncontrolled or poorly controlled OT network evolutions have, in many cases, over time led to weak or inadequate network and systems security.

In many industries, the control systems consist of packages, skids, or components that are self-contained and may be integrated as semi-autonomous portions of the network. These packages may not be as fully or tightly integrated into the overall

control system, network management tools, or security applications, resulting in potential risk.

2) Pervasive Legacy Systems

Due to the static nature and long lifecycles of equipment in industrial environments, many operational systems may be deemed legacy systems. For example, in a power utility environment, it is not uncommon to have racks of old mechanical equipment still operating alongside modern intelligent electronic devices (IEDs). In many cases, legacy components are not restricted to isolated network segments but have now been consolidated into the IT operational environment. From a security perspective, this is potentially dangerous as many devices may have historical vulnerabilities or weaknesses that have not been patched and updated, or it may be that patches are not even available due to the age of the equipment.

Beyond the endpoints, the communication infrastructure and shared centralized compute resources are often not built to comply with modern standards. In fact, their communication methods and protocols may be generations old and must be interoperable with the oldest operating entity in the communications path. This includes switches, routers, firewalls, wireless access points, servers, remote access systems, patch management, and network management tools. All of these may have exploitable vulnerabilities and must be protected.

3) Insecure Operational Protocols

Many industrial control protocols, particularly those that are serial based, were designed without inherent strong security requirements. Furthermore, their operation was often within an assumed secure network. In addition to any inherent weaknesses or vulnerabilities, their operational environment may not have been designed with secured access control in mind.

The structure and operation of most of these protocols is often publicly available. While they may have been originated by a private firm, for the sake of interoperability, they are typically published for others to implement. Thus, it becomes a relatively simple matter to compromise the protocols themselves and introduce malicious actors that may use them to compromise control systems for either reconnaissance or attack purposes that could lead to undesirable impacts in normal system operation. The following sections discuss some common industrial protocols and their respective security concerns. Note that many have serial, IP, or Ethernet-based versions, and the security challenges and vulnerabilities are different for the different variants.

4) Modbus

Modbus is commonly found in many industries, such as utilities and manufacturing environments, and has multiple variants (for example, serial, TCP/IP). It was created by the first programmable logic controller (PLC) vendor, Modicon, and has been in use since the 1970s. It is one of the most widely used protocols in industrial deployments, and its development is governed by the Modbus Organization. The security challenges that have existed with Modbus are not unusual. Authentication

of communicating endpoints was not a default operation because it would allow an inappropriate source to send improper commands to the recipient. For example, for a message to reach its destination, nothing more than the proper Modbus address and function call (code) is necessary.

Some older and serial-based versions of Modbus communicate via broadcast. The ability to curb the broadcast function does not exist in some versions. There is potential for a recipient to act on a command that was not specifically targeting it. Furthermore, an attack could potentially impact unintended recipient devices, thus reducing the need to understand the details of the network topology.

Validation of the Modbus message content is also not performed by the initiating application. Instead, Modbus depends on the network stack to perform this function. This could open up the potential for protocol abuse in the system.

5) DNP3 (Distributed Network Protocol)

DNP3 is found in multiple deployment scenarios and industries. It is common in utilities and is also found in discrete and continuous process systems. Like many other ICS/SCADA protocols, it was intended for serial communication between controllers and simple IEDs.

There is an explicit "secure" version of DNP3, but there also remain many insecure implementations of DNP3 as well. DNP3 has placed great emphasis on the reliable delivery of messages. That emphasis, while normally highly desirable, has a specific weakness from a security perspective. In the case of DNP3, participants allow for unsolicited responses, which could trigger an undesired response. The missing security element here is the ability to establish trust in the system's state and thus the ability to trust the veracity of the information being presented. This is akin to the security flaws presented by Gratuitous ARP messages in Ethernet networks, which has been addressed by Dynamic ARP Inspection (DAI) in modern Ethernet switches.

6) ICCP (Inter-Control Center Communications Protocol)

ICCP is a common control protocol in utilities across North America that is frequently used to communicate between utilities. Given that it must traverse the boundaries between different networks, it holds an extra level of exposure and risk that could expose a utility to cyber attack.

7) OPC (OLE for Process Control)

OPC is based on the Microsoft interoperability methodology Object Linking and Embedding (OLE). This is an example where an IT standard used within the IT domain and personal computers has been leveraged for use as a control protocol across an industrial network.

In industrial control networks, OPC is limited to operation at the higher levels of the control space, with a dependence on Windows-based platforms. Concerns around OPC begin with the operating system on which it operates. Many of the Windows devices in the operational space are old, not fully patched, and at risk due to a plethora of well-known vulnerabilities. The dependence on OPC may reinforce that dependence. While newer versions of OPC have enhanced security capabilities,

they have also opened up new communications modes, which have both positive and negative security potential.

Of particular concern with OPC is the dependence on the Remote Procedure Call (RPC) protocol, which creates two classes of exposure. The first requires you to clearly understand the many vulnerabilities associated with RPC, and the second requires you to identify the level of risk these vulnerabilities bring to a specific network.

OR

8. a How IT and OT Security Practices and Systems Vary? (12 Marks)

Ans. The differences between an enterprise IT environment and an industrial-focused OT deployment 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 in this chapter, and they are more explicitly discussed in the following sections.

The Purdue Model for Control Hierarchy

Regardless of where a security threat arises, it must be consistently and unequivocally treated. IT information is typically used to make business decisions, such as those in process optimization, whereas OT information is instead characteristically leveraged to make physical decisions, such as closing a valve, increasing pressure, and so on. Thus, the operational domain must also address physical safety and environmental factors as part of its security strategy—and this is not normally associated with the IT domain. Organizationally, IT and OT teams and tools have been historically separate, but this has begun to change, and they have started to converge, leading to more traditionally IT-centric solutions being introduced to support operational activities. For example, systems such as firewalls and intrusion prevention systems (IPS) are being used in IoT networks.

As the borders between traditionally separate OT and IT domains blur, they must align strategies and work more closely together to ensure end-to-end security. The types of devices that are found in industrial OT environments are typically much more highly optimized for tasks and industrial protocol-specific operation than their IT counterparts. Furthermore, their operational profile differs as well.

Industrial environments consist of both operational and enterprise domains. To understand the security and networking requirements for a control system, the use of a logical framework to describe the basic composition and function is needed. The Purdue Model for Control Hierarchy, introduced in Chapter 2, is the most widely used framework across industrial environments globally and is used in manufacturing, oil and gas, and many other industries. It segments devices and equipment by hierarchical function levels and areas and has been incorporated into the ISA99/IEC 62443 security standard, as shown in Figure 8-3. For additional detail on how the Purdue Model for Control Hierarchy is applied to the manufacturing and oil and gas industries, see Chapter 9, "Manufacturing," and Chapter 10, "Oil and Gas."

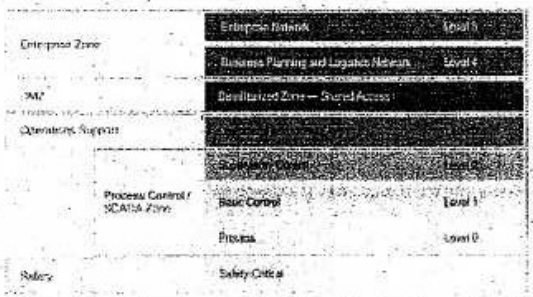


Figure 8: The Logical Framework Based on the Purdue Model for Control Hierarchy

This model identifies levels of operations and defines each level. The enterprise and operational domains are separated into different zones and kept in strict isolation via an industrial demilitarized zone (DMZ):

- Enterprise zone
- **Level 5: Enterprise network:** Corporate-level applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), document management, and services such as Internet access and VPN entry from the outside world exist at this level.
- **Level 4: Business planning and logistics network:** The IT services exist at this level and may include scheduling systems, material flow applications, optimization and planning systems, and local IT services such as phone, email, printing, and security monitoring.

Industrial demilitarized zone

- **DMZ:** The DMZ provides a buffer zone where services and data can be shared between the operational and enterprise zones. It also allows for easy segmentation of organizational control. By default, no traffic should traverse the DMZ; everything should originate from or terminate on this area.

Operational zone

- **Level 3: Operations and control:** This level includes the functions involved in managing the workflows to produce the desired end products and for monitoring and controlling the entire operational system. This could include production scheduling, reliability assurance, systemwide control optimization, security management, network management, and potentially other required IT services, such as DHCP, DNS, and timing.
- **Level 2: Supervisory control:** This level includes zone control rooms, controller status, control system network/application administration, and other control-related applications, such as human-machine interface (HMI) and historian.
- **Level 1: Basic control:** At this level, controllers and IEDs, dedicated HMIs, and other applications may talk to each other to run part or all of the control function.
- **Level 0: Process:** This is where devices such as sensors and actuators and machines such as drives, motors, and robots communicate with controllers or IEDs.

Safety zone

- **Safety-critical:** This level includes devices, sensors, and other equipment used to manage the safety functions of the control system.

One of the key advantages of designing an industrial network in structured levels, as with the Purdue model, is that it allows security to be correctly applied at each level and between levels. For example, IT networks typically reside at Levels 4 and 5 and use security principles common to IT networks. The lower levels are where the industrial systems and IoT networks reside. As shown in Figure 8, a DMZ resides between the IT and OT levels. Clearly, to protect the lower industrial layers, security technologies such as firewalls, proxy servers, and IPSs should be used to ensure that only authorized connections from trusted sources on expected ports are being used. At the DMZ, and, in fact, even between the lower levels, industrial firewalls that are capable of understanding the control protocols should be used to ensure the continuous operation of the OT network.

Although security vulnerabilities may potentially exist at each level of the model, it is clear that due to the amount of connectivity and sophistication of devices and systems, the higher levels have a greater chance of incursion due to the wider attack surface. This does not mean that lower levels are not as important from a security perspective; rather, it means that their attack surface is smaller, and if mitigation techniques are implemented properly, there is potentially less impact to the overall system. As shown in Figure 8-1, a review of published vulnerabilities associated with industrial security in 2011 shows that the assets at the higher levels of the framework had more detected vulnerabilities.

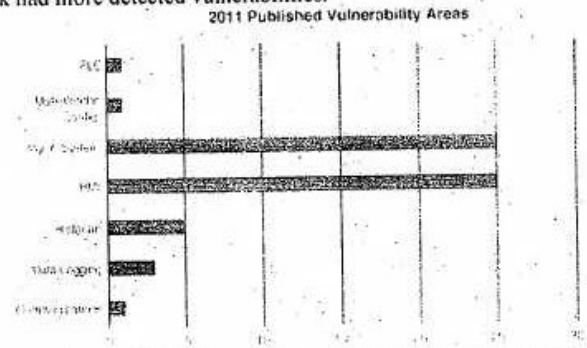


Figure 8-1 2011 Industrial Security Report of Published Vulnerability Areas (US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) https://ics-cert.us-cert.gov).

b. What is Network Security Monitoring ? Explain **(04 Marks)**

Ans. Network security monitoring (NSM) is a process of finding intruders in a network. It is achieved by collecting and analyzing indicators and warnings to prioritize and investigate incidents with the assumption that there is, in fact, an undesired presence. The practice of NSM is not new, yet it is not implemented often or thoroughly enough

even within reasonably mature and large organizations. There are many reasons for this underutilization, but lack of education and organizational patience are common reasons. To simplify the approach, there is a large amount of readily available data that, if reviewed, would expose the activities of an intruder.

It is important to note that NSM is inherently a process in which discovery occurs through the review of evidence and actions that have already happened. This is not meant to imply that it is a purely postmortem type of activity. If you recognize that intrusion activities are, much like security, an ongoing process, then you see that there is a similar set of stages that an attacker must go through. The tools deployed will slow that process and introduce opportunities to detect and thwart the attacker, but there is rarely a single event that represents an attack in its entirety. NSM is the discipline that will most likely discover the extent of the attack process and, in turn, define the scope for its remediation.

Module - 5

9. a. Explain the features of Ardunio UNO with regard to IOT **(08 Marks)**

Ans. The Arduino Uno is a microcontroller board based on the ATmega328. Arduino is an open-source, prototyping platform and its simplicity makes it ideal for hobbyists to use as well as professionals. The Arduino Uno has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Arduino Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 microcontroller chip programmed as a USB-to-serial converter.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Arduino Uno and version 1.0 will be the reference versions of Arduno, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform.

Features of the Arduino UNO:

- Microcontroller: ATmega328
- Operating Voltage: 5V
- Input Voltage (recommended): 7-12V
- Input Voltage (limits): 6-20V
- Digital I/O Pins: 14 (of which 6 provide PWM output)
- Analog Input Pins: 6
- DC Current per I/O Pin: 40 mA
- DC Current for 3.3V Pin: 50 mA
- Flash Memory: 32 KB of which 0.5 KB used by bootloader
- SRAM: 2 KB (ATmega328)
- EEPROM: 1 KB (ATmega328)
- Clock Speed: 16 MHz

b. What are the models of Raspberry pi ? **(05 Marks)**

Ans. **Raspberry Pi** — There are six different models of Raspberry Pi. The Pi 2 Model Bor Pi 1 Model B+ and Pi 3 Model B are ideal for beginner projects because they are the most versatile and have the widest range of capabilities. The Pi 3 Model B has the added bonus of having a quad-core processor and 1 GB of RAM so it supports heavier operating systems, like Ubuntu and Microsoft 10. The Model A+is a powerful board for building robotics, but doesn't have an Ethernet port and only comes with one USB port. Raspberry Pi Zero is basically a miniature version of the Model A+, but has a more robust computing power. It has a micro USB port and mini HDMI port for 1080p output compatibility but doesn't have wireless capability. It only costs $5 and Adafruit sells v.1.3 for just $5, but you can only buy one per order. The Raspberry Pi Zero W is the same single-board computer as the standard Zero but *does* support wireless and Bluetooth connectivity. It costs $10 on Adafruit,

c. What is a temperature sensor ? **(03 Marks)**

Ans. A **temperature sensor** is a device, typically, a thermocouple or RTD,that provides for **temperature** measurement through an electrical signal. A thermocouple (T/C) is made from two dissimilar metals that generate electrical voltage in direct proportion to changes in **temperature.**

OR

10. a. Explain how IOT can be used with consumer appliances **(06 Marks)**

Ans. Consumers benefit personally and professionally from the optimization and data analysis of IoT. IoT technology behaves like a team of personal assistants, advisors, and security. It enhances the way we live, work, and play.

Home

IoT takes the place of a full staff –

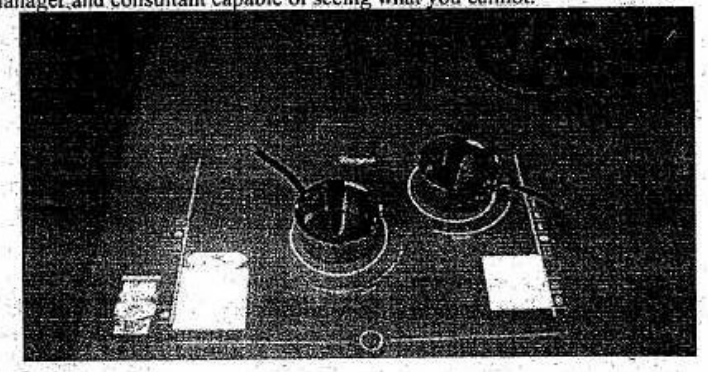
- **Butler** – IoT waits for you to return home, and ensures your home remains fully prepared. It monitors your supplies, family, and the state of your home. It takes actions to resolve any issues that appear.
- **Chef** – An IoT kitchen prepares meals or simply aids you in preparing them.
- **Nanny** – IoT can somewhat act as a guardian by controlling access, providing supplies, and alerting the proper individuals in an emergency.
- **Gardner** – The same IoT systems of a farm easily work for home landscaping.
- **Repairman** – Smart systems perform key maintenance and repairs, and also request them.
- **Security Guard** – IoT watches over you 24/7. It can observe suspicious individuals miles away, and recognize the potential of minor equipment problems to become disasters well before they do.

This smart, connected stove from Whirlpool allows two different heat settings on the same surface, remote monitoring, and remote control.

Work

A smart office or other workspace combines customization of the work environment with smart tools. IoT learns about you, your job, and the way you work to deliver an

optimized environment. This results in practical accommodations like adjusting the room temperature, but also more advanced benefits like modifying your schedule and the tools you use to increase your output and reduce your work time. IoT acts as a manager and consultant capable of seeing what you cannot.



Play

IoT learns as much about you personally as it does professionally. This enables the technology to support leisure –

- **Culture and Night Life** – IoT can analyze your real-world activities and response to guide you in finding more of the things and places you enjoy such as recommending restaurants and events based on your preferences and experiences.
- **Vacations** – Planning and saving for vacations proves difficult for some, and many utilize agencies, which can be replaced by IoT.
- **Products and Services** – IoT offers better analysis of the products you like and need than current analytics based on its deeper access. It integrates with key information like your finances to recommend great solutions.

b. Explain the IOT Application for smart cities. **(10 Marks)**

Ans. Approximately 70 percent of the world's population is expected to live in cities by 2050 according to Gartner. This rapid urban growth is already placing a considerable strain on the existing infrastructure, and with more people making the move to urban living, it's only going to get worse in the coming years.

To accommodate this new demand on cities, municipalities around the globe are turning to the Internet of Things innovation to enhance their services, reduce costs, and improve communication and interaction. Though the potential is there for IoT to improve nearly every aspect of urban living, there are three IoT applications for smart cities.

A more efficient water supply

The Internet of Things has the potential to transform the way cities consume water. Smart meters can improve leak detection and data integrity; prevent lost revenue due to inefficiency, and boost productivity by reducing the amount of time spent entering and analyzing data. Also, these meters can be designed to feature customer-

facing portals, providing residents with real-time access to information about their consumption and water supply.

An innovative solution to traffic congestion

As more and more people move to cities, traffic congestion – which is already a massive problem – is only going to get worse. Fortunately, the Internet of Things is well positioned to make improvements in this area that can benefit residents immediately. For example, smart traffic signals can adjust their timing to accommodate commutes and holiday traffic and keep cars moving. City officials can collect and aggregate data from traffic cameras, mobile phones, vehicles, and road sensors to monitor traffic incidents in real-time. Drivers can be alerted of accidents and directed to routes that are less congested. The possibilities are endless and the impact will be substantial.

More reliable public transportation

Public transportation is disrupted whenever there are road closures, bad weather, or equipment breakdowns. IoT can give transit authorities the real-time insights they need to implement contingency plans, ensuring that residents always have access to safe, reliable, and efficient public transportation. This might be done using insights from cameras or connected devices at bus shelters or other public areas.

Energy-efficient buildings

IoT technology is making it easier for buildings with legacy infrastructure to save energy and improve their sustainability. Smart building energy management systems, for instance, use IoT devices to connect disparate, nonstandard heating, cooling, lighting, and fire-safety systems to a central management application. The energy management application then highlights areas of high use and energy drifts so staff can correct them.

Research shows that commercial buildings waste up to 30 percent of the energy they use,[1] so savings with a smart building energy management system can be significant. As more smart city buildings use energy management systems, the city will become more sustainable as a whole.

Improved public safety

Smart cities and their CSP partners often implement video monitoring systems to tackle the safety concerns that come up in every growing city. Some cities now have hundreds of cameras monitoring traffic for accidents and public streets for safety concerns. Video analytics software helps process the thousands of hours of video footage each camera produces, whittling it down to only important events. Systems using IoT technology turn every camera attached to the system into a sensor, with edge computing and analytics starting right from the source. Artificial intelligence technology like machine learning will then complete the analysis and send video footage to humans who can react quickly to solve problems and keep residents safe. Cities are also improving public safety with smart lighting initiatives that replace traditional streetlights with connected LED infrastructure. Not only do the LED lights last longer and conserve energy, they also provide information on outages in real time. City workers can use that information to ensure important areas are well lit to deter crimes and make the public feel safer.

As Per New VTU Syllabus w.e.f 2015-16
Choice Based Credit System(CBCS)

SUNSTAR

SUNSTAR EXAM SCANNER

BIG DATA ANALYTICS

(VIII SEM. B.E. CSE / ISE)

Eight Semester B.E. Degree Examination, CBCS - June / July 2019

Internet of Things Technology

Time: 3 hrs. **Max. Marks:** 80

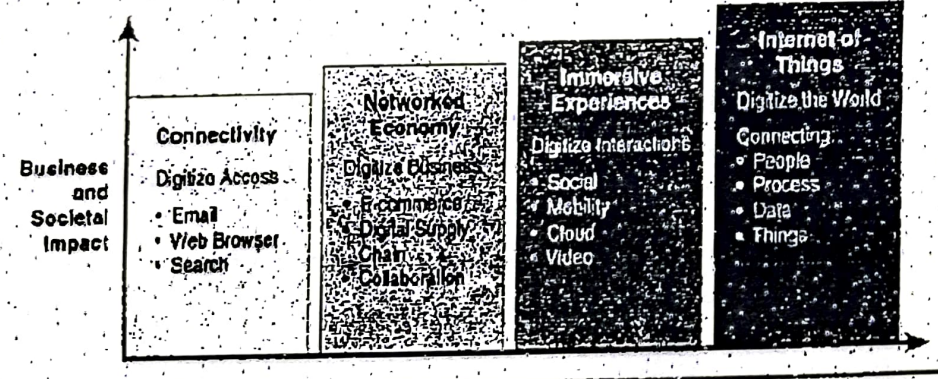
Note : *Answer any FIVE full questions, selecting ONE full question from each module.*

Module - 1

1. a. What is IOT? Explain in detail on Genesis of IOT. **(08 Marks)**

Ans. Internet of Things (IOT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IOT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken.

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. With more "things" connected to the Internet than people in the world, a new age was upon us, and the Internet of Things was born. The person credited with the creation of the term "Internet of Things" is Kevin Ashton. While working for Procter & Gamble in 1999, Kevin used this phrase to explain a new idea related to linking the company's supply chain to the Internet.



Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.

Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

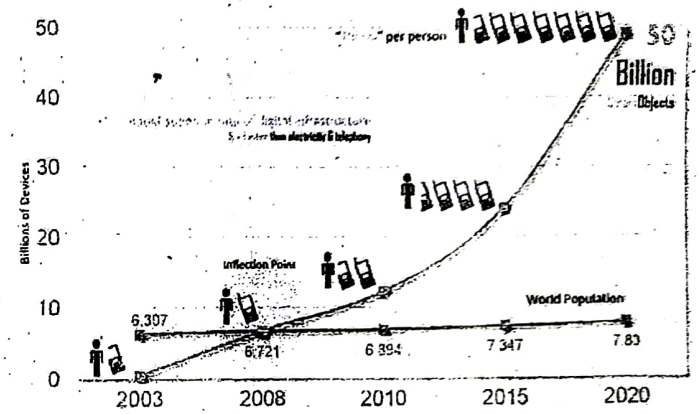
b. What does IoT and digitization mean? Elaborate on this concept. (04 Marks)

Ans. IoT and digitization are terms 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 and 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 and the business insights that result.

For example, in a shopping mall where Wi-Fi location tracking has been deployed, the "things" are the Wi-Fi devices. Wi-Fi location tracking is simply the capability of knowing where a consumer is in a retail environment through his or her smart phone's connection to the retailer's Wi-Fi network. While the value of connecting Wi-Fi devices or "things" to the Internet is obvious and appreciated by shoppers; tracking real-time location of Wi-Fi clients provides a specific business benefit to the mall and shop owners. In this case, it helps the business understand where shoppers tend to congregate and how much time they spend in different parts of a mall or store. Analysis of this data can lead to significant changes to the locations of product displays and advertising, where to place certain types of shops, how much rent to charge, and even where to station security guards.

c. Write a short note on "IoT impact in Real World". (04 Marks)

Ans. Projections on the potential impact of IoT are impressive. About 14 billion, or just 0.06%, of "things" are connected to the Internet today. Cisco Systems predicts that by 2020, this number will reach 50 billion. A UK government report speculates that this number could be even higher, in the range of 100 billion objects connected. Cisco further estimates that these new connections will lead to $19 trillion in profits and cost savings. Figure 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 and businesses interact with their surroundings. Managing and monitoring smart objects using real-time connectivity enables a whole new level of datadriven decision making. This in turn results in the optimization of systems and processes and delivers new services that save time for both people and businesses while improving the overall quality of life.

OR

2. a. Discuss IOT challenges. (08 Marks)

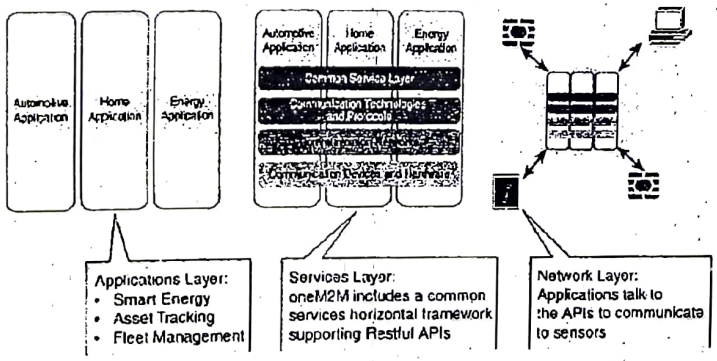
Ans.

Challenge	Description
Scale	While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger. For example, one large electrical utility in Asia recently began deploying IPv6-based smart meters on its electrical grid. While this utility company has tens of thousands of employees (which can be considered IP nodes in the network), the number of meters in the service area is tens of millions. This means the scale of the network the utility is managing has increased by more than 1,000-fold! "IP as the IoT Network Layer," explores how new design approaches are being developed to scale IPv6 networks into the millions of devices.
Security	With more "things" becoming connected with other "things" and people, security is an increasingly complex issue for IoT. Your threat surface is now greatly expanded, and if a device gets hacked, its connectivity is a major concern. A compromised device can serve as a launching point to attack other devices and systems. IoT security is also pervasive across just about every facet of IoT.

Privacy	As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment. For businesses, this data has monetary value. Organizations are now discussing who owns this data and how individuals can control whether it is shared and with whom.
Big data and data analytics	IoT and its large number of sensors is going to trigger a deluge of data that must be handled, This data will provide critical information and insights if it can be processed in an efficient maimer. The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner,
Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others arc open. Recent IoT standards ate helping minimize this problem. but there are often various protocols and implementations available for IoT networks.

b. With a neat diagram, explain architecture of IoT **(04 Marks)**

Ans.



Applications layer: The oneM2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

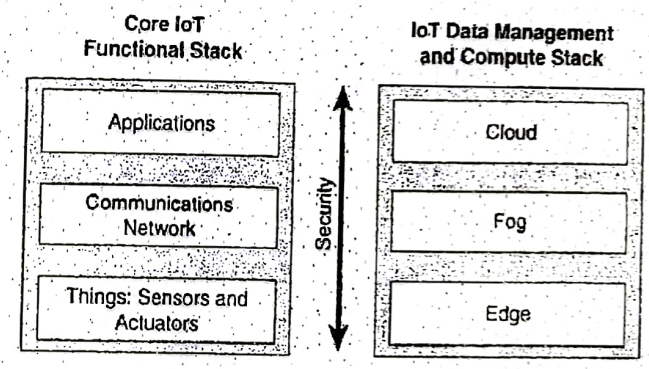
Services layer: This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the

hardware. Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on. Riding on top is the common services layer. This conceptual layer adds APIs and middleware supporting third-party services and applications.

Network layer: This is the communication domain for the IoT devices and endpoints. It includes the devices themselves and the communications network that links them. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah. Also included are wired device connections, such as IEEE 1901 power line communications.

c. Explain core "IoT" functional stack. **(04 Marks)**

Ans.



1. "Things" layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.

2. Communications network layer: When smart objects are not self contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers:

Access network sublayer: The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired.

Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a longer range medium (called the backhaul) to a headend central station where the information is processed.

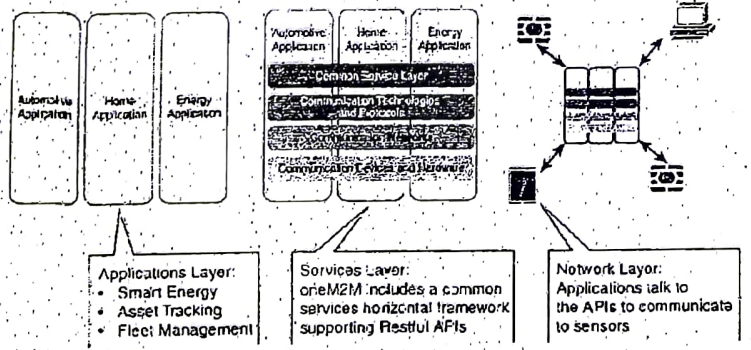
Network transport sublayer: For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use.

IoT network management sublayer: Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.

Privacy	As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment. For businesses, this data has monetary value. Organizations are now discussing who owns this data and how individuals can control whether it is shared and with whom.
Big data and data analytics	IoT and its large number of sensors is going to trigger a deluge of data that must be handled. This data will provide critical information and insights if it can be processed in an efficient maimer. The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner,
Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others are open. Recent IoT standards ate helping minimize this problem. but there are often various protocols and implementations available for IoT networks.

b. With a neat diagram, explain architecture of IoT **(04 Marks)**

Ans.



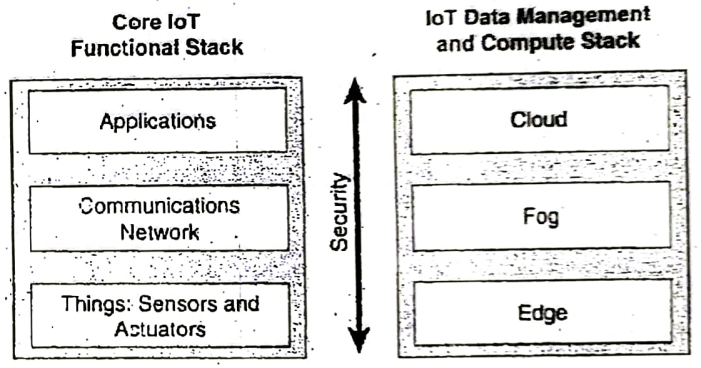
Applications layer: The oneM2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

Services layer: This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the hardware. Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on. Riding on top is the common services layer. This conceptual layer adds APIs and middleware supporting third-party services and applications.

Network layer: This is the communication domain for the IoT devices and endpoints. It includes the devices themselves and the communications network that links them. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah. Also included are wired device connections, such as IEEE 1901 power line communications.

c. Explain core "IoT" functional stack. **(04 Marks)**

Ans.



1. "Things" layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.

2. Communications network layer: When smart objects are not self contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers:

Access network sublayer: The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired.

Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a longer range medium (called the backhaul) to a headend central station where the information is processed.

Network transport sublayer: For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use.

IoT network management sublayer: Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.

3. Application and analytics layer: At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the "things" or other systems to adapt to the analyzed conditions and change their behaviors or parameters.

Module - 2

3. a. List and explain different types of sensors. **(08 Marks)**

Ans. Here is the list of Sensors most commonly used in the IoT devices,

1. Temperature Sensor
2. Pressure Sensor
3. Proximity Sensor
4. Accelerometer and Gyroscope Sensor
5. IR Sensor
6. Optical Sensor
7. Gas Sensor
8. Smoke Sensor

1. Temperature Sensor: A Temperature Sensor senses and measures the temperature and converts it into an electrical signal. They have a major role in Environment, Agriculture and Industries. For example, these sensors can detect the temperature of the soil, which is more helpful in the production of crops.

2. Pressure Sensor: A pressure sensor senses the pressure applied ie, force per unit area, and it converts into an electrical signal. It has high importance in weather forecasting. There are various Pressure sensors available in the market for many purposes.

3. Proximity Sensor: A proximity sensor is a sensor able to detect the presence of nearby objects without any physical contact. A proximity sensor often emits an electromagnetic field or a beam of electromagnetic radiation and looks for changes in the field or return signal. A most common application of this sensor is used in cars.

4. Accelerometer and Gyroscope Sensor: The difference between Accelerometer and the gyroscope is accelerometer measures linear acceleration based on vibration whereas, the gyroscope is intended to determine an angular position based on the principle of the rigidity of space. Accelerometers in mobile phones are used to detect the orientation of the phone. The gyroscope, adds an additional dimension to the information supplied by the accelerometer by tracking rotation or twist. A 3D gyroscope has three gyroscopic sensors mounted orthogonally. Accelerometers and gyroscopes are the sensors of choice for acquiring acceleration and rotational information in drones, cell phones, automobiles, airplanes, and mobile IoT devices.

5. Infrared Sensors: An Infrared Sensor is an electronic device, which senses certain characteristics of its surroundings by emitting Infrared radiation. It has the ability to measure the heat being emitted by an object and also measures the distance. It has been implemented in various applications. It is used in Radiation thermometers depend on the material of the object. IR sensors are also used in Flame monitors

and moisture analysis. IR sensors are used in gas analyzers which use absorption characteristics of gases in the IR region. Two types of methods are used to measure the density of gas such as dispersive and nondispersive. IR imaging devices are used for thermal imagers and also for night vision.

6. Optical Sensors: The Optical Sensors convert light rays into an electronic signal, it measures a physical quantity of light and transforms into a form which is readable, maybe digital form. It detects the electromagnetic energy and sends the results to the units. It involves no optical fibers. It is a great boon to the cameras on mobile phones. Also, it is used in mining, chemical factories, refineries, etc. LASER and LED are the two different types of light source. Optical sensors are integral parts of many common devices, including computers, copy machines (Xerox) and light fixtures that turn on automatically in the dark.

7. Gas Sensor: A Gas Sensor or a Gas detector is a device that detects the gas in an area, which is very helpful in safety systems. It usually detects a gas leak in an area, that results are sent to a control system or a microcontroller, that finally shuts down. it can detect combustible, flammable and toxic gases.

8. Smoke Sensor: A smoke sensor detects smoke and its level of attainment. Nowadays, the manufacturers of the sensor implement it with a voice alarm through ALEXA, also notifies in our smartphones. The smoke sensor if of two types, Optical smoke sensor, and the ionization smoke sensor. The optical smoke sensor also called photoelectric smoke alarms works using the light scattering principle. The alarm contains a pulsed Infrared LED which pulses a beam of light into the sensor chamber every 10seconds to check for smoke particles.

b. Elaborate on small physical objects and small virtual objects. **(04 Marks)**

Ans. Refer Q.no 3 od Model Paper 1

c. Explain "IoT Access Technologies" **(04 Marks)**

Ans. IoT Access Technology is spread across licensed and unlicensed spectrum and there are several number of Radio technologies. At high this access can be classified in two categories:

1. Non –Cellular Technologies
2. Cellular Technologies

Each of the technologies available for IoT connectivity has its own advantages and disadvantages. However, the range of IoT connectivity requirements – both technical and commercial – means cellular technologies can provide clear benefits across a wide variety of applications. While choosing technology following requirement needs to be considered

- It should have Global Reach
- Matured Ecosystem
- Diverse and Secure
- Scalable and QoS support
- Low Total Cost of Ownership (TOC)

A common information set is being provided. Particularly, the following topics are addressed for each IoT access technology:

1. Standardization and alliances: The standards bodies that maintain the protocols for a technology

2. Physical lay : The wired or wireless methods and relevant frequencies

3. MAC layer. the Media Access Control (MAC) layer, which bridges the phy control

4. Topology: T y the technology

5. Security: Security aspects of the technology

6. Competitive technologies: Other technologies that are similar and may be suitable alternatives to the given technology

OR

4. a. Briefly Expla)2.15.4. (08 M

Ans.

Protocol	
ZigBee	P Alliance, r-layer ce h applicati ication pr ron include bu ion, home au and althca e. ZigBee a delines vice object fu such as device role, device di overy, network join, and se For more information on ZigBee, see the ZigBee Alliance w page, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6L0WPAN is an IPv6 adaptation layer defined by the IETF 6L0WPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4.
ZigBee IP	An evolution of the ZigBee protocol stack. ZigBee IP adopts the 6F0WPAN adaptation layer, IPv6 network layer, and RPI. routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETK 6L0WPAN, IPv6, .nut UDP standards.

Wireless HART	WirelessHART, promoted by the HART Communieation Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band, A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/ system-engineering-guidelines-iec-625yi-wirelesshart--dar.a-79y00.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

b. What is SANET? Explain some advantages and disadvantages that a wireless based solution offers. **(08 Marks)**

Ans. A sensor/actuator network (SANET), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment. The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner. Effective and well coordinated communication and cooperation is a prominent challenge, primarily because the sensors and actuators SANETs are diverse, heterogeneous, and resource-constrained.

e following are some advantages and disadvantages that a wireless-based solution ers:

Advantages:

1. Greater deployment flexibility (especially in extreme environments or
2. hard-to-reach places)
3. Simpler scaling to a large number of nodes
4. Lower implementation costs
5. Easier long-term maintenance
6. Effortless introduction of new sensor/actuator nodes
7. Better equipped to handle dynamic/rapid topology changes

Disadvantages:

1. Potentially less secure (for example, hijacked access points)
2. Typically lower transmission speeds
3. Greater level of impact/influence by environment

Module - 3

5. a. Explain working of IP as the IoT network layer. **(08 Marks)**

Ans. IoT network technologies to be aware of toward the bottom of the protocol stack include cellular, wifi, and Ethernet, as well as more specialized solutions such as LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID. When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:

1. Range
2. Bandwidth
3. Power usage
4. Intermittent connectivity
5. Interoperability
6. Security

Range

Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network:

PAN (Personal Area Network)

PAN is short-range, where distances can be measured in meters, such as a wearable fitness tracker device that communicates with an app on a cell phone over BLE.

LAN (Local Area Network)

LAN is short- to medium-range, where distances can be up to hundreds of meters, such as home automation or sensors that are installed within a factory production line that communicate over wifi with a gateway device that is installed within the same building.

MAN (Metropolitan Area Network)

MAN is long-range (city wide), where distances are measured up to a few kilometers, such as smart parking sensors installed throughout a city that are connected in a mesh network topology.

WAN (Wide Area Network)

WAN is long-range, where distances can be measured in kilometers, such as agricultural sensors that are installed across a large farm or ranch that are used to monitor micro-climate environmental conditions across the property.

Bandwidth

Bandwidth, or the amount of data that can be transmitted in a specific period of time, limits the rate at which data can be collected from IoT devices and transmitted upstream.

Power usage

Transmitting data from a device consumes power, and transmitting data over long ranges requires more power than over a short range. You must consider the devices that operate on a battery to conserve power to prolong the life of the battery and reduce operating costs.

Intermittent connectivity

IoT devices aren't always connected. In some cases, devices will connect periodically by design in order to save power or bandwidth.

Interoperability

With so many different devices connecting to the IoT, interoperability can be a challenge. Adopting standard protocols has been the traditional approach for maintaining interoperability on the internet. However, for the IoT, standardization processes sometimes struggle to keep up with the rapid pace of change and

technologies are released based on upcoming versions of standards that are still subject to change.

Security

Security is always a priority, so be sure to select networking technologies that implement end-to-end security, including authentication, encryption, and open port protection.

b. Write note on Business case for IP **(04 Marks)**

Ans. 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. Dedicated applications are then run over virtualized or traditional operating systems or on network edge platforms (for example, fog computing). These lightweight applications communicate with the data center servers. Therefore, the system solutions combining various physical and data link layers call for an architectural approach with a common layer(s) independent from the lower (connectivity) and/or upper (application) layers. This is how and why the Internet Protocol (IP) suite started playing a key architectural role in the early 1990s. IP was not only preferred in the IT markets but also for the OT environment.

c. Discuss need for optimization. **(04 Marks)**

Ans. The Internet of Things will largely be built on the Internet Protocol suite. However, challenges still exist for IP in IoT solutions. In addition to coping with the integration of non-IP devices, you may need to deal with the limits at the device and network levels that IoT often imposes. Therefore, optimizations are needed at various layers of the IP stack to handle the restrictions that are present in IoT networks. The following sections take a detailed look at why optimization is necessary for IP. Both the nodes and the network itself can often be constrained in IoT solutions. Also, IP is transitioning from version 4 to version 6, which can add further confinements in the IoT space.

OR

6. a. Describe application protocols for IoT. **(08 Marks)**

Ans. The IoT application protocols you select should be contingent on the use cases and vertical industries they apply to. In addition, IoT application protocols are dependent on the characteristics of the lower layers themselves. For example, application protocols that are sufficient for generic nodes and traditional networks often are not well suited for constrained nodes and networks.

The Transport Layer: IP-based networks use either TCP or UDP. However, the constrained nature of IoT networks requires a closer look at the use of these traditional transport mechanisms.

IoT Application Transport Methods: This section explores the various types of IoT application data and the ways this data can be carried across a network. As in traditional networks, TCP or UDP are utilized in most cases when transporting IoT

application data. The transport methods are covered in depth and form the bulk of the material in this chapter. You will notice that, as with the lower-layer IoT protocols, there are typically multiple options and solutions presented for transporting IoT application data. This is because IoT is still developing and maturing and has to account for the transport of not only new application protocols and technologies but legacy ones as well.

b. Discuss the various methods used in IoT application transport. (08 Marks)

Ans. The following categories of IoT application protocols and their transport methods are explored in the following sections:

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.

Supervisory control and data acquisition (SCADA): SCADA is one of the most common industrial protocols in the world, but it was developed long before the days of IP, and it has been adapted for IP networks.

Generic web-based protocols: Generic protocols, such as Ethernet, Wi-Fi, and 4G/LTE, are found on many consumer- and enterprise-class IoT devices that communicate over non-constrained networks.

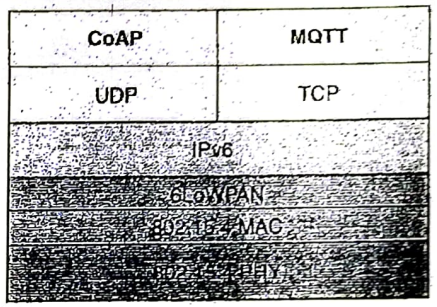
IoT application layer protocols: IoT application layer protocols are devised to run on constrained nodes with a small compute footprint and are well adapted to the network bandwidth constraints on cellular or satellite links or constrained 6LoWPAN networks. Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), covered later in this chapter, are two well-known examples of IoT application layer protocols.

SCADA

In the world of networking technologies and protocols, IoT is relatively new. Combined with the fact that IP is the de facto standard for computer networking in general, older protocols that connected sensors and actuators have evolved and adapted themselves to utilize IP. A prime example of this evolution is supervisory control and data acquisition (SCADA). Designed decades ago, SCADA is an automation control system that was initially implemented without IP over serial links, before being adapted to Ethernet and IPv4.

IoT Application Layer Protocols

When considering constrained networks and/or a large-scale deployment of constrained nodes, verbose web-based and data model protocols. To address this problem, the IoT industry is working on new lightweight protocols that are better suited to large numbers of constrained nodes and networks. Two of the most popular protocols are CoAP and MQTT. Figure 6-6 highlights their position in a common IoT protocol stack.



Module - 4

7. a. What do you mean by data and analytics for IoT? Explain. (04 Marks)

Ans. Data Analytics has a significant role to play in the growth and success of IoT applications and investments. Analytics tools will allow the business units to make effective use of their datasets as explained in the points listed below.

Volume: There are huge clusters of data sets that IoT applications make use of. The business organizations need to manage these large volumes of data and need to analyze the same for extracting relevant patterns. These datasets along with real-time data can be analyzed easily and efficiently with data analytics software.

Structure: IoT applications involve data sets that may have a varied structure as unstructured, semi-structured and structured data sets. There may also be a significant difference in the data formats and types. Data analytics will allow the business executive to analyze all of these varying sets of data using automated tools and software.

Driving Revenue: The use of data analytics in IoT investments will allow the business units to gain an insight into customer preferences and choices. This would lead to the development of services and offers as per the customer demands and expectations. This, in turn, will improve the revenues and profits earned by the organizations.

Competitive Edge: IoT is a buzzword in the current era of technology and there are numerous IoT application developers and providers present in the market. The use of data analytics in IoT investments will provide a business unit to offer better services and will, therefore, provide the ability to gain a competitive edge in the market.

b. Discuss Bigdata analytics tools and technology. (04 Marks)

Ans. Generally, the industry looks to the "three Vs" to categorize big data:

1. Velocity: Velocity refers to how quickly data is being collected and analyzed. Hadoop Distributed File System is designed to ingest and process data very quickly. Smart objects can generate machine and sensor data at a very fast rate and require database or file systems capable of equally fast ingest functions.

2. Variety: Variety refers to different types of data. Often you see data categorized as structured, semi structured, or unstructured. Different database technologies may only be capable of accepting one of these types. Hadoop is able to collect and store all three types. This can be beneficial when combining machine data from IoT devices that is very structured in nature with data from other sources, such as social media or multimedia, that is unstructured.

3. Volume: Volume refers to the scale of the data. Typically, this is measured from gigabytes on the very low end to petabytes or even exabytes of data on the other extreme. Generally, big data implementations scale beyond what is available on locally attached storage disks on a single node. It is common to see clusters of servers that consist of dozens, hundreds, or even thousands of nodes for some large deployments.

c. With a case study relate the concept of securing IoT. **(08 Marks)**

Ans. It is often said that if World War III breaks out, it will be fought in cyberspace. As IoT brings more and 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 and efficient way, security of the networks, devices, and the applications that use them is foundational and essential for all modern communications systems. Providing security in such a world is not easy. Security is among the very few, if not the only, technology disciplines that must operate with external forces continually working against desired outcomes. To further complicate matters, these external forces are able to leverage traditional technology as well as nontechnical methods (for example, physical security, operational processes, and so on) to meet their goals. With so many potential attack vectors, information and cybersecurity is a challenging, but engaging, topic that is of critical importance to technology vendors, enterprises, and service providers alike.

Information technology (IT) environments have faced active attacks and information security threats for many decades, and the incidents and lessons learned are well-known and documented. By contrast, operational technology (OT) environments were traditionally kept in silos and had only limited connection to other networks. Thus, the history of cyber-attacks on OT systems is much shorter and has far fewer incidents documented. Therefore, the learning opportunities and the body of cataloged incidents with their corresponding mitigations are not as rich as in the IT world. Security in the OT world also addresses a wider scope than in the IT world. For example, in OT, the word security is almost synonymous with safety. In fact, many of the industrial security standards that form the foundation for industrial IoT security also incorporate equipment and personnel safety recommendations.

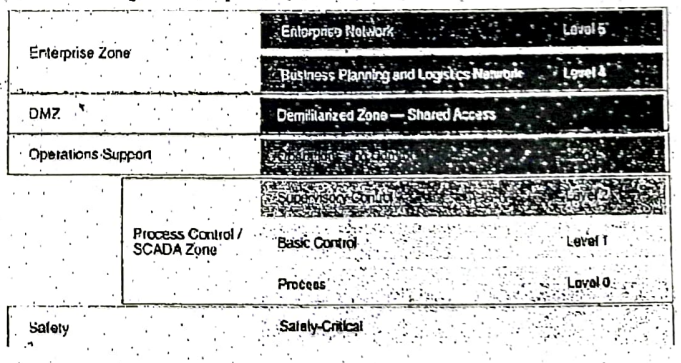
OR

8. a. Explain in detail how IT and OT security practices and systems vary in real time. **(08 Marks)**

Ans. **The Purdue Model for Control Hierarchy**

Regardless of where a security threat arises, it must be consistently and unequivocally treated. IT information is typically used to make business decisions, such as those in process optimization, whereas OT information is instead characteristically leveraged to make physical decisions, such as closing a valve, increasing pressure, and so on. Thus, the operational domain must also address physical safety and environmental factors as part of its security strategy—and this is not normally associated with the IT domain. Organizationally, IT and OT teams and tools have been historically separate, but this has begun to change, and they have started to converge, leading to more traditionally IT-centric solutions being introduced to support operational activities. For example, systems such as firewalls and intrusion prevention systems (IPS) are being used in IoT networks.

As the borders between traditionally separate OT and IT domains blur, they must align strategies and work more closely together to ensure end-to-end security. The types of devices that are found in industrial OT environments are typically much more highly optimized for tasks and industrial protocol-specific operation than their IT counterparts. Furthermore, their operational profile differs as well.



Enterprise zone

- **Level 5: Enterprise network:** Corporate-level applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), document management, and services such as Internet access and VPN entry from the outside world exist at this level.
- **Level 4: Business planning and logistics network:** The IT services exist at this level and may include scheduling systems, material flow applications, optimization and planning systems, and local IT services such as phone, email, printing, and security monitoring.

Industrial demilitarized zone

- DMZ: The DMZ provides a buffer zone where services and data can be shared between the operational and enterprise zones. It also allows for easy segmentation of organizational control. By default, no traffic should traverse the DMZ; everything should originate from or terminate on this area.

Operational zone

- **Level 3: Operations and control:** This level includes the functions involved in managing the workflows to produce the desired end products and for monitoring and controlling the entire operational system. This could include production scheduling, reliability assurance, systemwide control optimization, security management, network management, and potentially other required IT services, such as DHCP, DNS, and timing.
- **Level 2: Supervisory control:** This level includes zone control rooms, controller status, control system network/application administration, and other control-related applications, such as human machine interface (HMI) and historian.
- **Level 1: Basic control:** At this level, controllers and IEDs, dedicated HMIs, and other applications may talk to each other to run part or all of the control function.
- **Level 0: Process:** This is where devices such as sensors and actuators and machines such as drives, motors, and robots communicate with controllers or IEDs.

Safety zone

- **Safety-critical:** This level includes devices, sensors, and other equipment used to manage the safety functions of the control system.

b. Discuss OCTAVE and FAIR formal risk analysis. **(08 Marks)**

Ans. Refer Q. no 8 b of Model Paper 1

Module - 5

9. a. Give a brief note on Arduino UNO **(04 Marks)**

Ans. The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

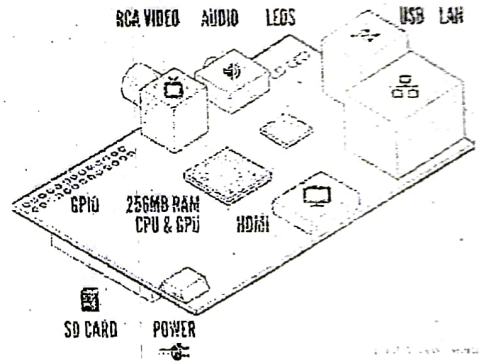
The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Revision 2 of the Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode. Revision 3 of the board has the following new features:

- pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins
- placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes.
- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions

b. With a neat diagram, explain Raspberry PI board. **(04 Marks)**

Ans.



Here are the various components on the Raspberry Pi board:

1. **ARM CPU/GPU** -- This is a Broadcom BCM2835 System on a Chip (SoC) that's made up of an ARM central processing unit (CPU) and a Videocore 4 graphics processing unit (GPU). The CPU handles all the computations that make a computer work (taking input, doing calculations and producing output), and the GPU handles graphics output.
2. **GPIO** -- These are exposed general-purpose input/output connection points that will allow the real hardware hobbyists the opportunity to tinker.
3. **RCA** -- An RCA jack allows connection of analog TVs and other similar output devices.
4. **Audio out** -- This is a standard 3.55-millimeter jack for connection of audio output devices such as headphones or speakers. There is no audio in.
5. **LEDs** -- Light-emitting diodes, for all of your indicator light needs.
6. **USB** -- This is a common connection port for peripheral devices of all types (including your mouse and keyboard). Model A has one, and Model B has two. You can use a USB hub to expand the number of ports or plug your mouse into your keyboard if it has its own USB port.
7. **HDMI** – This connector allows you to hook up a high-definition television or

other compatible device using an HDMI cable.

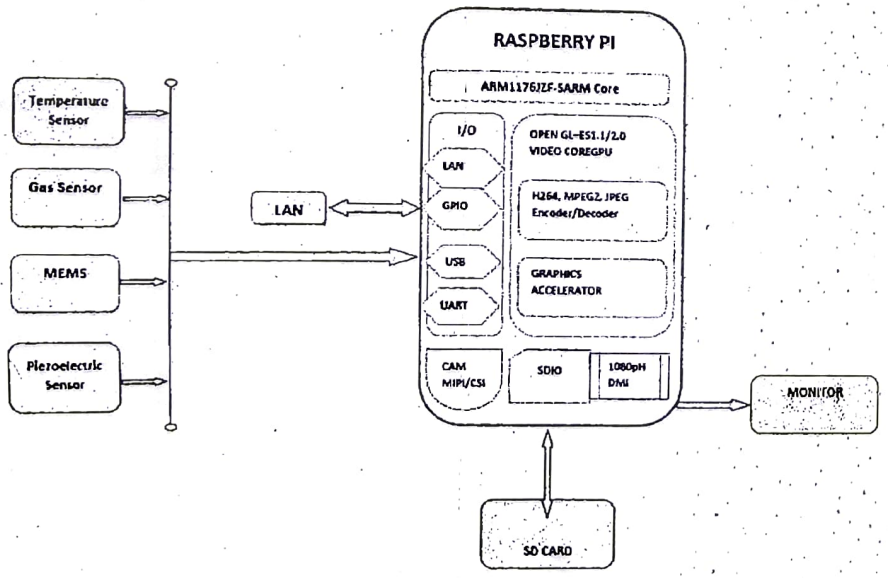
8. Power -- This is a 5v Micro USB power connector into which you can plug your compatible power supply.

9. SD cardslot -- This is a full-sized SD card slot. An SD card with an operating system (OS) installed is required for booting the device. They are available for purchase from the manufacturers, but you can also download an OS and save it to the card yourself if you have a Linux machine and the wherewithal.

10. Ethernet -- This connector allows for wired network access and is only available on the Model B.

c. With a neat diagram, explain wirless temperature monitoring system using Raspberry PI. **(08 Marks)**

Ans.



The components required for the implementation are Digital temperature sensor DS18B20, Resistor4.7kΩ, Breadboard, Jumper Wires, Connecting Wires and Raspberry Pi kit. The resistor is utilized as a 'pull-up' for the data-line. It ensures that the 1-Wire data line is at a described logic level, and limits interference from mechanical sound if the pin is left floating. Jumper wires is used for interfacing raspberry and sensor. Connect GPIO GND [Pin 6] on the Pi to the negative side of the breadboard and link GPIO 3.3V [Pin 1] on the Pi to the positive side on the breadboard. Next step is to insert the DS18B20+ into the breadboard, Connect DS18B20+ GND [Pin 1] to the negative side of the breadboard and + VDD [Pin 3] to the positive side of the breadboard. Next step is to place one arm of 4.7kΩ resistor to DS18B20+ DQ [Pin 2] and other end to the positive side of the breadboard. Finally, link DS18B20+ DQ [Pin 2] to GPIO 4 [Pin 7] alongside a jumper wire.

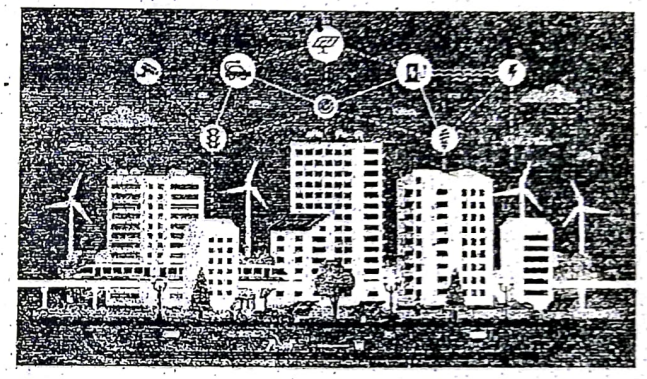
OR

10. a. Explain in detail smart city IoT Architecture **(08 Marks)**

Ans. Refer Q. no 10 b. of Model paper 2

b. With case study explain smart and connected cities using Raspberry PI **(08 Marks)**

Ans.



IoT-enabled smart city use cases span multiple areas: from contributing to a healthier environment and improving traffic to enhancing public safety and optimizing street lighting. Below, we provide an overview of the most popular use cases that are already implemented in smart cities across the globe.

Road traffic

Smart cities ensure that their citizens get from point A to point B as safely and efficiently as possible. To achieve this, municipalities turn to IoT development and implement smart traffic solutions.

Smart traffic solutions use different types of sensors, as well as fetch GPS data from drivers' smart phones to determine the number, location and the speed of vehicles. At the same time, smart traffic lights connected to a cloud management platform allow monitoring green light timings and automatically alter the lights based on current traffic situation to prevent congestion. Additionally, using historical data, smart solutions for traffic management can predict where the traffic could go and take measures to prevent potential congestion.

For example, being one of the most traffic-affected cities in the world, Los Angeles has implemented a smart traffic solution to control traffic flow. Road-surface sensors and closed-circuit television cameras send real-time updates about the traffic flow to a central traffic management platform. The platform analyzes the data and notifies the platform users of congestion and traffic signal malfunctions via desktop user apps. Additionally, the city is deploying a network of smart controllers to automatically make second-by-second traffic lights adjustments, reacting to changing traffic conditions in real time.

Eight Semester B.E. Degree Examination, CBCS - Dec 2019 / Jan 2020

Internet of Things Technology

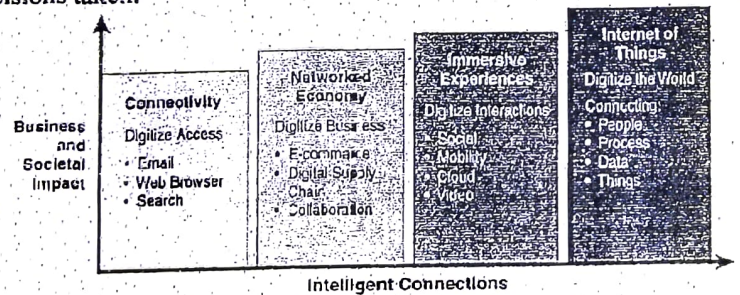
Time: 3 hrs. **Max. Marks: 80**

Note : ***Answer any FIVE full questions, selecting ONE full question from each module.***

Module - 1

1. a. What is IOT? Explain evolutionary phases of the internet. **(06 Marks)**

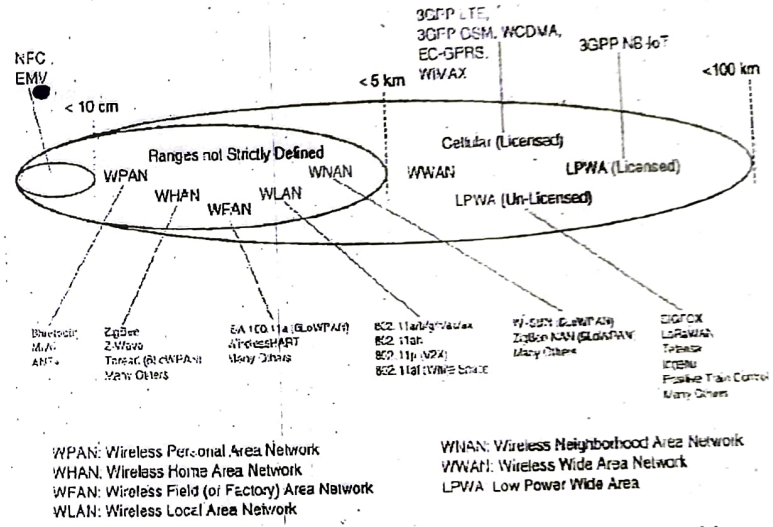
Ans. Internet of Things (IOT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IOT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken.



Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

b. Explain Access Network sublayer with a neat diagram. **(06 Marks)**

Ans. The last mile of the IOT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired.



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network
WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWA: Low Power Wide Area

As IOT continues to grow exponentially, you will encounter a wide variety of applications and special use cases. For each of them, an access technology will be required. IOT sometimes reuses existing access technologies whose characteristics match more or less closely the IOT use case requirements. Whereas some access technologies were developed specifically for IOT use cases, others were not.

One key parameter determining the choice of access technology is the range between the smart object and the information collector. Above Figure lists some access technologies you may encounter in the IOT world and the expected transmission distances.

Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected. Common groups are as follows:

1. **PAN (personal area network):** Scale of a few meters. This is the personal space around a person. A common wireless technology for this scale is Bluetooth.
2. **HAN (home area network):** Scale of a few tens of meters. At this scale, common wireless technologies for IOT include ZigBee and Bluetooth Low Energy (BLE).
3. **NAN (neighborhood area network):** Scale of a few hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.
4. **FAN (field area network):** Scale of several tens of meters to several hundred meters. FAN typically refers to an outdoor area larger than a single group of

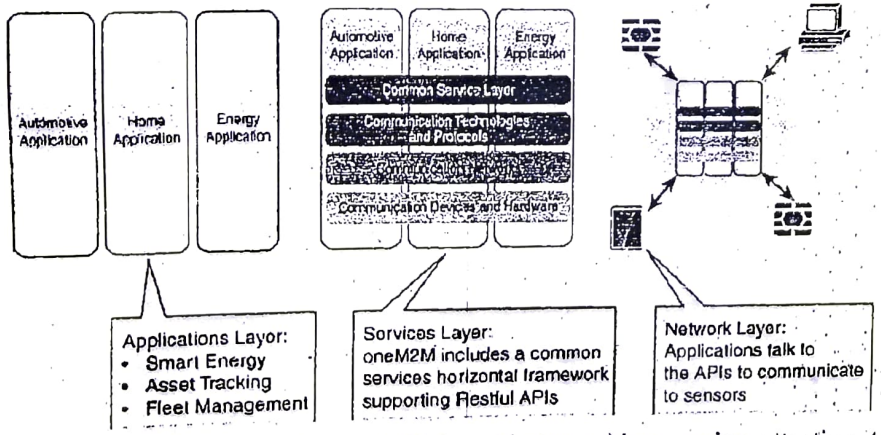
house units. The FAN is often seen as "open space" (and therefore not secured and not controlled). A FAN is sometimes viewed as a group of NANs, but some verticals see the FAN as a group of HANs or a group of smaller outdoor cells. As you can see, FAN and NAN may sometimes be used interchangeably. In most cases, the vertical context is clear enough to determine the grouping hierarchy.

5. **LAN (local area network):** Scale of up to 100 m. This term is very common in networking, and it is therefore also commonly used in the IOT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used. Other networking classifications, such as MAN (metropolitan area network, with a range of up to a few kilometers) and WAN (wide area network, with a range of more than a few kilometers), are also commonly used.

Note that for all these places in the IOT network, a "W" can be added to specifically indicate wireless technologies used in that space. For example, HomePlug is a wired technology found in a HAN environment, but a HAN is often referred to as a WHAN (wireless home area network) when a wireless technology, like ZigBee, is used in that space.

c. **What are the elements of one M2MIOT Architecture? Explain.** (04 Marks)

Ans.



1. **Applications layer:** The oneM2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.
2. **Services layer:** This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IOT applications run on, the underlying management protocols, and the hardware. Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on. Riding on top is the common services layer.

This conceptual layer adds APIs and middleware supporting third-party services and applications. One of the stated goals of oneM2M is to "develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software nodes, and rely upon connecting the myriad of devices in the field area network to M2M application servers, which typically reside in a cloud or data center." A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains, including telematics and intelligent transportation, healthcare, utility, industrial automation, and smart home applications, to name just a few.

3. **Network layer:** This is the communication domain for the IOT devices and endpoints. It includes the devices themselves and the communications network that links them. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah. Also included are wired device connections, such as IEEE 1901 power line communications.

OR

2. a. **Explain the functionality of IOT network management sublayer.** (05 Marks)

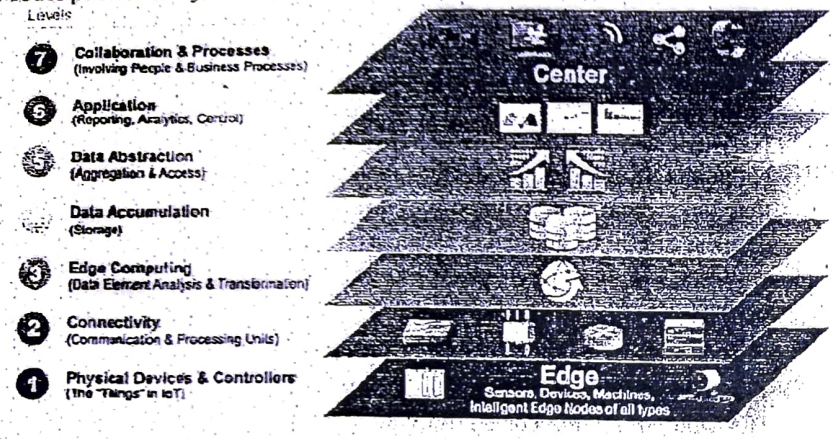
Ans. IP, TCP, and UDP bring connectivity to IOT networks. Upper-layer protocols need to take care of data transmission between the smart objects and other systems. Multiple protocols have been leveraged or created to solve IOT data communication problems. Some networks rely on a push model (that is, a sensor reports at a regular interval or based on a local trigger), whereas others rely on a pull model (that is, an application queries the sensor over the network), and multiple hybrid approaches are also possible.

Following the IP logic, some IOT implementers have suggested HTTP for the data transfer phase. After all, HTTP has a client and server component. The sensor could use the client part to establish a connection to the IOT central application (the server), and then data can be exchanged. You can find HTTP in some IOT applications, but HTTP is something of a fat protocol and was not designed to operate in constrained environments with low memory, low power, low bandwidth, and a high rate of packet failure. Despite these limitations, other web-derived protocols have been suggested for the IOT space. One example is WebSocket. WebSocket is part of the HTML5 specification, and provides a simple bidirectional connection over a single connection. Some IOT solutions use WebSocket to manage the connection between the smart object and an external application. WebSocket is often combined with other protocols, such as MQTT (described shortly) to handle the IOT-specific part of the communication.

b. **Describe IOT World Forum (IOTWF) standardize architecture.** (07 Marks)

Ans. In 2014 the IOTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others) published a seven-layer IOT architectural reference model. While various IOT reference models exist, the one put forth by the IOT World Forum

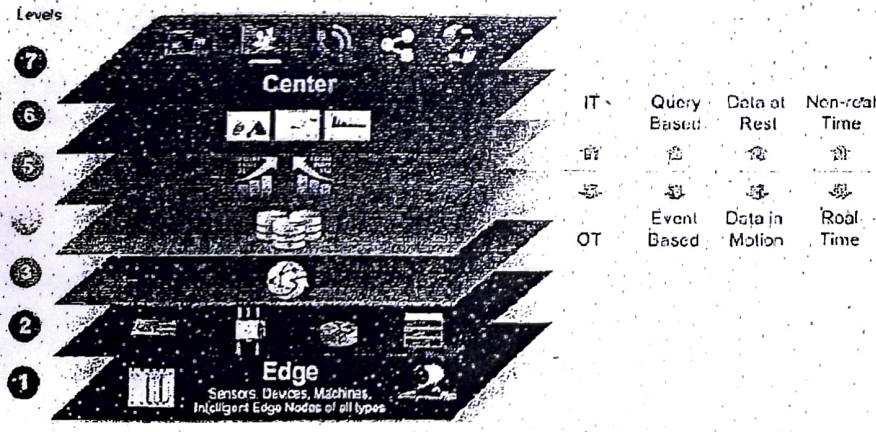
offers a clean, simplified perspective on IOT and includes edge computing, data storage, and access. It provides a succinct way of visualizing IOT from a technical perspective. Each of the seven layers is broken down into specific functions, and security encompasses the entire model. Above Figure details the IOT Reference Model published by the IOTWF.



the IOT Reference Model defines a set of levels with control flowing from the center (this could be either a cloud service or a dedicated data center), to the edge, which includes sensors, devices, machines, and other types of intelligent end nodes. In general, data travels up the stack, originating from the edge, and goes northbound to the center.

c. Compare and contrast IT and OT. **(04 Marks)**

Ans.



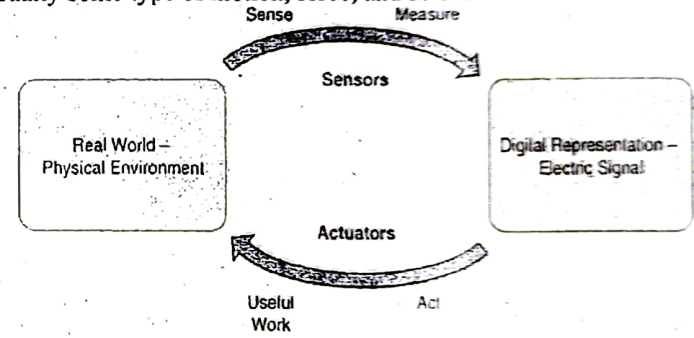
An interesting aspect of visualizing an IOT architecture this way is that you can start to organize responsibilities along IT and OT lines. Above Figure illustrates a natural demarcation point between IT and OT in the IOT Reference Model framework.

IOT systems have to cross several boundaries beyond just the functional layers. The bottom of the stack is generally in the domain of OT. For an industry like oil and gas, this includes sensors and devices connected to pipelines, oil rigs, refinery machinery, and so on. The top of the stack is in the IT area and includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT. In the past, OT and IT have generally been very independent and had little need to even talk to each other. IOT is changing that paradigm.

Module - 2

3. a. With a neat diagram, explain how actuators and sensors interact with physical world. Classify actuators based on energy type. **(08 Marks)**

Ans. Sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human). Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.



Much like sensors, actuators also vary greatly in function, size, design, and so on. Some common ways that they can be classified include the following: Type of motion: Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).

- Power: Actuators can be classified based on their power output (for example, high power, low power, micro power)
- Binary or continuous: Actuators can be classified based on the number of stable-state outputs.
- Area of application: Actuators can be classified based on the specific industry or vertical where they are used.
- Type of energy: Actuators can be classified based on their energy type.

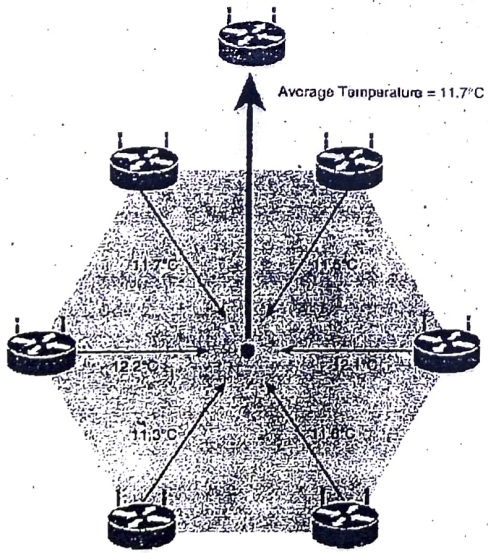
Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode

Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestricrive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

b. List out the limitations of the smart objects in WSNs and explain the data aggregation in WSN with a near diagram. **(08 Marks)**

Ans. The following are some of the most significant limitations of the smart objects in WSNs:

1. Limited processing power
2. Limited memory
3. Lossy communication
4. Limited transmission speeds
5. Limited power



Above Figure shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading. These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSNs with

very large numbers of deployed smart objects. While there are certain instances in which sensors continuously stream their measurement data, this is typically not the case. Wirelessly connected smart objects generally have one of the following two communication patterns:

1. **Event-driven:** Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.
2. **Periodic:** Transmission of sensory information occurs only at periodic intervals.

The decision of which of these communication schemes is used depends greatly on the specific application. For example, in some medical use cases, sensors periodically send postoperative vitals, such as temperature or blood pressure readings. In other medical use cases, the same blood pressure or temperature readings are triggered to be sent only when certain critically low or high readings are measured.

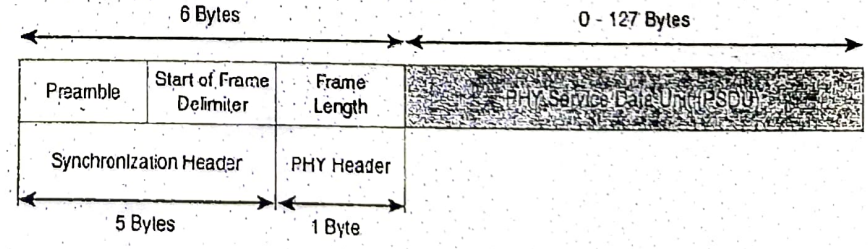
OR

4. a. What is Zigbee? Explain 802.15.4 physical layer, MAC layer, and security. **(08 Marks)**

Ans. Zigbee is based on the IEEE's 802.15.4 personal-area network standard. All you need to know is that Zigbee is a specification that's been around for more than a decade, and it's widely considered an alternative to Wi-Fi and Bluetooth for some applications including low-powered devices that don't require a lot of bandwidth - like your smart home sensors.

Physical Layer

The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands. The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation. DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth. The original physical layer transmission options were as follows: 2.4 GHz, 16 channels, with a data rate of 250 kbps 915 MHz, 10 channels, with a data rate of 40 kbps 868 MHz, 1 channel, with a data rate of 20 kbps



MAC Layer

The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated. At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer

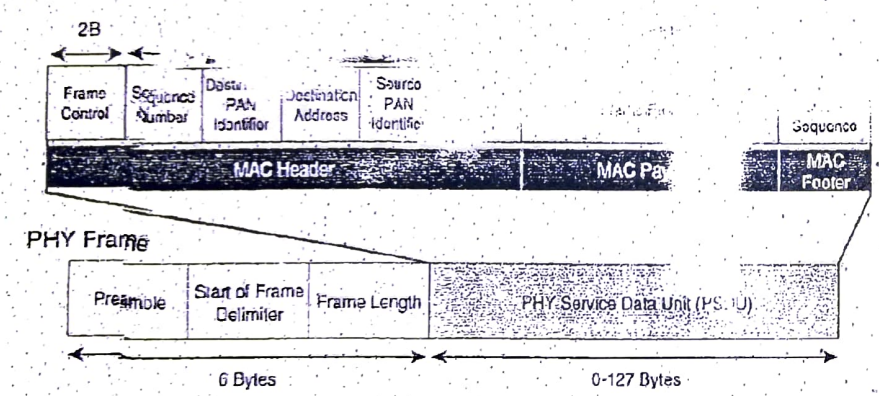
performs the following tasks:

- Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
- PAN association and disassociation by a device
- Device security
- Reliable link communications between two peer MAC entities

The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of MAC frames are specified in 802.15.4:

- Data frame: Handles all transfers of data
- Beacon frame: Used for the transmission of beacons from a PAN coordinator
- Acknowledgment frame: Confirms successful reception of a frame
- MAC command frame: Handles control communication between

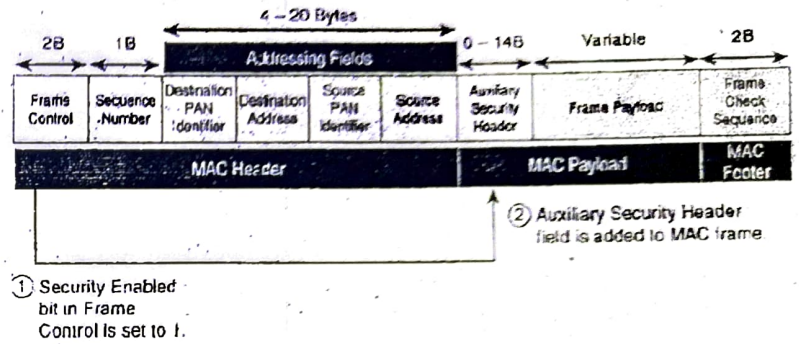
MAC Frame



Security

The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data. Established by the US National Institute of Standards and Technology in 2001, AES is a block cipher, which means it operates on fixed-size blocks of data. The use of AES by the US government and its widespread adoption in the private sector has helped it become one of the most popular algorithms used in symmetric key cryptography. (A symmetric key means that the same key is used for both the encryption and decryption of the data.)

In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent. This is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption.

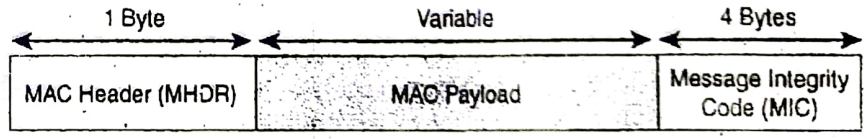


b. Explain LoRaWAN standard and alliance MAC layer and security (08 Marks)

Ans. MAC Layer

The MAC layer is defined in the LoRaWAN specification. This layer takes advantage of the LoRa physical layer and classifies LoRaWAN endpoints to optimize their battery life and ensure downstream communications to the LoRaWAN endpoints. The LoRaWAN specification documents three classes of LoRaWAN devices:

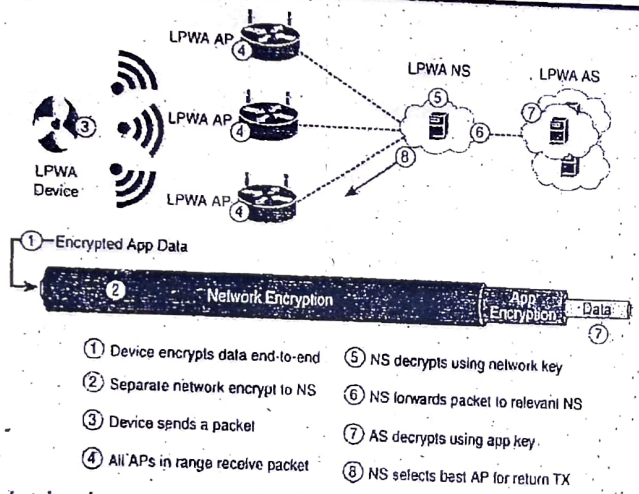
- **Class A:** This class is the default implementation. Optimized for battery powered nodes, it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting. Two receive windows are available after each transmission.
- **Class B:** This class was designated "experimental" in LoRaWAN 1.0.1 until it can be better defined. A Class B node or endpoint should get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process.
- **Class C:** This class is particularly adapted for powered nodes. This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.



Security

Security in a LoRaWAN deployment applies to different components of the architecture, as detailed in Figure. LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.

The first layer, called "network security" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server. Also, it protects LoRaWAN packets by performing encryption based on AES.



Each endpoint implements a network session key (NwkSKey), used by both itself and the LoRaWAN network server. The NwkSKey ensures data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-only data message payloads.

The second layer is an application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server. Furthermore, it computes and checks the application-level MIC, if included. This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access. Endpoints receive their AES-128 application key (AppKey) from the application owner. This key is most likely derived from an application specific root key exclusively known to and under the control of the application provider.

For production deployments, it is expected that the LoRaWAN gateways are protected as well, for both the LoRaWAN traffic and the network management and operations over their backhaul link(s). This can be done using traditional VPN and IPsec technologies that demonstrate scaling in traditional IT deployments. Additional security add-ons are under evaluation by the LoRaWAN Alliance for future revisions of the specification.

LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated. This can be achieved through one of the two join mechanisms:

- **Activation by personalization (ABP):** Endpoints don't need to run a join procedure as their individual details, including DevAddr and the NwkSKey and AppSKey session keys, are preconfigured and stored in the end device. This same information is registered in the LoRaWAN network server.
- **Over-the-air activation (OTAA):** Endpoints are allowed to dynamically join a particular LoRaWAN network after successfully going through a join procedure.

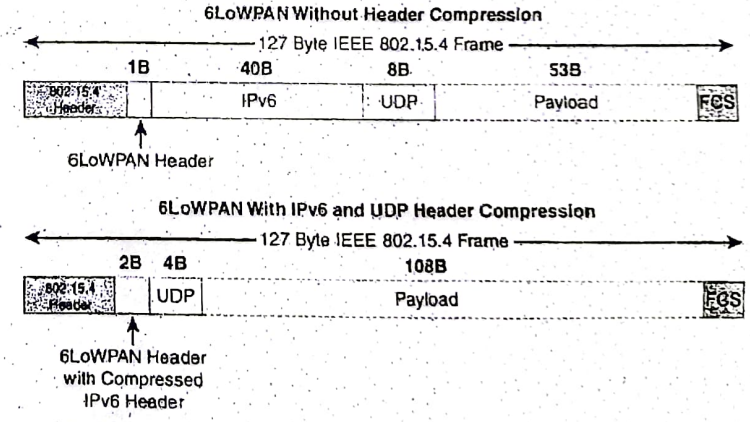
The join procedure must be done every time a session context is renewed. During the join process, which involves the sending and receiving of MAC layer join request and join accept messages, the node establishes its credentials with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey. The AppKey is then used to derive the session NwkSKey and AppSKey keys.

Module - 3

5. a. With a neat diagram, explain 6LOWPAN protocol header compression and fragmentation. (08 Marks)

Ans. Header Compression

IPv6 header compression for 6LoWPAN was defined initially in RFC 4944 and subsequently updated by RFC 6282. This capability shrinks the size of IPv6's 40-byte headers and User Datagram Protocol's (UDP's) 8-byte headers down as low as 6 bytes combined in some cases. Note that header compression for 6LoWPAN is only defined for an IPv6 header and not IPv4. The 6LoWPAN protocol does not support IPv4, and, in fact, there is no standardized IPv4 adaptation layer for IEEE 802.15.4. 6LoWPAN header compression is stateless, and conceptually it is not too complicated. However, a number of factors affect the amount of compression, such as implementation of RFC 4944 versus RFC 6922, whether UDP is included, and various IPv6 addressing scenarios. It is beyond the scope of this book to cover every use case and how the header fields change for each.



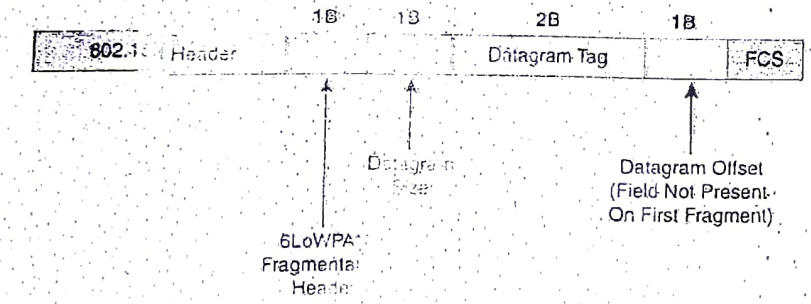
Fragmentation

The maximum transmission unit (MTU) for an IPv6 network must be at least 1280 bytes. The term MTU defines the size of the largest protocol data unit that can be passed. For IEEE 802.15.4, 127 bytes is the MTU. You can see that this is a problem because IPv6, with a much larger MTU, is carried inside the 802.15.4 frame with a much smaller one. To remedy this situation, large IPv6 packets must be fragmented

across multiple 802.15.4 frames at Layer 2.

The fragment header utilized by 6LoWPAN is composed of three primary fields: Datagram Size, Datagram Tag, and Datagram Offset. The 1-byte Datagram Size field specifies the to[illegible]ze of the unfragmented payload. Datagram Tag identifies the set of fragments f[illegible]yload. F[illegible]lly, the Datagram Offset field delineates how far into a payload a[illegible]ccurs. Below figure provides an overview of a 6LoWPAN frag[illegible]

[illegible]mentation Header



b. List and explai[illegible] protocol (04 Marks)

Ans.

- **Adoption is just a matter of time** Ti[illegible]ol is a must and a requirement for any Internet connectivity [illegible]dressing scheme for any data transfer on the web. The limited add[illegible]ity of its predecessor, IPv4, has made the transition to IPv6 unavoida[illegible] Google's figures are revealing an IPv6 adoption rate following an exponenti[illegible]ve, doubling every 6 months.
- **Scalability**: IPv6 offers a highly scalable address scheme. The present scheme of Internet Governance provides at most 2 x 1019 unique, globally routable, addresses. This is many orders of magnitude more that the 2 x 109 that is possible with IPv4 and the 1013 that is the largest estimate of IOT devices that will be used this century. It is quite sufficient to address the needs of any present and future communicating device still allowing it to have many addresses.
- **Solving the NAT barrier**: Due to the limits of the IPv4 address space, the current Internet had to adopt a stopgap solution to face its unplanned expansion: the Network Address Translation (NAT). It enables several users and devices to share the same public IP address. This solution is working but with two main trades-off: The NAT users are borrowing and sharing IP addresses with others. While this technique allows single stakeholders to mount large applications, it becomes completely unmanageable if the same end-points are to be used by many different stakeholders; this would occur in an IOT deployment where the same sensors are to be used by multiple, independent, stakeholders. Secondly the mechanism cannot be used to access specific end-points from the Internet.

- **Multi-Stakeholder Support:** IPv6 provides for end devices to have multiple addresses and an even more distributed routing mechanism than the IPv4 Internet. This allows different stakeholders to assign IOT end-device addresses that are consistent with their own application and network practices. Thus multiple stakeholders can deploy their own applications, sharing a common sensor/ actuation infrastructure, without impacting the technical operation or governance of the Internet.

c. **Explain RPL encryption and authentication on constraint node.** (04 Marks)

Ans. **ACE**

Much like the RoLL working group, the Authentication and Authorization for Constrained Environments (ACE) working group is tasked with evaluating the applicability of existing authentication and authorization protocols and documenting their suitability for certain constrained-environment use cases. Once the candidate solutions are validated, the ACE working group will focus its work on CoAP with the Datagram Transport Layer Security (DTLS) protocol.

DICE

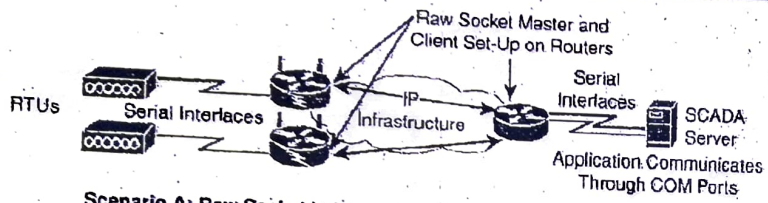
New generations of constrained nodes implementing an IP stack over constrained access networks are expected to run an optimized IP protocol stack. For example, when implementing UDP at the transport layer, the IETF Constrained Application Protocol (CoAP) should be used at the application layer. In constrained environments secured by DTLS, CoAP can be used to control resources on a device. (Constrained environments are network situations where constrained nodes and/or constrained networks are present.

The DTLS in Constrained Environments (DICE) working group focuses on implementing the DTLS transport layer security protocol in these environments. The first task of the DICE working group is to define an optimized DTLS profile for constrained nodes. In addition, the DICE working group is considering the applicability of the DTLS record layer to secure multicast messages and investigating how the DTLS handshake in constrained environments can get optimized.

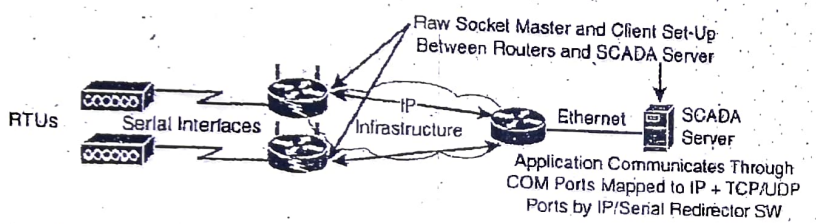
OR

6. a. **Explain tunneling legacy SCADA over IP networks and SCADA protocol translation with a neat diagram.** (08 Marks)

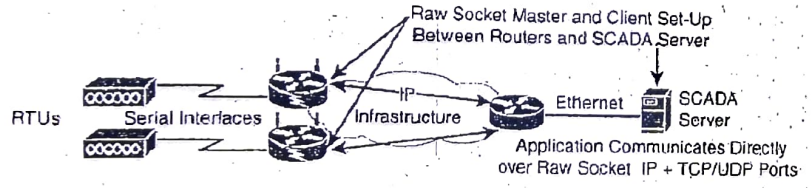
Ans. Deployments of legacy industrial protocols, such as DNP3 and other SCADA protocols, in modern IP networks call for flexibility when integrating several generations of devices or operations that are tied to various releases and versions of application servers. Native support for IP can vary and may require different solutions. Ideally, end-to-end native IP support is preferred, using a solution like IEEE 1815 2012 in the case of DNP3. Otherwise, transport of the original serial protocol over IP can be achieved either by tunneling using raw sockets over TCP or UDP or by installing an intermediate device that performs protocol translation between the serial protocol version and its IP implementation.



Scenario A: Raw Socket between Routers – no change on SCADA server



Scenario B: Raw Socket between Router and SCADA Server – no SCADA application change on server but IP/Serial Redirector software and Ethernet interface to be added



Scenario C: Raw Socket between Router and SCADA Server – SCADA application knows how to directly communicate over a Raw Socket and Ethernet interface

A raw socket connection simply denotes that the serial data is being packaged directly into a TCP or UDP transport. A socket in this instance is a standard application programming interface (API) composed of an IP address and a TCP or UDP port that is used to access network devices over an IP network. More modern industrial application servers may support this capability, while older versions typically require another device or piece of software to handle the transition from pure serial data to serial over IP using a raw socket. Above Figure details raw socket scenarios for a legacy SCADA server trying to communicate with remote serial devices.

In all the scenarios in above figure, notice that routers connect via serial interfaces to the remote terminal units (RTUs), which are often associated with SCADA networks. An RTU is a multipurpose device used to monitor and control various systems, applications, and devices managing automation. From the master/slave perspective, the RTUs are the slaves. Opposite the RTUs in each Figure scenario is a SCADA server, or master, that varies its connection type. In reality, other legacy industrial

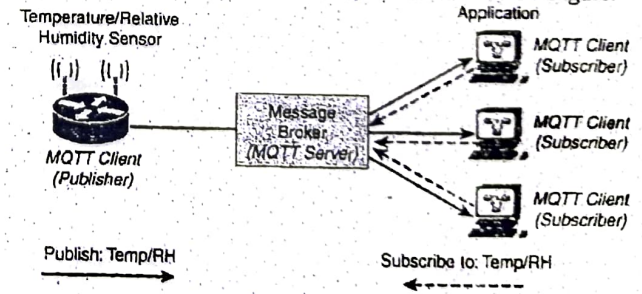
application servers could be shown here as well.

In Scenario A in Figure, both the SCADA server and the RTUs have a direct serial connection to their respective routers. The routers terminate the serial connections at both ends of the link and use raw socket encapsulation to transport the serial payload over the IP network. Scenario B has a small change on the SCADA server side. A piece of software is installed on the SCADA server that maps the serial COM ports to IP ports. This software is commonly referred to as an IP/serial redirector. The IP/serial redirector in essence terminates the serial connection of the SCADA server and converts it to a TCP/IP port using a raw socket connection. In Scenario C in Figure, the SCADA server supports native raw socket capability. Unlike in Scenarios A and B, where a router or IP/serial redirector software has to map the SCADA server's serial ports to IP ports, in Scenario C the SCADA server has full IP support for raw socket connections.

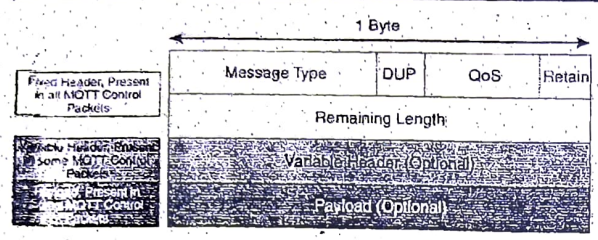
b. Describe MQTT framework and message format in detail. **(08 Marks)**

Ans. Message Queuing Telemetry Transport (MQTT)

At the end of the 1990s, engineers from IBM and Arcom (acquired in 2006 by Eurotech) were looking for a reliable, lightweight, and cost-effective protocol to monitor and control a large number of sensors and their data from a central server location, as typically used by the oil and gas industries. Their research resulted in the development and implementation of the Message Queuing Telemetry Transport (MQTT) protocol that is now standardized by the Organization for the Advancement of Structured Information Standards. Considering the harsh environments in the oil and gas industries, an extremely simple protocol with only a few options was designed, with considerations for constrained nodes, unreliable WAN backhaul communications, and bandwidth constraints with variable latencies. These were some of the rationales for the selection of a client/server and publish/subscribe framework based on the TCP/IP architecture, as shown in below Figure.



MQTT is a lightweight protocol because each control packet consists of a 2- byte fixed header with optional variable header fields and optional payload. You should note that a control packet can contain a payload up to 256 MB. Below Figure provides an overview of the MQTT message format.



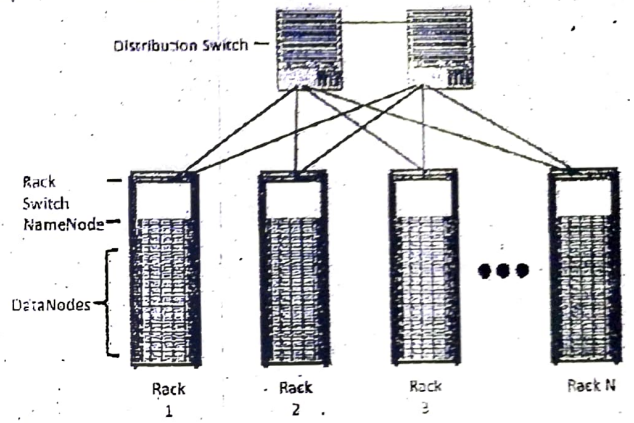
Message Type	Value	Flow	Description
CONNECT	1	Client to server	Request to connect
CONNACK	2	Server to client	Connect acknowledgement
PUBLISH	3	Client to server Server to client	Publish message
PUBACK	4	Client to server Server to client	Publish acknowledgement
PURREC	5	Client to server Server to client	Publish received
PUEREL	6	Client to server Server to client	Publish release
PTJBCOMP	7	Client to server Server to client	Publish complete
SUBSCRIM	8	Client to server	Subscribe request
SUBACK	9	Server to client	Subscribe acknowledgement
UNSUBSCRIBE	10	Client to server	Unsubscribe request
UNSUBACK	11	Server to client	Unsubscribe acknowledgement
PINGRBQ	12	Client to server	Ping request
PINGRESP	13	Server to client	Ping response
DISCONNLCT	14	Client to server	Client disconnecting

Module - 4

7. a. Explain the elements of Hadoop with a neat diagram. **(07 Marks)**

Ans. Hadoop is the most recent entrant into the data management market, but it is arguably the most popular choice as a data repository and processing engine. Hadoop was originally developed as a result of projects at Google and Yahoo!, and the original intent for Hadoop was to index millions of websites and quickly return search results for open source search engines. Initially, the project had two key elements:

- **Hadoop Distributed File System (HDFS):** A system for storing data across multiple nodes
- **MapReduce:** A distributed processing engine that splits a large task into smaller ones that can be run in parallel



Hadoop relies on a scale-out architecture that leverages local processing, memory, and storage to distribute tasks and provide a scalable storage system for data. Both MapReduce and HDFS take advantage of this distributed architecture to store and process massive amounts of data and are thus able to leverage resources from all nodes in the cluster. For HDFS, this capability is handled by specialized nodes in the cluster, including NameNodes and DataNodes

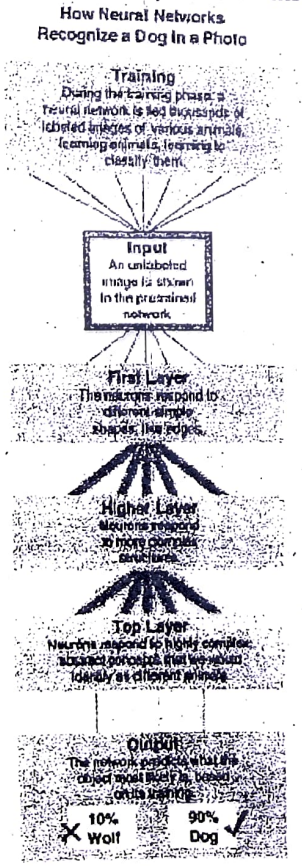
NameNodes: These are a critical piece in data adds, moves, deletes, and reads on HDFS. They coordinate where the data is stored, and maintain a map of where each block of data is stored and where it is replicated. All interaction with HDFS is coordinated through the primary (active) NameNode, with a secondary (standby) NameNode notified of the changes in the event of a failure of the primary. The NameNode takes write requests from clients and distributes those files across the available nodes in configurable block sizes, usually 64 MB or 128 MB blocks. The NameNode is also responsible for instructing the DataNodes where replication should occur.

DataNodes: These are the servers where the data is stored at the direction of the NameNode. It is common to have many DataNodes in a Hadoop cluster to store the data. Data blocks are distributed across several nodes and often are replicated three, four, or more times across nodes for redundancy. Once data is written to one of the DataNodes, the DataNode selects two (or more) additional nodes, based on replication policies, to ensure data redundancy across the cluster. Disk redundancy techniques such as Redundant Array of Independent Disks (RAID) are generally not used for HDFS because the NameNodes and DataNodes coordinate block-level redundancy with this replication technique.

b. Explain neural network in machine learning with a detailed example. **(05 Marks)**

Ans. Neural networks are ML methods that mimic the way the human brain works. When you look at a human figure, multiple zones of your brain are activated to recognize

colors, movements, facial expressions, and so on. Your brain combines these elements to conclude that the shape you are seeing is human. Neural networks mimic the same logic. The information goes through different algorithms (called units), each of which is in charge of processing an aspect of the information. The resulting value of one unit computation can be used directly or fed into another unit for further processing to occur. In this case, the neural network is said to have several layers. For example, a neural network processing human image recognition may have two units in a first layer that determines whether the image has straight lines and sharp angles because vehicles commonly have straight lines and sharp angles, and human figures do not. If the image passes the first layer successfully (because there are no or only a small percentage of sharp angles and straight lines), a second layer may look for different features (presence of face, arms, and so on), and then a third layer might compare the image to images of various animals and conclude that the shape is a human (or not). The great efficiency of neural networks is that each unit processes a simple test, and therefore computation is quite fast. This model is demonstrated



c. Describe the components of FNF. **(04 Marks)**

Ans.

- **FNF Flow Monitor (NetFlow cache):** The FNF Flow Monitor describes the NetFlow cache or information stored in the cache. The Flow Monitor contains the flow record definitions with key fields (used to create a flow, unique per flow record: match statement) and non-key fields (collected with the flow as attributes or characteristics of a flow) within the cache. Also, part of the Flow Monitor is the Flow Exporter, which contains information about the export of NetFlow information, including the destination address of the NetFlow collector. The Flow Monitor includes various cache characteristics, including timers for exporting, the size of the cache, and, if required, the packet sampling rate.
- **FNF flow record:** A flow record is a set of key and non-key NetFlow field values used to characterize flows in the NetFlow cache. Flow records may be predefined for ease of use or customized and user defined. A typical predefined record aggregates flow data and allows users to target common applications for NetFlow. User-defined records allow selections of specific key or non-key fields in the flow record. The user-defined field is the key to Flexible NetFlow, allowing a wide range of information to be characterized and exported by NetFlow. It is expected that different network management applications will support specific user-defined and predefined flow records based on what they are monitoring (for example, security detection, traffic analysis, capacity planning).
- **FNF Exporter:** There are two primary methods for accessing NetFlow data: Using the show commands at the command-line interface (CLI), and using an application reporting tool. NetFlow Export, unlike SNMP polling, pushes information periodically to the NetFlow reporting collector. The Flexible NetFlow Exporter allows the user to define where the export can be sent, the type of transport for the export, and properties for the export. Multiple exporters can be configured per FlowMonitor.
- **Flow export timers:** Timers indicate how often flows should be exported to the collection and reporting server.
- **NetFlow export format:** This simply indicates the type of flow reporting format.
- **NetFlow server for collection and reporting:** This is the destination of the flow export. It is often done with an analytics tool that looks for anomalies in the traffic patterns.

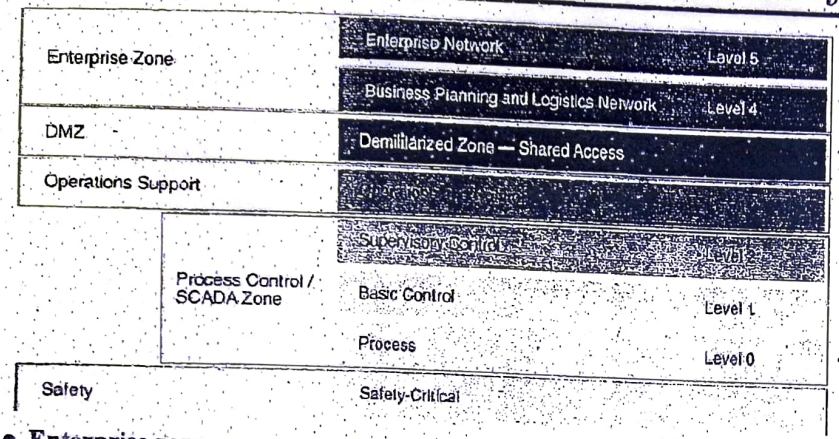
OR

8. a. Explain Formal Risk Analysis Structures. **(08 Marks)**

Ans. Refer Q. no 8 b of June/July 2019

b. Explain the purude model for control hierarchy and OT network characteristics. **(08 Marks)**

Ans. This model identifies levels of operations and defines each level. The enterprise and operational domains are separated into different zones and kept in strict isolation via an industrial demilitarized zone (DMZ):



- **Enterprise zone**
  1. Level 5: Enterprise network: Corporate-level applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), document management, and services such as Internet access and VPN entry from the outside world exist at this level.
  2. Level 4: Business planning and logistics network: The IT services exist at this level and may include scheduling systems, material flow applications, optimization and planning systems, and local IT services such as phone, email, printing, and security monitoring.
- **Industrial demilitarized zone**
  1. DMZ: The DMZ provides a buffer zone where services and data can be shared between the operational and enterprise zones. It also allows for easy segmentation of organizational control. By default, no traffic should traverse the DMZ; everything should originate from or terminate on this area.
- **Operational zone**
  1. Level 3: Operations and control: This level includes the functions involved in managing the workflows to produce the desired end products and for monitoring and controlling the entire operational system. This could include production scheduling, reliability assurance, systemwide control optimization, security management, network management, and potentially other required IT services, such as DHCP, DNS, and timing.
  2. Level 2: Supervisory control: This level includes zone control rooms, controller status, control system network/application administration, and other control-related applications, such as human machine interface (HMI) and historian.
  3. Level 1: Basic control: At this level, controllers and IEDs, dedicated HMIs, and other applications may talk to each other to run part or all of the control function.

4. Level 0: Process: This is where devices such as sensors and actuators and machines such as drives, motors, and robots communicate with controllers or IEDs

- **Safety zone**
  1. Safety-critical: This level includes devices, sensors, and other equipment used to manage the safety functions of the control system.

Module - 5

9. a. Explain the following with respect to Arduino programming.
i) Structure ii) Functions
iii) Variables iv) Flow control statements
v) Data type vi) Constants. (08 Marks)

Ans. **i) Structure:** Arduino programs can be divided in three main parts: Structure, Values (variables and constants), and Functions. In this tutorial, we will learn about the Arduino software program, step by step, and how we can write the program without any syntax or compilation error. Let us start with the Structure. Software structure consist of two main functions – Setup( ) function, Loop( ) function

```
Void setup ( ) {
}
```

PURPOSE – The setup() function is called when a sketch starts. Use it to initialize the variables, pin modes, start using libraries, etc. The setup function will only run once, after each power up or reset of the Arduino board.

INPUT – -
OUTPUT – -
RETURN – -

```
Void Loop ( ) {
}
```

PURPOSE – After creating a setup() function, which initializes and sets the initial values, the loop() function does precisely what its name suggests, and loops consecutively, allowing your program to change and respond. Use it to actively control the Arduino board.

INPUT – -
OUTPUT – -
RETURN – -

ii) Functions: A function is declared outside any other functions, above or below the loop function. We can declare the function in two different ways – The first way is just writing the part of the function called a function prototype above the loop function, which consists of – Function return type Function name Function argument type, no need to write the argument name Function prototype must be followed by a semicolon (;). The following example shows the demonstration of the function declaration using the first method.

Example

```
int sum_func (int x, int y) // function declaration {
  int z = 0;
  z = x+y ;
  return z; // return the value
}
void setup () {
  Statements // group of statements
}
Void loop () {
  int result = 0 ;
  result = Sum_func (5,6) ; // function call
}
```

iii) Variables: Variables that are declared inside a function or block are local variables. They can be used only by the statements that are inside that function or block of code. Local variables are not known to function outside their own. Following is the example using local variables

```
Void setup () {
}
Void loop () {
  int x , y ;
  int z ; Local variable declaration
  x = 0;
  y = 0; actual initialization
  z = 10;
}
```

iv) Flow Control statements:

S.No.	Control Statement & Description
1	If statement It takes an expression in parenthesis and a statement or block of statements. If the expression is true then the statement or block of statements gets executed otherwise these statements are skipped.
2	If …else statement An **if** statement can be followed by an optional else statement, which executes when the expression is false.
3	If…else if …else statement The **if** statement can be followed by an optional **else if...else** statement, which is very useful to test various conditions using single if...else if statement.

4	switch case statement Similar to the if statements, **switch...case** controls the flow of programs by allowing the programmers to specify different codes that should be executed in various conditions.
5	Conditional Operator ? : The conditional operator ? : is the only ternary operator in C.

v) Data Type: Data types in C refers to an extensive system used for declaring variables or functions of different types. The type of a variable determines how much space it occupies in the storage and how the bit pattern stored is interpreted. The following table provides all the data types that you will use during Arduino programming.

void	Boolean	char	Unsigned char	byte	int	Unsigned int	word
long	Unsigned long	short	float	double	array	String-char array	String-object

vii) Constants: The const keyword stands for constant. It is a variable qualifier that modifies the behavior of the variable, making a variable "read-only". This means that the variable can be used just as any other variable of its type, but its value cannot be changed. You will get a compiler error if you try to assign a value to a const variable. Constants defined with the const keyword obey the rules of variable scoping that govern other variables. This, and the pitfalls of using #define, makes the const keyword a superior method for defining constants and is preferred over using #define.

Example Code

```
const float pi = 3.14;
float x;
// ....
x = pi * 2; // it's fine to use consts in math
pi = 7;    // illegal - you can't write to (modify) a constant
```

b. Explain Raspberry Pi learning board. **(08 Marks)**

Ans. Refer Q. no 9 b of June/July 2019

OR

10. a. Write a python program on Raspberry Pi to blink an LED. **(06 Marks)**

Ans.

```
/*
  Blink
  Turns on an LED on for one second, then off for one second, repeatedly.
*/
// the setup function runs once when you press reset or power the board
void setup() {  // initialize digital pin 13 as an output.
  pinMode(2, OUTPUT);
```

```
}
// the loop function runs over and over again forever
void loop() {
  digitalWrite(2, HIGH); // turn the LED on (HIGH is the voltage level)
  delay(1000); // wait for a second
  digitalWrite(2, LOW); // turn the LED off by making the voltage LOW
  delay(1000); // wait for a second
}
```

b. Explain smart city security architecture.

Ans. Refer Q. no 10 a. of June/July 2019 **(06 Marks)**

c. Write a short note on:
i) IOT Challenges.
ii) Backhaul Technologies.

Ans. **i) IOT Challenges:** Refer Q. no 2 a. of June/July 2019 **(04 Marks)**

ii) Backhaul Technologies: Manufacturers of network switching equipment use the term to mean "getting data to the network backbone" (which is similar to its use in the satellite communication industry). For example, Ascend uses the term to describe how its MAX 2000 switch can be used to interconnect data from a backhaul T-1 line on which mobile and remote office users are connected to an Internet service provider and the backbone of the Internet. Backhauling may sometimes be used to mean the use of the back channel on a bidirectional communications line.