Subject: IOT (

Module-1

Assignment

ACY-2020-21

1SV17CS004

Date: / /

Page No. 1

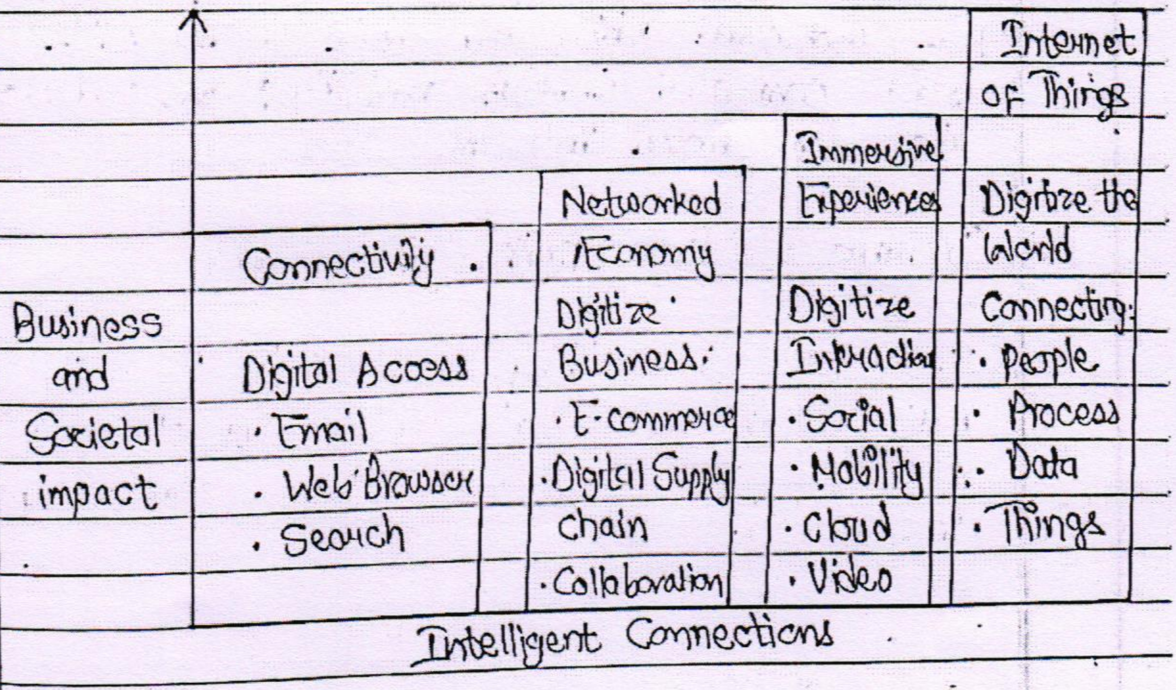
1. What is IOT? Explain the Genesis of IOT.

→ IOT is a technology in which devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.

When objects and machines are sensed and controlled remotely across a network, a tighter integration between the physical world and computers is enabled.

Genesis of IOT

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.



Date: / /
Page No.

The evolution of the Internet can be categorized into four phases. Each of these phases had a profound impact on our society and our lives. These four phases are further defined in below:

i) Connectivity (Digitize access)

This phase connected people to email, web services and search so that information is easily accessed.

ii) Networked Economy (Digitize Business)

This phase enabled e-commerce and supply chain enhancements along with the collaborative engagement to drive increased efficiency in business processes.

iii) 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.

iv) 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.

PRINCIPAL
SIET TUMAKURU.

Date: / /
Page No.

2. What does IoT and digitization mean? Elaborate on this concept.

→ 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 defined and 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.

Digitization, as defined in its simplest form, is the conversion of information into a digital format. Digitization has been happening in one or the other form for several decades.

For example, the whole photography industry has been digitized. Pretty much everyone has a digital cameras these days, either standalone devices or built into their mobile phones.

Almost no one has to buy films and takes it to a retailer to get it developed. The digitization of photography has completely charged our experience when it comes to capturing images.

Date: / /
Page No.

3. Write a short note on "IOT" impact in Real World.

→ IoT has various impacts in real world. 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 predicts in 2020, it may go upto 50 billion and says this new connection will lead to $19 trillion in profit and cost savings. Managing and monitoring smart objects using real-time connectivity enables a new level-data-driven decision making.

- Connected Roadways: It is a term associated with both drivers and driverless cars fully integrating with the surrounding transportation infrastructure.

- Connected Car: With automated vehicle tracking, a vehicle's location is used for notification of arrival times, theft prevention of high way assistance.

- Connected Factory: "Machine to people" connections are implemented to bring sensor data directly to operator via mobile devices. Real Time Location System for status of product.

- Smart Connected Buildings: Sensors are used to control the heating, ventilation and air-conditioning system. Building Automation System provides a single management system for HVAC, lighting and alarm detection system.

- Smart Creatures - IOT Enabled Roach to find survivors IOT provides the ability to connect living things to the Internet. Sensors can be placed on roaches to save life in disaster situations.

PRINCIPAL
SIET., TUMAKURU.

Scanned with CamScanner

Date: / /

Page No.

4. Discuss IOT challenges.

→ The most significant challenges that IOT is currently facing are:

Scale

- IT networks scale is larger. The scale of IOT is several orders of magnitude larger.
- Example: Electrical Company is deployed tons of millions meters in service area where they employed tons of thousands of employees for acting as IP Nodes using IPv6.
- i.e. the scale of network, the utility is managing has increased by more than 1000 fold.

Security

- With more "things" connected with other "things" and people security is an increasingly complex issue for IoT.
- Threat surface is greatly expanded and if device gets hacked, its connectivity is a major concern.
- A compromised device can severe as a launching point to attack other devices and systems.

Privacy

- A sensor become more prolific in every day lives, the data what they gather will be specific to individual and their activities.
- Example: Health information, Shopping patterns, transactions at retail establishments.
- For Businesses, the data has monetary value.
- Organizations discusses about who owns the data and how individuals can control whether it is shared and with whom.

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

Big Data and Data Analytics.

- IoT and lauge number of sensors are going to trigger deluge of data that must be handled.
- This data will provide critical information and insights if it can be processed in an efficient manner.
- Challenge is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner.
- Since the number of IoT devices and the amount of data generated from these devices is increasing at fast pace, it is challenging to analyze the data and evaluate it.
- It takes a huge amount of time to process the data generate the required analysis.

Interoperability

- As with nascent technology, various protocols and architectures are jockeying for market share and standardizations within IoT.
- Some of these protocols and architectures are based on proprietary elements and others are open.
- Recently IoT standards are helping minimize the problem, but there are often various protocols and implementations available for IoT networks.
- The prominent protocols and architectures - especially open, standard-based implementations can be challenge for IoT.
- Thus, interoperability can be a challenge for IoT as some proprietary based protocols are present.

5. With a neat diagram, explain architecture of IoT. :

→ One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods.

By developing a horizontal platform architecture, oneM2M is developing standards that allow interoperability at all levels of the IOT stack.

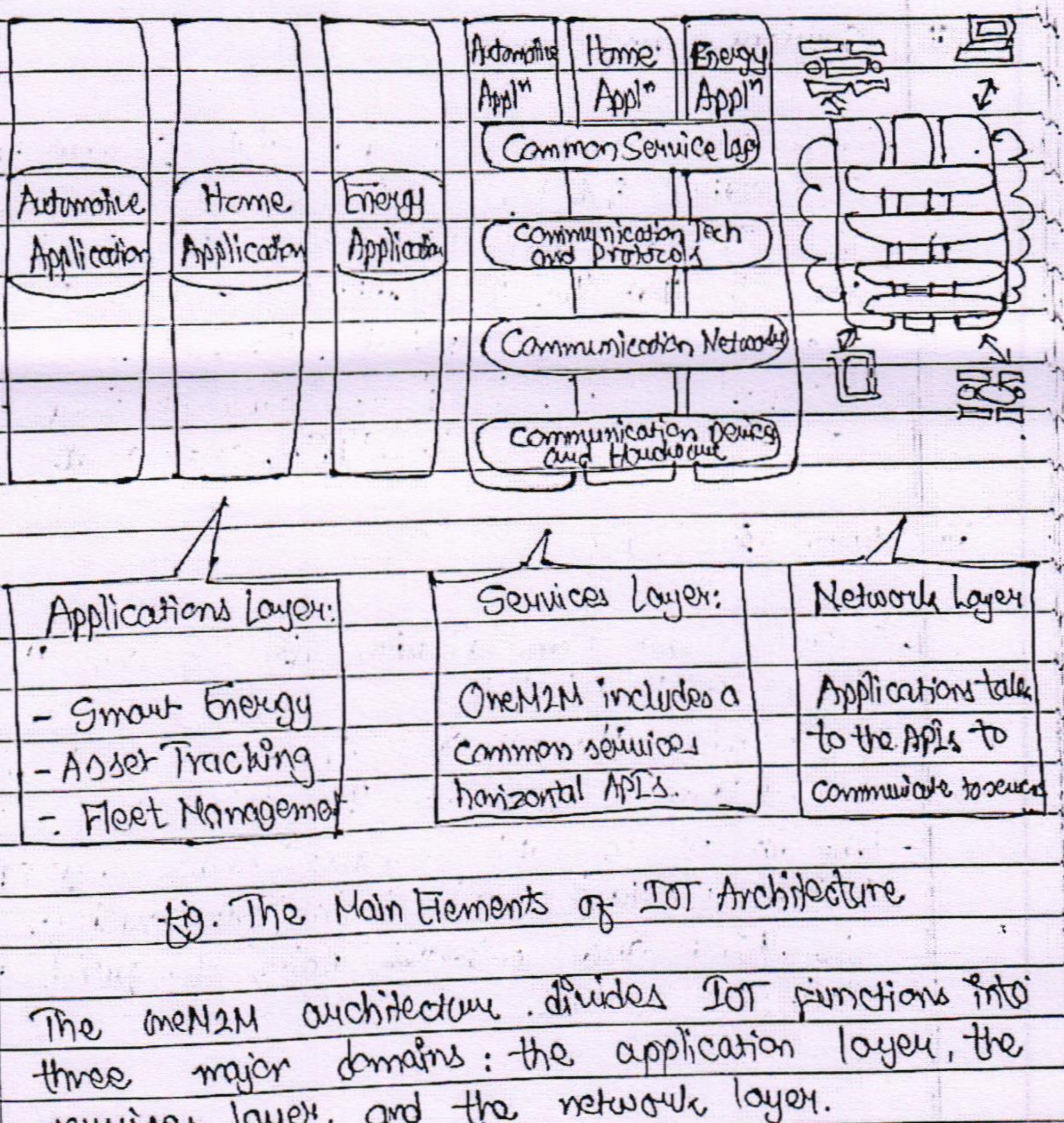


fig. The Main Elements of IoT Architecture

The oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer.

PRINCIPAL
SIET., TUMAKURU.

i) Applications Layer

- The architecture gives major attention to connectivity between devices and their applications.
- The domain includes the application-layer protocols and attempts to standardize northbound API definition for interactions with BI systems.
- Applications tend to be industry specific and have their own sets of data models.

ii) Services Layer

- This layer is shown as 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.

iii) 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 infrastructures include wireless mesh technologies, such as IEEE 802.15.4, and wireless point to point and multipoint systems.

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

6. Explain Core IoT functional stack.

→ IoT network are built around the concept of "things" or smart objects.
The components of an IoT network are as follows:

i) "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.

ii) 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. The four layers under this layer are:
a) Access network sublayer: The last mile of the IoT network is the access network made up of wireless technologies.
b) Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway.
c) Network transport Layer: IP and UDP must be implemented to support the variety of devices to connect & use.
d) IoT Network management sublayer: Additional protocols must be in place for headened applications to exchange data.

iii) 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 charge their behaviors or paarameters.

PRINCIPAL
SIET., TUMAKURU.

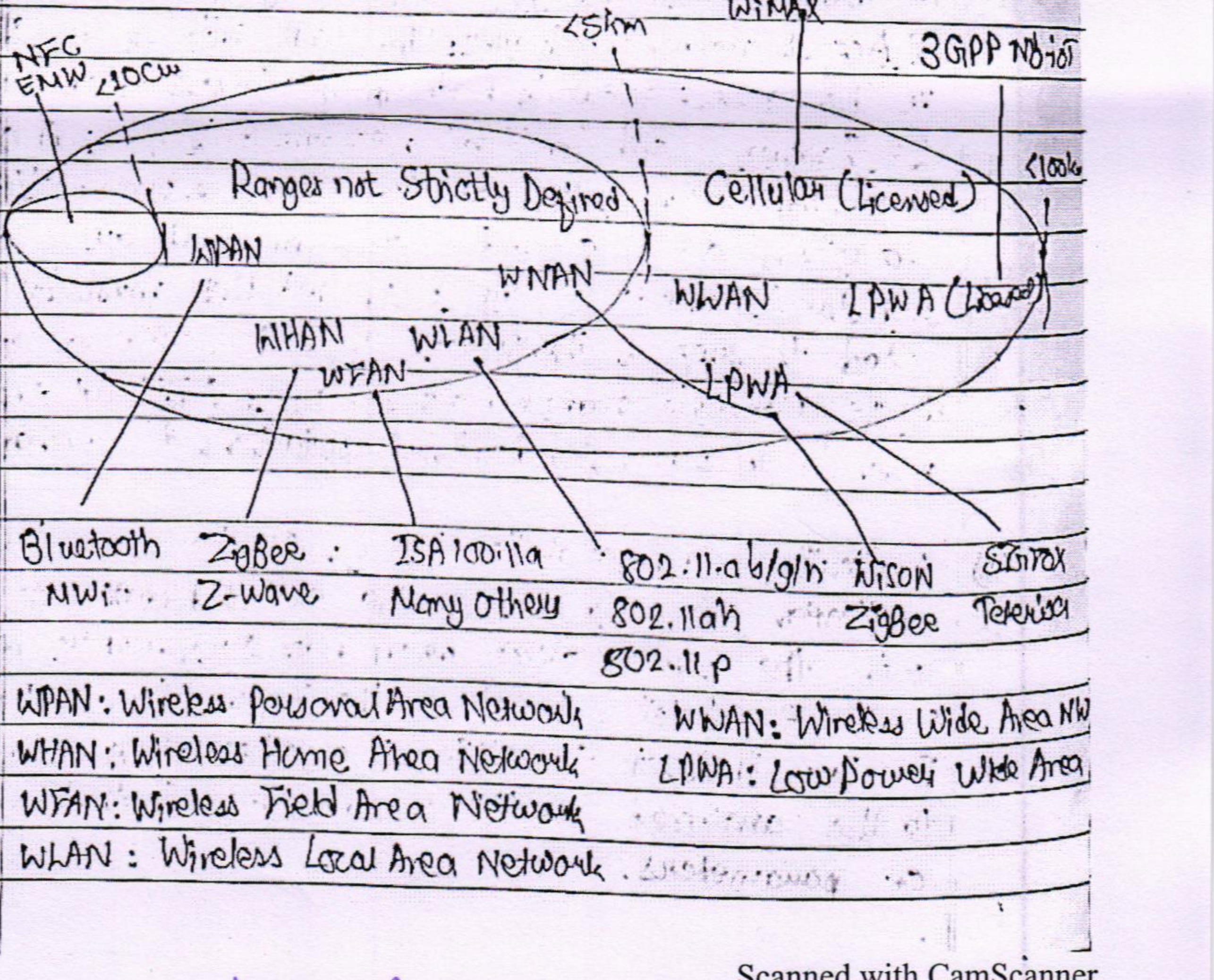
Date : / /
Page No.

7. Explain Access Network sublayer with a neat diagram.

→ Access Network sublayer is explained below with a neat diagram:

Each technology was designed with a certain number of use cases in mind. These use cases determined the frequency band that was expected to be most suitable.

Figure lists some access technologies we may encounter in the IoT world and the expected.



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field Area Network
WLAN: Wireless Local Area Network
WWAN: Wireless Wide Area NW
LPWA: Low Power Wide Area

Scanned with CamScanner

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

- PAN (Personal Area Network)
Scale of a few meters. A common wireless technology is Bluetooth. It is the personal space around a person.

- HAN (Home Area Network)
Scale of a few tens of meters. At this scale, common wireless technologies for IoT include ZigBee.

- NAN (Neighborhood Area Network)
Scale of a hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.

- FAN (Field Area Network)
Scale of a several tens of meters to several hundred meters. The FAN is often seen as open space (and therefore not secured and not controlled.

- LAN (Local Area Network)
Scale of up to 100m. This term is very similar and common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies are used.

Similar ranges do not mean similar topologies. Some topologies offer flexible connectivity structure to extend communication possibilities.
- Point to point topologies
- Point to multipoint
These topologies of LAN provide flexibility in communication.

PRINCIPAL
SIET., TUMAKURU.

8. Explain the functionality of IOT network management sub layer.

→ IP, TCP, and UDP bring connectively 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, whereas others rely on a pull model, and multiple hybrid approaches are also possible.

Following the IP logic, some IOT implementations have suggested HTTP for the data transfer phase. After all, HTTP has a client and server components. The sensor could use the client part to establish a connection to the IOT central application (the server), and then data can be exchanged. We can find HTTP in some IOT applications, but HTTP is something of a fat protocol and was not designed to operate in a constrained environment with low memory, low power, low bandwidth, and a high rate of packet failure.

Despite these limitations, other web-based 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. It is often combined with MQTT to handle the IOT-specific part of the communication.

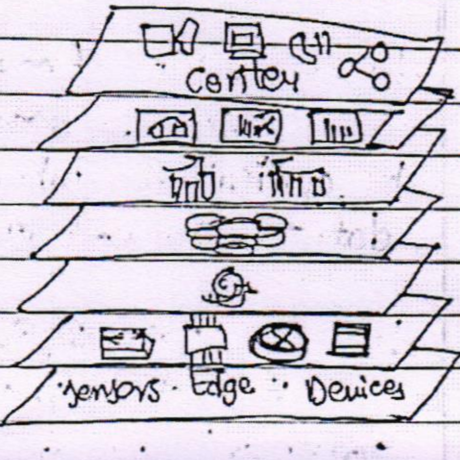
PRINCIPAL
SIET., TUMAKURU.

9. Describe IOT World Forum (IOTWF) Standardized architecture.

> The IOT World Forum (IOTWF) Standardized Architecture is given below:

- The model put forth by the IOT World Forum offers a clean, simplified perspective on IoT and includes edge computing, data storage, and access.

7. Collaboration & Processes
6. Application
5. Data Abstraction
4. Data Accumulation
3. Edge Computing
2. Connectivity
1. Physical Devices & Controllers
(The "Things in IOT)



Layer 1: Physical Devices and Controllers Layer

The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is home to the "things" in the IoT.

Layer 2: Connectivity Layer

In second layer of the IoT Reference Model, the focus is on connectivity. The most important function of the IoT layer is the reliable and timely transmission of data.

Layer 3: Edge Computing Layer

It is often referred as "fog" layer and is discussed in the section. At this layer, emphasis is given on data reduction and converting network data flows

Date: / /
Page No.

into information that is ready for storage and processing by higher layers.

Upper Layers: Layers 4-7

The upper layers deals with handling and processing the IoT data generated by the bottom layer.

Layer 4: Data Accumulation Layer
Captures data and stores it so it is usable by applications when necessary. Converts event based data to query-based processing.

Layer 5: Data Abstraction Layer
Reconciles multiple data forms and ensures consistent semantics from various sources.
Confirms that the data set is complete and consolidates data into one place or multiple data stores using virtualization.

Layer 6: Applications Layer
Interprets data using software applications. Applications may monitor, control and provide reports based on the analysis of the data.

Layer 7: Collaboration and processes Layer
Consumes and shares the application information. Collaborating on and communicating IoT information often requires multiple steps, and it is what makes IoT useful.

PRINCIPAL
SIET., TUMAKURU.

10. Compare and contrast IT and IOT.

→ Until recently, Information Technology and Operational Technology, IT and OT have for the most part lived in separate worlds.

IT supports connections to the Internet along with related data and technology systems. OT monitors and controls devices and processes on physical operational systems.

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keeps the business operating 24x7.	Manages the computers, data and employee communication system
Types of data	Monitoring, control, and supervisory data	Voice; video, transactional and bulk data.
Security	Controlled by physical access to devices.	Devices and users authentication to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible.
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols.	High: continual patching of hosts is required, and the network is connected to Internet and requires protection.

ACY-2020-21

1SV17CS004.

Date: / /

Page No.

Module - 2
Assignment

1. List and explain different types of sensors.

→ A list of different types of sensors along with their explanation is given below:

i) Active or passive: Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically no external power supply (passive).

ii) Invasive or non-invasive: Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).

iii) Contact or no-contact: Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no contact).

iv) Absolute or relative: Sensors can be categorized based on whether they measure on absolute scale (absolute) or based on a different with a fixed or variable reference value (relative).

v) Area of application: Sensors can be categorized based on the specific industry or vertical where they are used.

vi) How sensors measure: Sensors are categorized on the basis of physical mechanism used to measure output.

vii) What sensors measure: They can be categorized on the basis of what physical variables they measure.

Scanned with CamScanner

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

2. Explain "IOT Access Technologies."

→ 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. Following requirement needs to be considered while choosing technology:

- 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:

1. Standardization and alliances: The standards bodies that maintain the protocols for a technology.
2. Physical Layer: The wired or wireless methods and relevant frequencies.
3. MAC Layer: Media Access Control (MAC) layer, which bridges the physical layer and access control.
4. Topology: Topology that are in LAN. technology.
5. Security: Security aspects of the technology.
6. Competitive technologies: Other technologies that are scalable alternative of the given technology.

PRINCIPAL
SIET., TUMAKURU.

3. Explain small physical objects and small virtual objects.

→ 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 and, embedded computers, etc.)

A virtual object is a digital representation, semantically enriched, of a real world object (human or lifeless, static or mobile, solid or intangible), which is able to acquire, analyse and interpret information about its context, to augment the possentiabilities of the associated services for the benefits of quality.

Virtual objects are evolving to address the challenges the IOT is and will be facing in the near future.

In day to day life, we have a lot of object with internet or wireless connection such as:

- Smartphone
- Tablets
- TV. computer

These objects can be interconnected among them and facilitate our daily life.

PRINCIPAL
SIET., TUMAKURU.

4. With a neat diagram, explain how actuators and sensors interact with physical world. Classify actuators on energy type.

→ Sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements into electric signals or digital representations. On the other hand, actuators receive some type of control signal that triggers a physical effect.

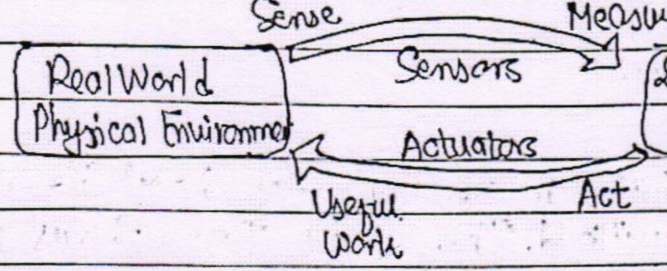


Fig. How Sensors and Actuators interact with the environment

Much like sensors, actuators also vary greatly in function, size, design, and so on. Some common ways of classification:

- Type of motion: Actuators can be classified based on the type of motion they produce.
- Power: 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
- Type of Energy: Based on the type of energy:

Actuators classification based on Energy Type

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyrisor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic	Electromagnet, linear solenoid
Micro & nano actuators	Electrostatic motor, microvalve

Date: / /
Page No.

5. List out limitations of smart objects in WSNs with diagram.

→ Wireless Sensors Networks are made up of smart objects, motes.

→ The following are the limitations of the smart objects in WSNs:

= Limited processing power

- Limited memory

- Lossy communication

- Limited transmission speeds

- Limited power

These limitations greatly influence how WSN's are designed deployed, and utilized. The below figure shows an example of data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.

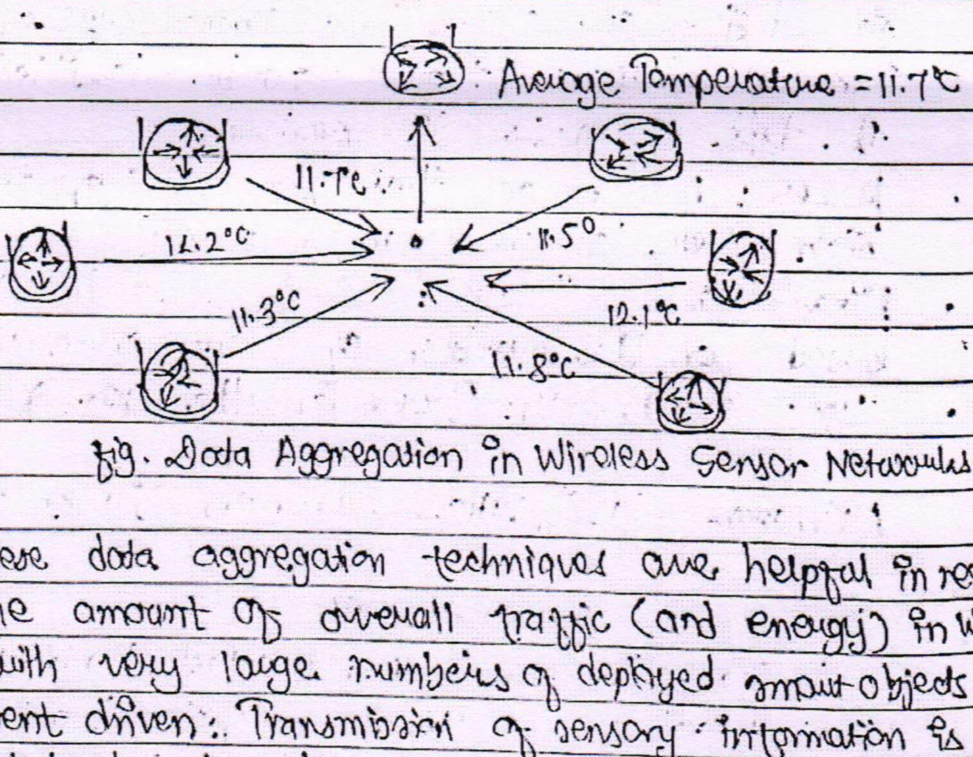


fig. Data Aggregation in Wireless Sensor Networks

These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSN's with very large numbers of deployed smart objects.

Event driven: Transmission of sensory information is triggered only when a smart object detects a threshold.

Periodic: Transmission of sensory information occurs only at periodic intervals.

PRINCIPAL
SIET., TUMAKURU.

6. Explain LoRaWAN standard allionce MAC layer and security.

→ LORaWAN MAC Layer: There are three classes of LORAWAN devices. Class A is the default implementation. Class B was designated "experimental" in LORaWAN until it can be better defined. Class C is particularly adopted for powered nodes.

1 Byte	Variable	4 Bytes
MAC Header(HDR)	MAC Payload	Message Integrity

fig. High-level LORaWAN MAC Frame Format

LoRAWAN endpoints are uniquely addressable through a variety of methods.

Security

LoRaWAN endpoints must implement two layers of security protecting communications and data privacy across the network.

Security in a LORaWAN deployment applies to different components of the architecture.

The first layer, called "network security" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server.

LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated.

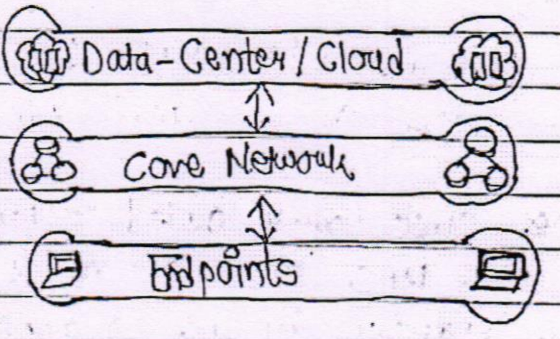
7. Explin the limitations of data management and compule stack.

→ The data management and compute stack model has some limitations. As the volume of data, the variety of objects connecting to the network, and the need for more efficiency increase, new representations appear. These are the following requirements:

(i) Minimizing latency: Since milliseconds matter for many types of industrial systems, and when we are trying to prevent manufacturing line shutdowns or restore electrical servic

ii) Conserving network Bandwidth: The offshore oil rigs generate 500GB of data weekly and commercial jets generate more than 10TB of data every 30 minutes. So, it is not necessary to tansfer all these data and many do not require cloud scale processing.

iii) Increasing local efficiency: It may not be useful for collecting and securing data across a wide geographic area. Analyzing both areas in the same system of cloud may not be necessary.



There are several data related problems that needs to be addressed: Bandwidth, Latency, The volume of data and Big Data which is getting bigger should be solved.

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

8. Define smart objects. Explain its characteristics.

→ Smart objects are the building blocks of IOT. They are what transform everyday objects into a network of Intelligent objects. These intelligent objects are able to learn from and interact with their environment.

The characteristics of smart objects are as follows:

(i) Processing unit: Smart objects contain processing unit for acquiring data, processing and analysing sensing information received by the sensors, coordinating control signals to any actuators, and controlling a variety of functions on the smart object, like communication.

(ii) Communication Device: The communication unit is responsible for connecting a smart object with other smart objects and the outside would (via the network). Communication devices for smart objects can be either wired or wireless.

(iii) Sensors and actuators: Smart objects are capable of interacting with the physical world through sensors and actuators. A smart object doesn't need to contain both sensors and actuators. Smart objects can contain multiple sensors and actuators.

(iv) Power source: The components of smart objects require power. The communication unit of a smart object uses the high volume of power. So, there is need of a power source since the objects component consume power.

PRINCIPAL
SIET., TUMAKURU.

Module-3

Assignment

1. Explain working of IP as the IOT network layer.

→ The working of IP as the IOT Network Layer is given below:

(i) The Business Case for IP: This section discusses the advantages of IP from an IOT perspective and introduces the concepts of adoption and adaptation.

(ii) The Need for Optimization: There are several challenges of constrained nodes and devices when deploying IP. This section looks at the need of migration from IPv4 to IPV6 and how it affects IOT networks.

(iii) Optimizing IP for IOT: There are some common protocols and technologies in IOT networks utilizing IP, including 6LoWPAN, 6TiSCH, and RPL.

(iv) Profiles and Compliances: It provides a summary of some of the most significant organizations and standards bodies involved with IP connectivity and IOT

The key advantages of Internet Protocol

- One of the main differences between traditional information technology (IT) and operational technology (OT) is the lifetime of the underlying technologies and products.

- IP is able to maintain its operations for large numbers of devices and users.

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

2. Write note on Business case for IP.

→ Business Case for IP:

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

Dedicated applications are then run over virtualized or traditional operating systems or on network edge platforms (for example, fog computing).

Lightweight applications communicate with the data center servers.

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.

3. Explain need for Optimization.

→ Optimizations are needed at various layers of the IP stack to handle the restrictions that are present in IOT networks.

Constrained Nodes:

In IOT solutions, different classes of devices coexist. Depending on its functions in a network, a "thing" architecture may or may not offer similar character-

PRINCIPAL
SIET., TUMAKURU.

istics compared to a generic PC or server in an IT environment.

Another limit is that this network protocol stack on an IoT node may be required to communicate through an unreliable path.

Even if a full IP stack is available on this node, this causes problems such as limited or unpredictable throughput and low convergence when a topology change occurs.

Finally, power consumption is a key characteristic of constrained nodes.

4. Describe application protocols for IoT.

→ With the TCP/IP protocols, two main protocols are specified for the transport layer.

i) Transmission Control Protocol (TCP):
This connection oriented protocol requires a session to get established between the source and destination before exchanging data.

ii) User Datagram Protocol (UDP)
With this connectionless protocol data can be quickly sent between source and destination but with no guarantee of delivery.
This is analogous to the traditional mail system in which a letter is mailed to a destination.

Date: / /
Page No.

- TCP is the main protocol used at the transport layer. This is largely due to its inherent characteristics, such as its ability to transport large volumes of data into smaller sets of packets.

- In addition, it ensures reassembly in a correct sequence, flow control and wind adjustment, and retransmission of lost packets.

- In contrast, UDP is most often used in the content of network services, such as Domain Name System (DNS), Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), and Dynamic Host Control Protocol (DHCP), or for real-time data traffic, including voice and video over IP.

- In these cases, performance and latency are more important than packet retransmission because re-sending a lost voice or video packet does not add value.

5. Discuss the various methods used in IOT application transport.

→ There are various means of transporting. Some of them are as follows:

i) Application layer protocol not present.
ii) Supervisory control and data acquisition (SCADA)
iii) Generic web-based protocols
iv) IoT application layer protocols

These are the categories of IoT application protocol

PRINCIPAL
SIET., TUMAKURU.

① Application layer protocol Not Present

In class 0 send or receive only a few bytes of data.

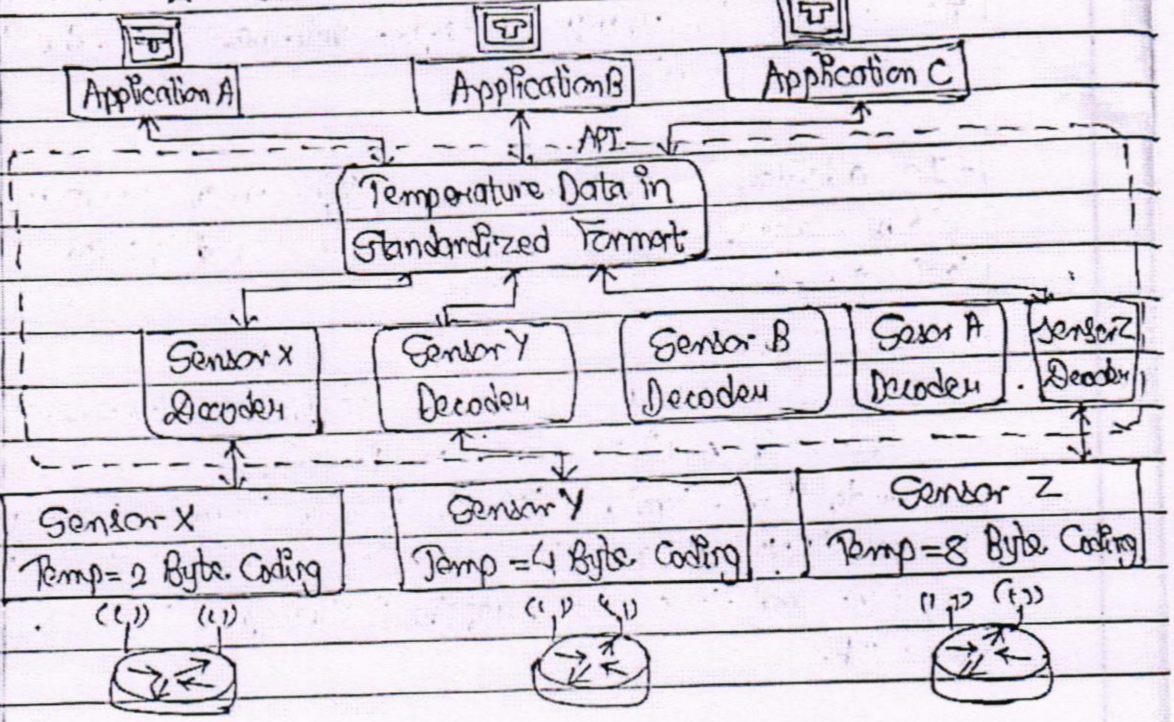


fig. IoT Data Broker

- An IoT Data Broker is a piece of middleware that standardizes sensor output into a common format that can then be retrieved by authorized applications.

- In figure sensors X, Y and Z are all temperature sensors but their output is encoded differently.

- Applications A, B and C in figure can access this temperature data without having to deal with decoding multiple temperature data formats.

ii) Supervisory Control and Data Acquisition (SCADA)

Defined decades ago, SCADA is an automation control

PRINCIPAL
SIET., TUMAKURU.

Date : / /
Page No.

system that was initially implemented without IP over serial links (such as RS-232 and RS-485, before being used to Ethernet and IPv4.

- SCADA networking protocols, running directly over serial physical and data link layers.

- At high level, SCADA systems allow collect data from sensor and telemetry remote devices, and to control them.

- SCADA systems allow global, real-time, data-driven decisions to be made about how to improve business processes.

iii) Generic Web-Based Protocols

- The level of familiarity with generic web-based protocols is high. Therefore, programmers with basic web programming skills can work on IOT applications, and this may lead to innovative ways to deliver and handle real-time IOT data.

- On non-constrained networks, such as Ethernet, Wi-Fi, or 3G/4G cellular, where bandwidth is not perceived as a potential issue, data payloads based on a verbose data model representation.

iv) Constrained Application Protocol (CoAP)

- CoAP is to develop a generic framework for resource-oriented applications targeting constrained nodes and networks.

PRINCIPAL
SIET., TUMAKURU.

Scanned with CamScanner

6. Explain in detail the 6LOWPAN.

→ In the IP architecture, the transport of IP packets over any given Layer 1 (PHY) and Layer 2 (MAC) protocol must be defined.

The initial focus of the 6LoWPAN working group was to optimize the transmission of IPv6 packets over constrained networks such as IEEE 802.15.4.

IoT Protocol Stack with
6LoWPAN Adaptation Layer

Application Protocols	
UDP	ICMP
IPv6	
LoWPAN	
IEEE 802.15.4 MAC	
IEEE 802.15.4 PHY	

- The 6LoWPAN working group published severeral RFC's but RFC 4994 is foundational because it defined frame headers compression, fragmentation and mesh addressing.

Header Compression:

- IPv6 headers compression for 6LOWPAN was defined initially in RFC 4944 & subsequently updated by RFC 6282.

- 6LOWPAN header compression is stateless & conceptually it is not too complicated.

Fragmentation Header:

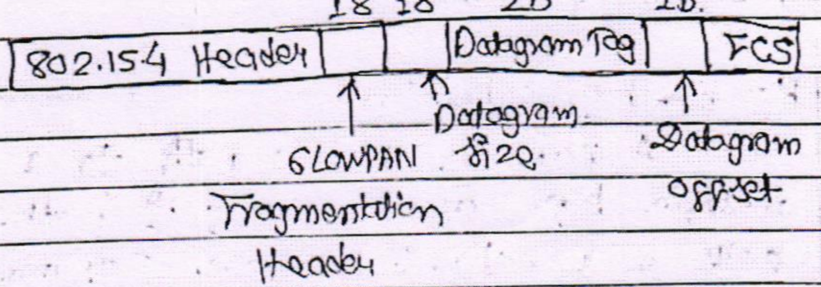


fig. 6LOWPAN Fragmentation Header

- 6LOWPAN fragmentation header field itself uses a unique bit value to identify that the subsequent fields as opposed to another capability.

7. Explain the different schedule management and packet forwarding models of 6TiSCH.

→ The 6TiSCH architecture defines four schedule management mechanisms:

- Static scheduling:
It is a simple scheduling mechanism that can be used upon initial implementation or as a fallback in the case of network malfunction.

- Neighbour-to-neighbor scheduling:
A schedule is established that correlates with the observed number of transmissions between nodes. Cells in this schedule can be added or deleted as traffic requirements & bandwidth needs change.

- Remote monitoring and scheduling management:
Time slots and other resource allocation

are handled by a management entity that can be multiple hops away.

- Hop-by-hop scheduling:
A node reserves a path to a destination node multiple hops away by requesting the allocation of cells in a schedule at each intermediate node hop in the path.

There are three 6TiSCH forwarding models:

i) Track Forwarding (TF):
- This is the simplest & fastest forwarding model. TF a "track" in this model is a unidirectional path between a source and a destination.

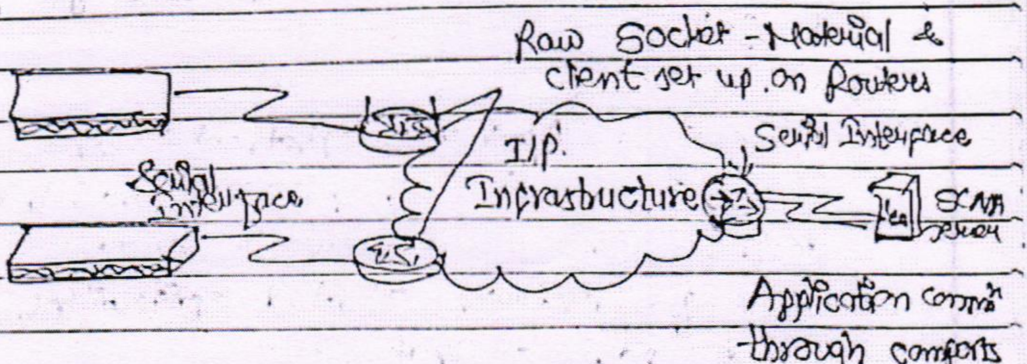
ii) Fragment Forwarding (FF):
- This model takes advantage of 6LoWPAN fragmentation to build a layer 2 forwarding table.

iii) IPv6 Forwarding (6F):
- This model forwards traffic based on its IPV6 routing table.

8. Explain the raw socket tunneling of SCADA using different scenarios.

→ Tunneling legacy SCADA over IP networks:-

- A raw socket connection simply denotes that the serial data is being packaged directly into a TCP or UDP transport.


Raw Socket - Material & client set up on Routers
Serial Interface
I/P Infrastructure
RTUs
Serial Interface
SCADA server
Application comm through comports

Scenario A: Raw socket between routers - no chage on SCADA server.

In scenario A, both the SCADA servers of RTUs have a direct serial connection to their respective routers.

The routers terminate the serial communication at both ends of the link & use raw socket encapsulation to transport the serial payload over I/P network.

In scenario B, there is small change on the SCADA server side. A piece of software is installed on the SCADA server that manages the serial COM ports to IP ports.

In case of scenario C, the servers support native reaw socket capability.

Unlike in Scenario A & B, where a router or IP/ serial redirector software has to map the SCADA server's serial ports to IP ports.

9. What is COAP? Draw COAP message format. Explain its fields.

→ Constrained Application Protocol (COAP) resulted from the IETF constrained RESTFUL Environments (CORE) working group's efforts to develop a generic framework for resource-oriented applications targeting constrained nodes of networks.

← 4 Bytes →

<table>
<tr><td>Ver</td><td>T</td><td>TKL</td><td>Code</td><td>Message ID</td></tr>
<tr><td colspan="5">Token (optional, Length, Assigned TKL)</td></tr>
<tr><td colspan="5">Options (optional)</td></tr>
<tr><td colspan="3">11111111</td><td colspan="2">Payload (optional)</td></tr>
</table>

fig. COAP Message format

- The COAP message format is relatively simpler and flexible.

COAP Message Fields:

i) Ver (Version) → Identifies the COAP version.

ii) T (Type) → Defines one of the following message types:
- Confirmable (CON),
- Non-confirmable (NON),
- Acknowledgement (ACK),
- or Reset (RST)

iii) TKL (Token length) - Specifies the size (0-8) bytes of the Token field.

iv). Code → Indicates the request method for a request message & a responds code for a response message.

v) Message ID → Detects message duplication & used to match ACK & RST message types to Con & Non message types.

vi) Token → With a length specified by TKL, correlatives requests & responses.

10. Compare between COAP and MQTT.

→

Factors	COAP	MQTT
- Main Transport protocol	- UDP	- TCP
- Typical messaging	- Request/ response	- Publish/ subscribe
- Security	- DTLS	- SSL/TLS.
- Communication Mode	- One-to-one	- Many-to many
Weakness	- Not as reliable as TCP-based MQTT, so the application must ensure reliability.	- Higher overload for constrained devices and network.

PRINCIPAL
SIET., TUMAKURU.

Date: / /
Page No.

12. List and explain the key advantages of internet protocol.

→ The key advantages of Internet Protocol are as follows:

① Open & Standard based.

- The IOT creates a new paradigm in which devices, applications, and users can leverage a large set of devices & functionalities.

(ii) Versatile

- A large spectrum of access technologies is available to offer connectivity of "things" in the last mile.

(iii) Ubiquitous:

- All recent operating systems releases, from general purpose computers and servers to lightweight embedded systems have an integrated dual stack,

(iv) Scalable;

- As the internet common protocol of the internet IP has been massively deployed & tested for robust scalability.

PRINCIPAL
SIET., TUMAKURU.

ACY-2020-21

1SV17CS004

Date: / /

Page No.

Module-4 & 5 Assignment

1. Explain in details the core functions of edge analytics with necessary diagram.

→ The core functions of edge analytics are as follows:

(i) Raw input data:
This is the raw data coming from the sensors into the analytics processing unit.

(ii) Analytics Processing Unit (APU):
The APU filters and combines data streams organizes them by time windows, & perform various analytical functions.

(iii) Output Streams:
The data that is output is organized into insightful streams and is used to influence the behaviour of smart objects, and passed on for storage and further processing in the cloud.

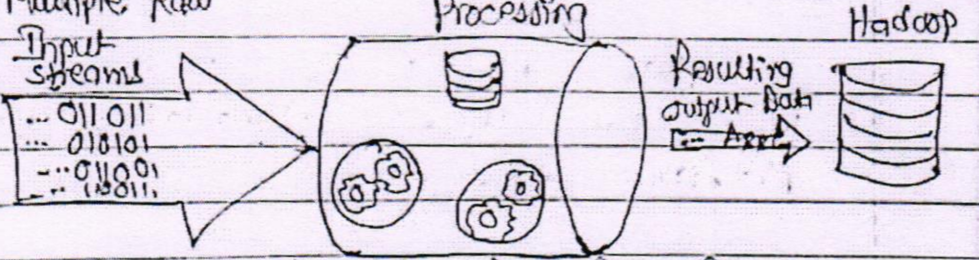


fig. Edge Analytics Processing Unit

(A) Filter :
The streaming data generates by IOT endpoint is likely to be very large, and most of its irrelevant.

Date: / /
Page No.

(v) Transform:

In the data warehousing world, extract, transform & Load (ETL) operations are used to manipulate the data structure into a form that can be used for other purposes.

(vi) Time:

- As the real-time streaming data flows, a timing content needs to be established.

2> Explain the different components of Flexible Net Flow Architecture (FNF).

-> FNF Flow Monitor (Net Flow Cache): The FNF flow monitor container 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 flows as attributes or characteristics of a flow) within the cache,

FNF Flow record:

- A flow record is a set of key & non-key Netflow field values used to characterize flows in the NetFlow cache.

- Flow records may be predefined for each of use or customized & user defined.

FNF exporter:

- There are two primary methods for accessing NetFlow data: Using the show commands at the

Scanned with CamScanner

PRINCIPAL
SIET., TUMAKURU.

command line interface (CLI), and using an application reporting tool.

Flow export timers:
Timers indicates how often flows should be exported to the collection & reporting server.

NetFlow export Format:
This simply indicates the type of flow reporting format.

3> Explain Secured Network Infrastructure by using process control hierarchy model.

→ As a first step we need to analyze and secure the basic network logic.

Most automated process systems or even hierarchical energy distribution systems have a high degree of correlation between the network design and the operational design.

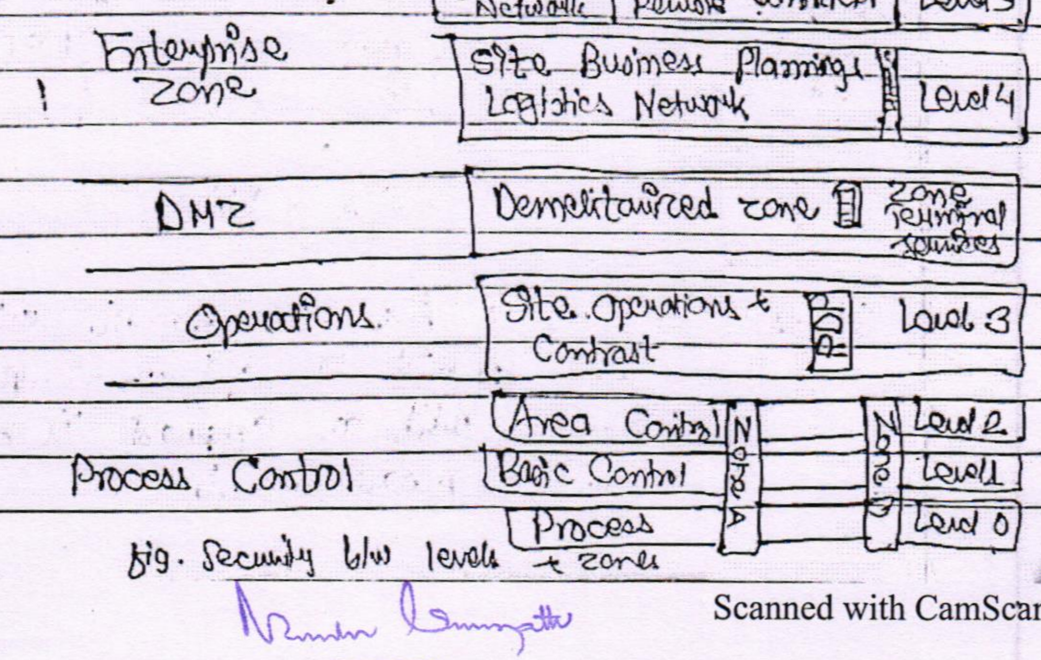


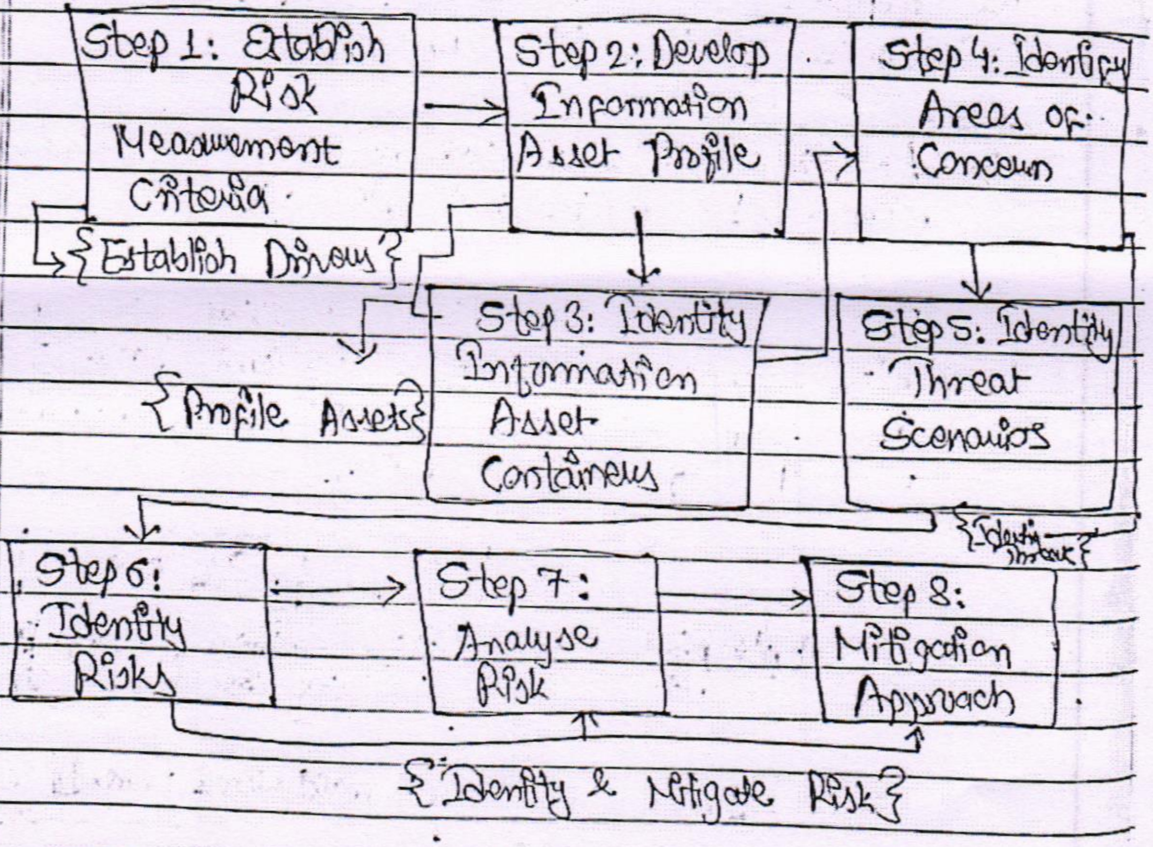
fig. Security b/w levels + zones

- Normal n/w discovery processes can be highly problematic for adder networking equipment.

- In fact, the discovery process in persuit of improved safety, security, and operational state can be result in degradation of all three.

4) Explain the different steps and phases of OCTAVE Allegro methodology.

→ The steps and phases of OCTAVE allegro :


Step 1: Establish Risk Measurement Criteria
{Establish Drivers}
Step 2: Develop Information Asset Profile
Step 4: Identify Areas of Concern
Step 3: Identity Information Asset Containers
{Profile Assets}
Step 5: Identify Threat Scenarios
{Identify threat}
Step 6: Identify Risks
Step 7: Analyse Risk
Step 8: Mitigation Approach
{Identify & Mitigate Risk}

Step 1: Establish a risk management criterion:
- OCTAVE provides a fairly simple means of doing the with an emphasis is on impact, value & measurement.

PRINCIPAL
SIET., TUMAKURU.

Step 2 :- To develop an information asset profile.
- This profile is populated with assets, a prioritization of assets, attributes association with each other asset.

Step 3:- To identify information asset containers.
- This is the range of transports and possible locations where the information weight reside.

Step 4 :- To identify area of concern.
- We depart from a data flow, touch, and attribute focus to one where judgements are made through a mapping of security related attributed to more business-focused use cases.

Step 5 :- Where threat scenarios are identified.
- Threats are broadly (i.e properly) identified as potential undesirable events.

Step 6 :- Risks are identified
- Within OCTAVE, risk is possibility of an undesired outcome.

Step 7 :- Risk Analysis
- With the effort placed on qualitative evaluation of the impacts of the risk.

Step 8 :- Finally, mitigation is applied at the eighth step.

Date : / /
Page No.

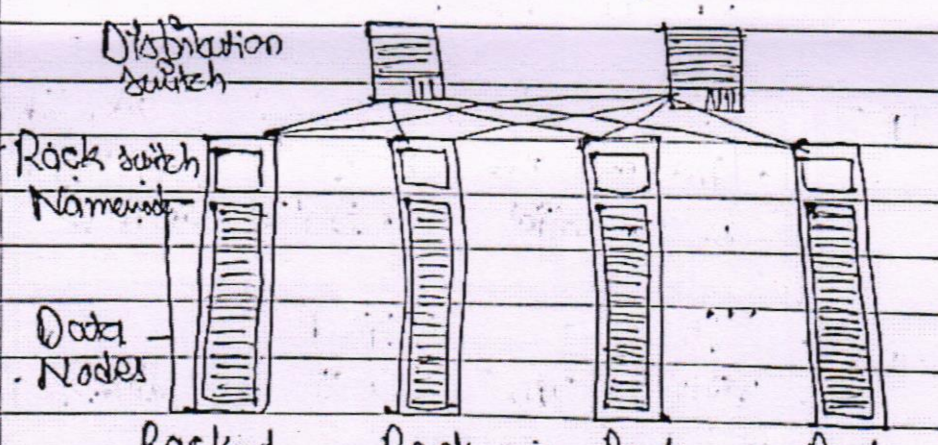
5) Explain the elements of Hadoop with a neat diagram.

→ Hadoop is the most recent entrant into the data management market, but it is arguably the most popular choice as a data repository & processing engine.

The two main key elements:

(i) Hadoop Distributed File System (HDFS):- A system for storing data across multiple nodes.

(ii) MapReduce :
A distributed processing engine that splits a large task into smaller ones that can be run in parallel.



Namenode:
These are a critical piece of data adds, moves deletes. and reads on HDFS.

DataNodes:
These are the servers where the data is stored at the direction of the NameNode.

Scanned with CamScanner

PRINCIPAL
SIET., TUMAKURU.

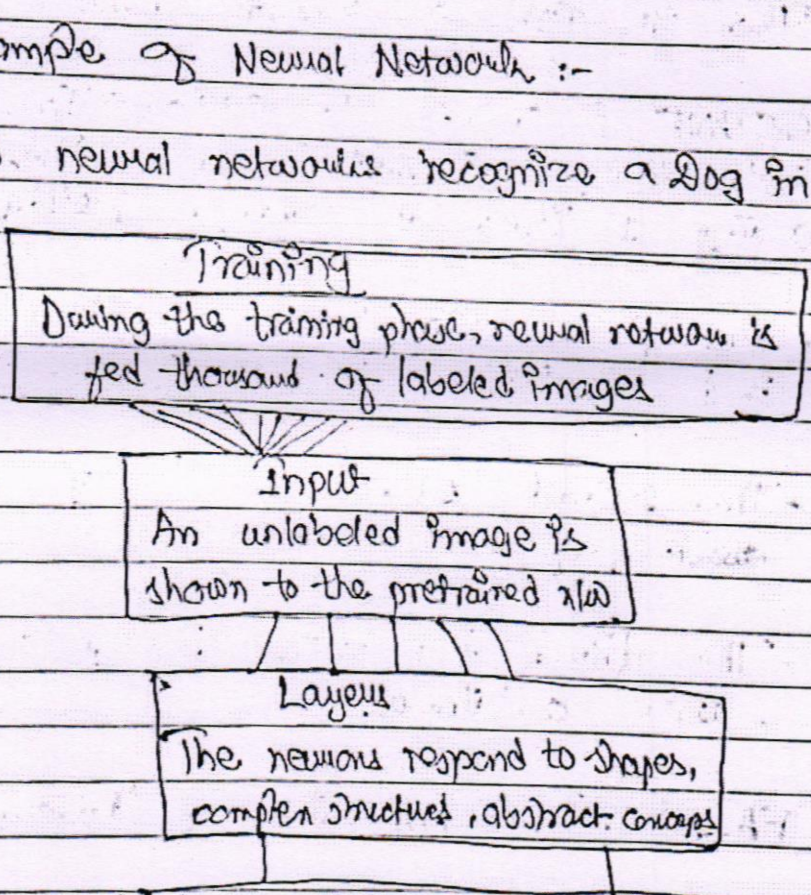
6) Explain neural network in machine learning with a detailed example.

→ Neural Network 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, & also so on. Neural network mimic the same logic.

Example of Neural Network :-

. How neural networks recognize a Dog in a photoo



Training
During the training phase, neural network is fed thousand of labeled images

Input
An unlabeled image is shown to the pretrained n/w

Layers
The neurons respond to shapes, complex structures, abstract concepts

Output
The n/w predicts what the object most likely is based on its training.

fig. Neural Network Example.

7. Explain the formal risk analytics structures.

> Within the industrial environment, there are a number of standards, guidelines and best practices available to help understand risk and how to mitigate it.

The key for any industrial environment is that it needs to address security holistically and not just focus on technology.

The two risk assessment frameworks:

(i) OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) from the Software Engineering Institute at Caunegie Mellon University.

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

- The second step is to develop an information asset profile.

- The third step is to develop an information asset containers.

(ii) FAIR(Factor Analysis of Information Risk)

- FAIR is a technical standard for risk definition from the Open Group.

- FAIR has clear applications within operational technology.

Date : / /
Page No.

8. What do you mean by data and analytics for IoT ? Explain.

→ In the world of IoT, the creation of massive aments of data from sensors is common & one of the biggest challenges not only from a transport perspective but also from a data managemaint standpont.

A great example of the deluge of data can be generated by IoT is found in the commercial aviation industry & the sensors that are deployed throughout an aircraft.

- Modern jet engines are filled with thousands of sensors that generate a unhopping of sensors that generate over 500TB. of data daily, & this is just the data from the engines.

- A twin engine commercial aircraft with these engines operating on average. shows a day will generate over 500TB. of data.

9. Discuss. Bigdata analytics. tools and technology.

→ The industry looks to the "three Vs" to categorize big data :

* Velocity:
- Velocity refers to how quickly data is being calculated & analyzed.

PRINCIPAL
SIET., TUMAKURU.

- HDFS is designed to ingest and process data very quickly.

* Variety :
Variety refers to different types of data. Data categorized as structured, semi-structured or unstructured.

* Volume:
Volume refers to the scale of the data. Generally big data implementations scale beyond what is available on locally attached storage disks on a single node.

The characteristics of big data are: :

- First is machine data, which is generated by IoT devices by IoT devices & typically unstructured data.

- Second is transactional data, which is from sources that produce data from transactions on these system, and have high volume of structured.

10) With a case study relocate the concept of securing IoT.

→ Case Study:
The enterprise found itself attack by an organized Far East adversary who exploited firmware vulnerabilities in these camera systems and rapidly compromised nearly every camera on the network.

Date: / /
Page No.

The responsibilities for maintaning the digital security or surveillance systems typically consider the probability the use of unclassified n/w. communications, Issuing devices re-configured to threat cyber threats or implementing an add-on solution.

Solution:

- The enterprise can mitigate the threats to its video infrastructure by implementing an agile, simple and highly secure solution.

- This multiple - award - winning device has been widely recognized as the most portable & easiest to configure hardware VPN solution.

11) Explain in detail how IT and IOT security practices and systems vary in real time.

> The differences between an enterprise IT environment and an individual focused IOT deployment are important to underst and because they have a direct Impact on the security practice applied to them.

The information is typically used to make business decisions, such as these in process optimization, whereas OT performance is characteristically leveraged to make physical decisions, such as closing a value, increasing pressure & so on.

As the borders between traditionally separate OT and IT domains blur, they must align strategies and work 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 from their IT counterparts.

IOT Module-5 1SV17CS004
Assignment

Date / /
Page No.

1) Explain the different pins / pouts of Arduino Uno Board.

→ Different pins/ pouts of Arduino Uno Board are:

i) Reset Button : This will restart any code that is loaded to the Arduino Board.

ii) AREF : Stands for "Analog Reference" & is used to set an external reference voltage.

iii) Ground Pin : There are a few ground pins on the Arduino and they all work the same.

iv) Digital Input / output : Pins 0-13 can be used for digital input or output.

v) PWM : The pins marked with the (~) symbol can simulate analog output.

vi) USB Connection : Used for powering up your Arduino and uploading sketches.

vii) Power LED indicator : This LED lights up anytime the board is plugged in a power source.

viii) Voltage Regulator : This controls the amount of voltage going into the Arduino Board.

PRINCIPAL
SIET., TUMAKURU.

ix) <u>Ground Pins</u>: There are a few ground pins on the Arduino & they all work the same.

x) <u>Analog Pins</u>: These pins can read the signal from an analog sensor and convert it to digital.

2) Write a program to record the current room temperature using Raspberry pi.

→
```
import os
import glob
import time
os.system ('modprobe w1-gpio')
os. system ('modprobe w1 --therm')
base_dir = '/sys/bus/w1/devices/'
device_folder = glob. glob (base_dir + '28*')[0]
device_file = device_floder + '/w1_slave'
def read-temp_raw():
        f. = open (device_file, 'r')
        lines= f.readlines()
        f.close ()
        return lines

def read_temp():
        lines= read-temp_ raw()
        while lines[0]. strip () [-3:] != 'YES';
        time.sleep (0.2)
        lines= read_temp_raw ()
        equals_pos= lines[1]. find ('t=')
        if  equals_pos! = -1!
                temp_string = lines [1] [equals_pos+2: ]
```

PRINCIPAL
SIET., TUMAKURU.

```
        temp_c = float (temp_string) / 1000.0
        temp_f = temp_c * 9.0 / 5.0 + 32.0
        return temp_c, temp_f
while True :
    print (read_temp())
    time.sleep (1)
```

3) Explain the different layers of IoT Smart City layered architecture.

→ The smart city IoT infrastructure is a four-layered architecture:

(i) Street Layer:

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

A sensor is a data source that generates data receivers to understand the physical world. Sensor devices are able to detect and measure events in the physical world.

(ii) City Layer:

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

This layer aggregates all data collected by sensors

Date / /
Page No.

and the end-node network into a single transport network.

(iii) Data Center Layer:
Ultimately, data collected from the sensors is sent to the data center, where it can be processed and correlated.

Based on this processing of data, meaningful information and trends can be derived, and information can be provided back.

For example, an application in a data center can provide a global view of the city traffic and help authorised decide on the need for more or less common transport vehicles.

(iv) Service Layer:

- Ultimately, the true value of IOT connectivity comes from the services that can be measured data provide to different users operating within a city.

- Smart city applications can provide value to and visibility for a variety of users types, including city operations, citizens, and law enforcement.

-The collected data should be visualized according to the specific needs of each consumers of that data.

PRINCIPAL
SIET., TUMAKURU.

4) Explain Smart- parking architecture with advantages and disadvantages

> A variety of parking sensors are available on the market, and they take different approaches to sensing occupancy for parking spots.

- Example include in-ground magnetic sensors, which use embedded sensors to create a magnetic detection field in a parking spot.

- Most sensors installed in the ground must rely on battery power, since running a power line is typically too expensive.

- In high-density, environments (for example, indoor parking, parking decks), one or several gateways per floor may connect to the parking sensors, using shorter-range protocols such as ZigBee or Wi-Fi.

5) Explain the following with respect to Arduino programming.

i) Structure
ii) Functions
iii) Variables
iv) Flow Control statements
v) Data type
vi) Constants

→ (i) Structure: Software structure consists of two main functions:

PRINCIPAL
SIET., TUMAKURU.

i) setup () function.
ii) Loop () function.

```
void setup()
{
  ...
}
void loop()
{
  ...
}
```

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

ii) Functions:

The Arduino has two common functions setup() and loop(), which are called automatically in the background.

void setup(): It includes the initial part of the code, which is executed only once. It is called as the preparation block.

void loop(): It includes the statements, which are executed repeatedly. It is called the execution block.

iii) Vauiables:

Declaring vauiables,

```
int val= 5;
```

Using vauiables,

```
int delayTime = 2000;
int greenLED = 9;
void setup(){
        pincode (greenLED, OUTPUT);
   }
void loop(){
        digitalWrite (greenLED, HIGH);
        delay ( delayTime );
        digitalWrite (greenLED; LOW);
delayTime = delayTime - 100;
        delay(delayTime);
}
```

(iv) Flow Control Statements:

```
- if ("answer is true")
   {
     "perform some action";
   }

- if else
   if ("ans is true")
   {
     "do somethig"
   }
else
   { "do somethig another"
   }
```

v) Data type

Boolean operator - AND

```
if (vau >10 && val <20)
```

Boolean operator - OR

```
if ( val<10 ||val >20)
```

vi) Constant:

```
const float pi = 3.14;
float x;
x = pi* 2;
pi=7;
```

6) Explain Raspberry pi learning method.

→ Raspberry pi is a single computer board with card (credit-card) size, that can be used for many tasks that your computer does, like games, word processing, spreadsheets and also to play HD video.

- The main purpose of designing the raspberry pi board is to encourage learning, experimentation and innovation for school level students.

- Raspberry pi board is a portable and low cost. Maximum of the raspberry pi computer is used in mobile phones.

- Raspberry pi comes in two models, they are

PRINCIPAL
SIET., TUMAKURU.

model A and model B. The main difference between model A and model B is USB port.

- Model A board will consume less power and that does not include an Ethernet port. But model B board includes an Ethernet port and designed in China.

=> Explain Smart city security architecture.

-> . A serious concern of most smart cities & their citizens is data security.

Vast quantities of sensitive information are being shared at all times in a layered, real-time architecture, and cities have a duty to protect their citizens data from unauthorized access, collection and tampering.

A security architecture for smart cities must utilize security protocols to fortify each layer of the architecture and protect city data.

The city layer transports data b/w the street layer and the data center layer. It acts as the network layer.

Firewall: A firewall is located at the edge of it should be IPsec - and VPN-ready, and include user and role based access control.

VLAN : A VLAN provides end-to-end segmentation

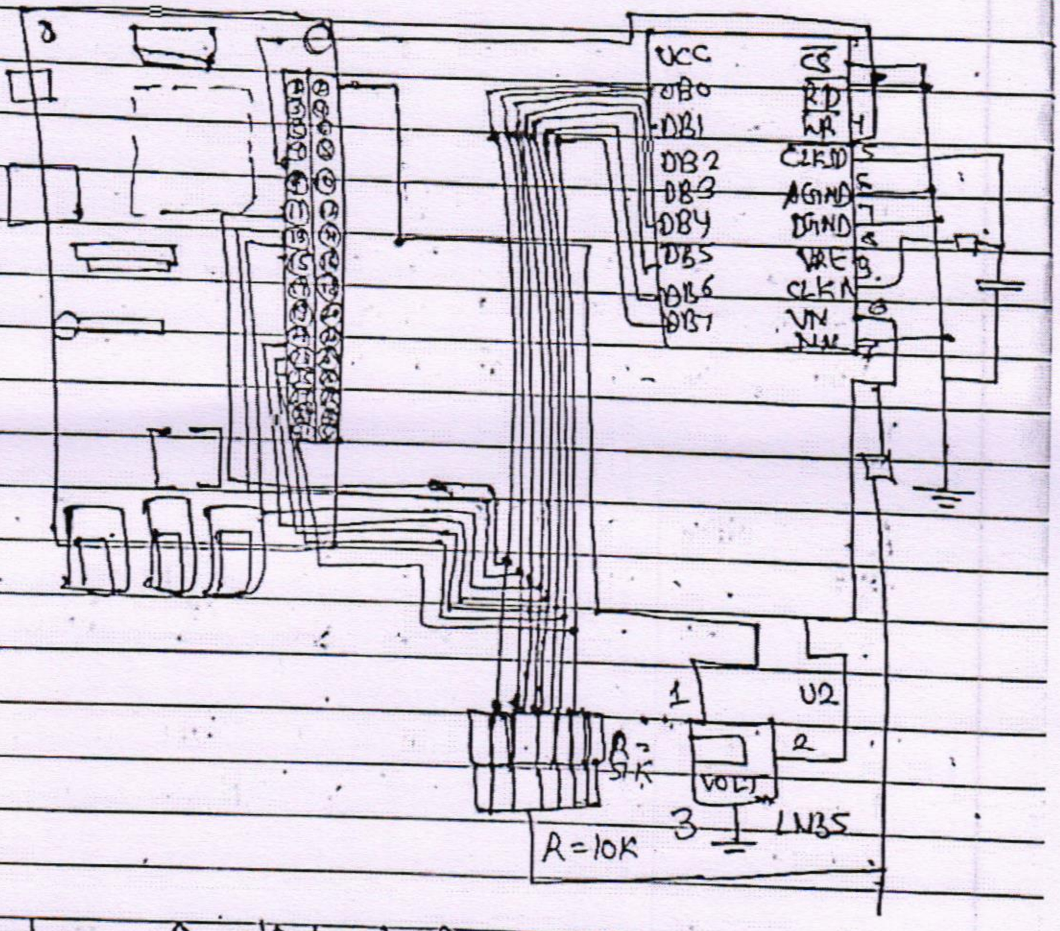
PRINCIPAL
SIET., TUMAKURU.

Of data transmission, further protecting data from rogue intervention.

Encryption : Protecting the traffic from the sensor to the application is a common requirements to avoid data tampering and eavesdropping.

8) With a neat diagram, explain wireless temperature monitoring s/m using Raspberry Pi.

→



Raspberry pi which having in built wi fi, which makes it suitable for IOT applications, so that by using IOT Technology this monitoring system works by uploading the temperature value to the Thingspeak cloud by this project you

PRINCIPAL
SIET., TUMAKURU.

Date / /
Page No.

can learn to have to handle cloud-based applications which is suitable to view the sensor legs in this form of graph plots.

- Here we created one field to monitor the temperature value that can be reconfigurable to monitor a number of sensor values in the various fields.

- This basic will teach us to how to work with acloud by using LM35 as a temperature sensor, to detect the temperature and to upload those values into the cloud.

PRINCIPAL
SIET., TUMAKURU.