# Internet Of Things

FOR DIPLOMA STUDENTS
Lecture Notes Prepared
by

Subrata Parida (Sr. Lect.)

IT Dept.

JHARSUGUDA ENGINEERING SCHOOL, JHARSUGUDA

# Ch-1

Date 2/5/21
Page

* What is internet of things ?

-> The Internet of things refers to a system of interrelated, internet connected objects that are able to collect and transfer data over a wireless network without human intervention.

* Characteristics of IOT :-

1. Intelligence :- Intelligence in IOT is only concerned as means of interaction between devices.
2. Connectivity :- Connectivity empowers internet of things by bringing together everyday objects.
3. Dynamic Nature :-
   The Primary activity of internet of things is to collect data from its environment this is achieved with the dynamic changes that take place around the device.
4. Sensing :- Sensing technologies provide the means to create capabilities that reflect a true awareness of the physical world and the people in it.
5. Heterogeneity :- Ability to interact with other devices / platforms through different networks.
6. Security :- Secures data from external world.

* Application of IOT :-

1. Environment monitoring
2. Healthcare
3. Smartcity
4. Smart Retail
5. Smart Industry
6. Smart Agriculture
7. Energy Management
8. Automative
9. Building & Home Automation

IOT categories :-
There are three type of IOT

(i) Consumer IOT (APPS, Sensors, Home security equipment)
(ii) Enterprise IOT
(iii) Intertial IOT (Robotics, car etc)

* Who are IOT Enablers ?

System installers, repairmen, craftsmen, electricians plumbers, designers and data-gatherers who connect devices and systems to the internet for personal use and for commercial and other business uses.

* Sensors :-

Sensors play an important role in creating solutions using IOT. sensors are devices that detect external information, replying it with a signal that humans and machines can distinguish.

In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action.

Examples of actuators
Comb drive
Digital micromirror device
Electric motor
Electroactive polymer
Hydraulic cylinder
Piezoelectric actuator
Pneumatic actuator
Screw jack

Component of IOT :-
Sensors is different type :-
(i) gateway (internet connecting device)
(ii) cloud server
(iii) IOT lab

Challenges challenges for IOT :-

(i) Security
(ii) IOT devices
(iii) Regulations
(iv) Compatibility
(v) Bandwidth
(vi) Customer expectation

Ch-2

Connectivity Technologies :-

IOT LAN :- Local, short range comm, may or may not connect to internet, building or organization wide.

IOT WAN :- Connection of various network segments, organizationally and geographically wide, connects to internet.

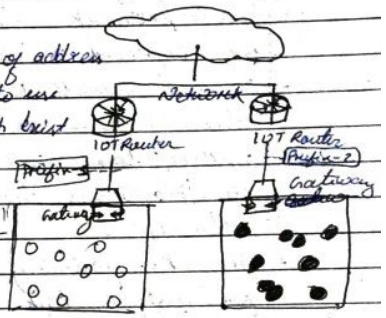
IOT Node :- Connected to other nodes inside a LAN via the IOT LAN, may be sometimes connected to the internet through a WAN directly.

IOT Gateway :- A router connecting the IOT LAN to a WAN to the internet, can implement several LAN and WAN, forwards packets between LAN and WAN on the IP layer.

IOT Proxy :- performs application layer functions between IOT nodes and other entities.

Gateway prefix Allotment :-

- One of the strategies of address conservation in IOT is to use local addresses which exist uniquely within the domain of the gateway. These are represented by the circles in this slide.




- The network connected to the internet has routers with their set of addresses and ranges.
- These routers have multiple gateways connected to them which can forward packets from the nodes, to the internet, only via these routers. These routers assign prefixes to gateways under them so that the gateways can be identified with them.

Impact of mobility on addressing :-

- The network prefix changes from 1 to 2 due to movement, making the IOT LAN safe from changes due to movements.
- IOT gateway WAN address changes without change in LAN address. This is achieved using VLR.

Multi-homing :-

- A node / network connected to multiple networks for improved reliability.
- In case of small IOT LANs, where allotment of address prefixes is not feasible and possible, a proxy based approach is used to manage multiple IP addresses and map them to link local addresses.
- In other, gateway-based approach is used for assigning link local addresses to the nodes under it.
- Providing source addresses, destination address and routing information to the multi-homed nodes is the real challange in multi-homing networks.
- In case the destination and source addresses originate from the same prefix, routing between gateways can be employed for IOT gateway selection.

Ch-3

Connectivity Technology :

~~Bluetooth : IEEE 802.15.4 :~~

(i) IEEE 802.15.4
(ii) zigBEE, 6LOWPAN
(iii) RFID, HART and wireless HART
(iv) NFC, z wave, ISA100.11.A.

(i) IEEE 802.15.4 :-

-> It's low data rate wireless personal area network (PAN).
-> The basic framework conceives a 10 meter communications range with a transfer rate of 250 Kbit/s.
-> It designed for low-cost and low power wireless personal area networks.
-> This is generally an application system such as zigbee, RF4CE, miwi.

(ii) Zigbee :-

-> zighee is an IEEE 802.15.4 based specification for a suite of high level communication protocols used to create personal area networks with small, low power digital radios, such as for home automation, medical device data collection, and others low power, low bandwidth needs, designed for small scale projects

which needs wireless connection.
International standard → IEEE 802.15.4
Developed by → Zigbee Alliance.
use area → Industrial Scientific Medical, IOT
Physical range :- 10 mts to 100 mts.

Applications :-
→ Wireless light switches
→ Electrical meters (Smart grid)
→ Industrial Equipment monitoring

6LOWPAN :-
→ 6LOWPAN is an acronym of IPv6 over low-power wireless Personal Area Network.
→ 6LOWPAN is the name of a concluded working group in the internet area of the IETF.
→ 6LOWPAN Provides the upper layer system for use with low power wireless communications for IOT and M2M, Originally intended for 802.15.4, it is now used with many other wireless standards.
→ The 6LOWPAN system is used for a variety of applications including wireless sensor networks.

RFID :-
→ A Radio frequency identification system is an automatic technology and aids machines or computers to identify objects, record meta-data or control individual target through radio waves. This is the so-called internet of Things.

HART and wireless HART :-
→ Wireless HART is a wireless sensor networking technology based on the highway addressable remote transducer protocol.
→ Developed as a multivendor, interoperable wireless standard, wireless HART was defined for the requirements of process field device network.

NFC :-
→ ~~The Internet of Things is a very popular term.~~
→ Near-field communication is a set of communication protocols for communication between two electronic devices over a distance of 4cm (1½ in) or less.
→ NFC offers a low-speed connection with simple setup that can be used to bootstrap more-capable wireless connections.

## Z Wave :-

→ A Z-Wave network consists of internet of things devices and a primary controller, also known as a smart home hub, which is the only device in a Z-Wave network that is usually connected to the internet.

→ Z wave offers transmission rates of small data packets using throughput rates of 9.6 Kbps, 40 KBPS or 100 Kbps.

## ISA 100.11a :-

→ ISA100.11a is a wireless networking technology standard developed by the international Society of Automation.

→ The official description is wireless system for industrial Automation: Process control and Related Applications.

# ch-4

## Wireless Sensor Networks

* What is wireless sensor networks with example ?

→ Wireless Sensor Network (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor Physical or environmental conditions, such as temperature, Sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location.

* Components of a Sensor networks -:

A sensor node is made up of four basic components such as sensing unit, Processing unit, transceiver unit and a power unit.

* Challenges in WSN -:

Challenges in such WSN include high bandwidth demand, high energy consumption, quality of service (QOS) Provisioning, data Processing and compressing techniques and cross layer design. Physical environment.

Mobile nodes have the ability to sense, compute and communicate like static nodes.

* Sensors Wave :-

Which wave can measure environmental conditions such as temperature, sound, pollution levels, humidity and wind that is known as the sensors wave, which is used in WSN. These are similare to wireless adhoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly.

* Application of WSN ?

1. Trasportation and logistics
2. Industrial applications
3. Precision agriculture & animal tracking.
4. Environmental monitioring
5. Urban terrain tracking & civil structure monitoring.
6. Entertainment
7. Security and surveillance
8. Health care
9. Smart grids & energy control systems
10. Smart buildings

* Wireless Nano-sensor Network ?

→ A wireless Nano sensor network is a collection of Nano sensor nodes that dynamically self organize them in a wireless network without a need but with possible utilization of any pre-existing infrastructure.

Ex: military, Biomedical, Environment, Industry & consumer good, Agriculture, smart office management.

# 5th Chapter

## M2M Communication :-

→ Machine-to-Machine communication or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction.

→ This includes serial connection, powerline connection, or wireless communications in the Industrial Internet of Things (IOT).

## M2M applications and Example :-

- In-car telemetry services.
- Smart meters.
- Smart asset tracking services.
- Supply chain management solutions.
- Wearable technologies.

## How does M2M work in IOT ?-

M2M systems use point-to-point communications between machines, sensors and hardware over cellular or wired networks, while IOT systems rely on IP-based networks to send data collected from IOT-connected devices to gateways, the cloud or middleware platforms.

5.2 M2M Ecosystem :-

M2M refers to the flow of data between physical objects, without the need for human interaction. M2M connectivity has opened a multi-billion dollar revenue opportunity for mobile operators, MVNOs and service aggregators, addressing the application needs of several verticals markets.

Application :

- Multimedia & video
- Remote monitoring, Maintenance & control
- Metering
- Tracking & Tracing
- Security
- Payments
- Others

5.3 M2M Platform :-

→ It is a software solution (unifies and simplifies the management of M2M devices and applications.)

→ * They manage data transmitted by devices.
* The backend systems that process the data.
* The provisioning of software updates to devices.
* General device lifecycle administration.

Ch- 6th

6.1 What is Arduino ?

(i) Arduino is an open source electronics platform based on easy to use hardware and software.

(ii) Arduino boards are able to read inputs:
- light on a sensor
- a finger on a button

and turn it into an output :
- activating a motor.
- turning on an LED.
- Publishing something online.

(iii) By using this we can remotely control the equipment.

(iv) It's a single-board micro controllers

Features of Arduino :

- The operating voltage is 5V the recommended input voltage will range from 7V to 12V.
- The input voltage ranges from 6V to 20V.
- Digital input / output pins are 14 analog i/p pins are 6.
- DC current for each input / output pin is 40 mA.
- DC current for 3.3V pin is 50mA
- Flash memory is 32 KB
- SRAM is 2KB
- EEPROM is 1KB
- CLK Speed is 16 MHz

Components of Arduino :

- Power (USB / Barrel Jack).
- Pins (5V, 3.3V, GND, Analog, Digital, PWM, AREF).
- Reset Button.
- Power LED Indicator.
- TX RX LEDs.
- Main IC.
- Voltage Regulator.

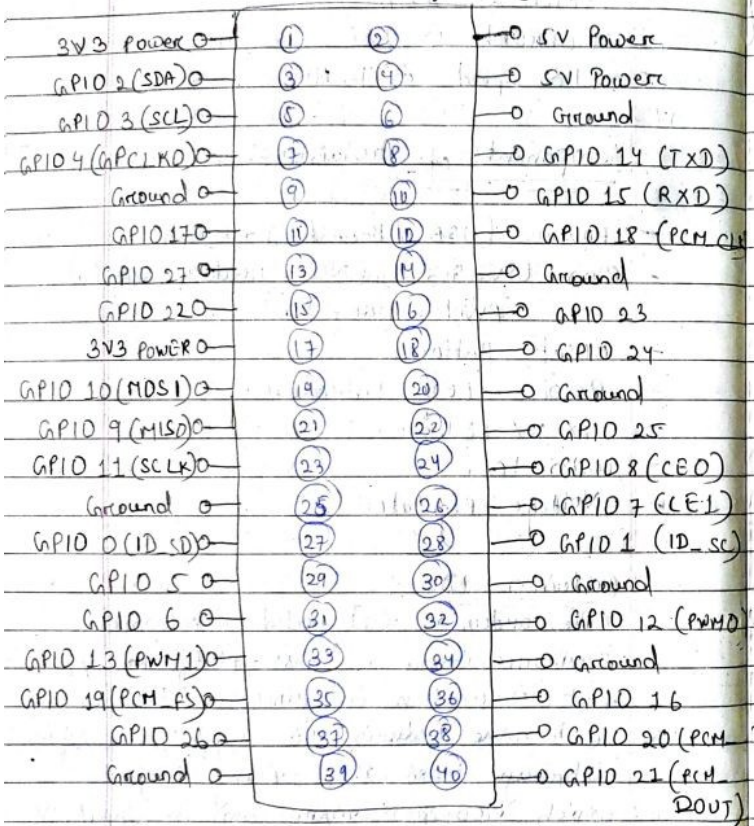
Arduino IDE :

The arduino integrated development Environment is a cross-platform appln that is written in functions from C and C++. The Arduino IDE supplies a software library from the wiring project, which provides many common input & output procedures.

CH-7

## Programming with Raspberry Pi

### Architecture and Pin configuration :-




Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi foundation in association with Broadcom. The Raspberry Pi Project originally leaned towards the promotion of teaching basic computer science in schools and in developing countries.

**Case studies :-** The raspberry Pi a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing and to learn how to program in languages like Scratch and Python. It's capable of doing everything you'd expect a desktop computer to do, from browsing the internet and playing high definition video, to making spreadsheets, word-processing, and playing games.

*** How can IOT application use Raspberry Pi :-**

With an inbuilt quadcore processor, Raspberry Pi can serve as the "Internet gateway" for IOT devices. Powered by a cloud network, Pi acts as a web server for uploading and transiting sensors data on IOT platforms.

## Implementation of IOT with Raspberry Pi:

### Raspberry Pi 4 pin description :-

This was the little intro to the Raspberry Pi 4. In this section, we'll cover the description of each pin incorporated into this tiny module.

Power and ground on RPi :-

This board comes with three types of power pins:

1. 5V
2. 3V3 (3.3V)
3. Ground (0V)

for example, if you have PIR or humidity sensors, you can use those power pins to power up those sensors.

### GPIO pins in Raspberry Pi 4 :-

GPIO pins are general-purpose input/output pins that are used for connection with external devices. These pins can be configured to either general-purpose input or general-purpose output pins or as one of up to six special settings those functions are pin dependent.

(i) External lables (from GPIO 2 to GPIO 27) come with the broadcom (BCM) naming convention. This convention is useful when you are going to program with python libraries.

(ii) Internal lables (from 1 to 40) Project the board naming convention. This convention is useful when BCM is not supported. It is used with some Programming libraries.

### SPI Pins in Raspberry Pi 4 :-

→ This Raspberry pi 4 module comes with SPI (Serial Peripheral interface) Communication Protocal. This is the type of communication Protocal that is used for master-slave communication.

→ It is employed to layout the communication between the controllers and other peripheral devices like shift registers and sensors. Two pins are used for SPI communication. i.e. MOSI (Master output Slave input) and MISO (Master input Slave output).

what is Raspberry Pi 4, Raspberry Pi 4 Pinout, Raspberry Pi 4 datasheet, raspberry pi 4 Projects ?

→ The data synchronization is done by using a clock (SCLK at GPIO 11) from the masters (RPi) and the data is conveyed to the SPI component from the module using the MOSI pin. If the component needs to reply to our module, then it sends back data through the MISO pin.

I2C pins in Raspberry Pi 4 :-

→ This RPi 4 module is incorporated with the I2C communication Protocol that comes with two pins SDL and SCL.

→ SCL :- The SCL is the serial clock line that ensures the synchronization of data transfers over the I2C bus.

→ SDL :- The SDL is the serial data pin that carries the data while this communication Protocol requires master slave roles between the devices.

UART pins in Raspberry Pi 4 :-

This board also features UART serial communication protocol. The UART Serial port comes with two pins Rx and Tx.

Tx :- The Tx is the transmission pin that is used for the transmission of serial data and Rx is the receiving pin that guarantees the receiving of serial data.

Ch-8

## Software defined Networking

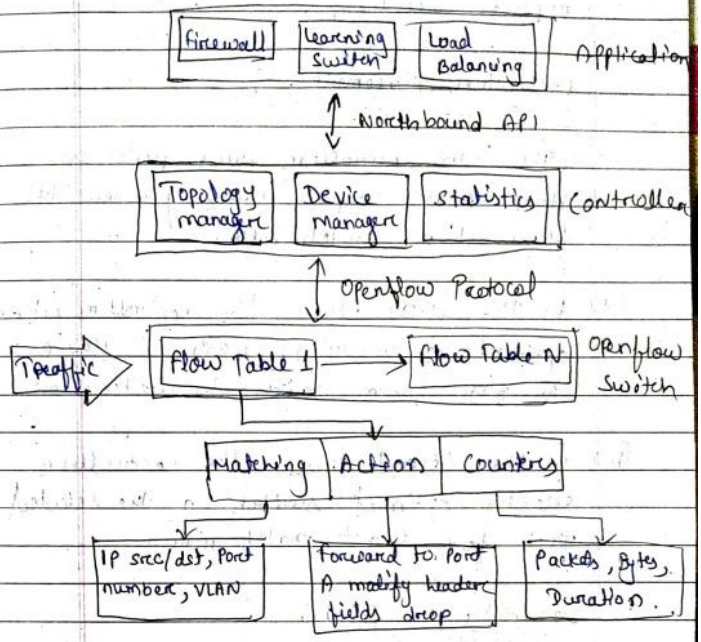
**Limitation of current Networking :-**

Traditional networking architecture and equipment are mostly built to be managed by human : on a device by device basis using manual processes. They are not built to be centrally managed, programmed or even automated.

**Origin of SDN :-** The history of SDN principles can be traced back to the separation of the control and data plane first used in the Public switched telephone network as a way to simplify provisioning and management well before this architecture began to be used in data networks.

**SDN architecture :-** Software-Defined networking (SDN) is a network architecture approach that enables the network to be intelligently and centrally controlled or programmed using software applications. This helps operators manage the entire network consistently and holistically, regardless of the underlying network technology.

**Openflow Protocol :-**




Openflow Protocol defines the communication between an openflow controller and an Openflow switch. This protocol is what most uniquely identifies openflow technology. At its essence, the protocol consists of a set of message that are sent from the controller to the switch and a corresponding set of

message that are sent in the opposite direction.

Controller Placement →

The SDN controller places rules in three phases upon receiving a new flow at a switch :

(a) In the first phase, the controller determine optimal forwarding path to route the flow from source to destination.

(b) In the second phase, the controller selects optimal switch in the selected path for exact-match rule.

Security in SDN :

Software-Defined networking (SDN) and a diverse set of SDN-based security applications will rapidly gain traction in the fight against cybercrime. SDN can make it easier to collect network usage information, which could support improved algorithm & design used to detect attacks.

Integrating SDN in IOT :

A framework for integrating IOT and SDN using Proposed OF-enable management device. Internet of things is an enabler for smart world. However the problems with internet of things is that they are devices which support heterogeneous methods of communication.

Ch-9

## Smart Homes

### Origin of smart home technology :-

The smart home concept started with the invention of remote controls, unveiled by Nikola Tesla in 1898. During the 1930s, inventors turned their attention to home automation technologies, but the idea didn't materialize until 1966, when the Echo IV, the first smart automation system was developed.

### Example of smart home technology :-

Hubs include Amazon Echo, Google Home, Insteon hub pro, Samsung smart things and Wink Hub. Some smart home systems can be created from scratch, for Example using a Raspberry Pi or other prototyping board.

### Implementation of smart home :-

(i) Temperature sensors
(ii) Lux sensors
(iii) Water level sensors
(iv) Air composition sensors
(v) video cameras for surveillance.
(vi) Voice / sound sensors
(vii) Pressure sensors.
(viii) Humidity Sensors

### what does home area network mean ?

A home network or home area network (HAN) is a type of computer network that facilitates communication among devices within the close vicinity of a home.

### Smart home benefits :-

(i) Flexibility for new devices and appliances
(ii) Maximizing home security.
(iii) Remote control of home functions.
(iv) Increased energy efficiency.
(v) Improved appliance functionality.
(vi) Home management insights.

Ch-10

## Smart city

### What is Smart city?

⇒ A smart city is an urban area that uses different types of electronic methods and sensors to collect data. Insights gained from that data are used to manage assets, resources and services efficiently; in return, that data is used to improve the operations across the city.

### Characteristics of a smart city :-

→ ~~Infrastructure~~ characteristics of a smart city Infrastructure Development. A smart city prioritizes the optimal development of infrastructure in order to enhance economy, and social, cultural and urban development.

→ Strategies to create a competitive Environment.

→ Inclusive and sustainable cities.

### Smart city framework :-

Smart city framework is a simple decision methodology that enables both the public and private sectors to plan and implement smart city initiatives more effectively. A structured method not only will enable efficiencies in city infrastructures, but also transparencies into how cities work.

### Challenges of Smart city :-

Challenge #1 : Infrastructure.

Challenge #2 : Security and Hackers.

Challenge #3 : Privacy Concerns.

Challenge #4 : Educating & Engaging the community.

Challenge #5 : Being socially inclusive.

Data fusion : The common technique for handeling multiple data source is data fusion, where it improves data output quality or extracts Knowledge

from the raw data.

**Smart parking →**

Smart parking utilizes smartphone and other sensing devices to as enabling the occupy of a parking structure or level.

Ch-11

## Industrial IOT

The industrial internet of things (IIOT) refers to the extension and use of the internet of things (IOT) in individual sectors and application.

**IOT Requirment :**

1. Cloud computing
2. Access (anywhere, anytime)
3. Security
4. Big data Analytical
5. UX (user experience)
6. Assets Management
7. Smart machines.

**Design Considerations :**

- Four considerations for manufacturing with the IIOT.
- Analytical Architecture is opening doors to new services.
- IIOT platform are Begining to converage and overtake traditional software application.
- Production efficiently and made of Production.
- Security still foremost on manufacturers minds.

## Application of IIOT :-

- Industrial automation.
- Smart robotics.
- Predictive maintainence.
- Intigration of smart tools / wearables.
- Smart logestics management.
- Software intigration for product optimization.
- Smart package management.
- Enhanced quality and security.

## Challange of IOT :-

- High - investment and ownership cost.
- Connectivity.
- Cyber security.
- Data analysis.
- Skill Gap
- Sources

## Benifits of IIOT :-

- Greater energy effeciency.
- Reduces costs.
- Better quality products.
- Improved decision - making potential.
- less equipment down time.