Date
09/03/23
Thursday/Wednesday

Date :
Page No.

IOT (Internet Of Things)

IOT is a system of interrelated computing devices mechanical and digital machines objects that are provided with unique identifiers (or sensors) and the ability to transfer data over a n/w without requiring human to human or human to computer interaction

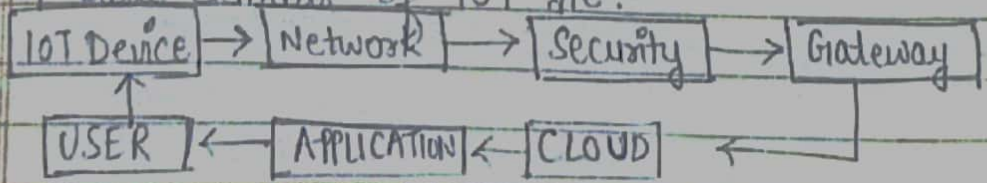
Some of the common benefits of IOT are :-

(1) Monitor overall business process.
(2) Improve customer experience
(3) Save time and money
(4) Ability to access information from anywhere, anytime.
(5) Improve communication b/w connected devices.
(6) Transferring data packets over a connected network
(7) Automated task helping to improve the quality of service (QoS) and reducing the need for human interaction.

DISADVANTAGES

(i) Security issues, as the no. of connected devices increases, more and more information is shared between the devices The potential that a hacker could steal confidential information also increases
(ii) Collecting and managing the huge data from various devices will be challenging.
(iii) If there is a bug in the system it is likely that every connected devices is corrupted.
(iv) There are no Ist for IOT compatibility i.e. why it is difficult for devices from different manufacturers to communicate with each other.

7 basic elements of IOT are :-



Date
15-03-23
Wednesday

Date / /
Page No.

TOP 10 STRATEGIC IOT TECHNOLOGIES AND TRENDS

1. Artificial Intelligence: Data in the fuel that fuels the IOT and the organisations ability to derive meaning from it & making it useful in reduction.

2. Social, legal & ethical IOT: These include ownership of data & the deduction made from it, privacy and compliance priviledges.

3. Infomatic & data storage: The theory of infomatic states monitisation of data further by seeing it as a strategic business asset

4. Shift from intelligent edge to intelligent mesh: The shift from centralised and Cloud- to edge architecture is well underway in iot space These arch will enable more flexible, intelligent and responsive iot systems.

5. IOT GOVERNANCE: As the IOT continued to expand the need for governance framework that ensures in the creation, storage, use & deletion of informat will become important.

6. SENSORS INNOVATION: Sensor mkt will evolve continously 2023 New sensors will enable a wider range of and events to be detected.

7. TRUSTED H/W & OS: By 2023, trusted h/w & OS we expect to see the deployment of that together create more trustworthy & secure iot centre.

8. NOVEL IOT USER EXPERIENCE: User experience Given by 4 factors:
(1) New sensors
(2) New algorithms
(3) New architecture
(4) New experience

9. Si Chip & innovation By 2023, it is expected to new special purpose chip will reduce the power consumption require to run iot devices

10 New wireless networking technology :-
IOT n/w involves balancing a set of competing requirements, in particular they should explore for better connectivity of iot.

Ass 1 TECHNOLOGY DRIVERS
1. CLOUD COMPUTING
2. BLOCKCHAIN
3. SENSORS
4. AI

IOT SECURITY: (1) Public preception
(2) Vulnerability to hacking
(3) Trust factors
~~(4) IOT~~

IOT PRIVACY:
(1) TOO MUCH DATA
(2) UNWANTED PUBLIC PROFILE
(3) EVE'S DROPING

Date : / /
Page No.

1. SECURITY OF THE DATA
2. RELIABELITY & STABILITY OF IOT SENSORS
3. Connectivity of all the system in iot
4. Maintaining & storing large data
5. Blending middi with the original legacy system and standardisation of protocol
6. Power consumption & optimisation in IOT devices

22/03/23 Wednesday

OVERVIEW OF GOVERNANCE IN IOT

SECURITY	PRIVACY
1 Security is mainly related to confidentiality of the data	It is more related to identification
2 Data integrity.	Data protection & legalisation.
3. Data encryption & authentication	Privacy by design & unlawful processing.

Role of governance in IOT

① An IOT governance framework should ensure data integrity & data security for information by all IOT devices in the n/w.

② It should also maintain the trusted src of info across the diff layer of the IOT Architecture.

③ An IOT usage become more widespread, the physical n/w of IOT devices grows larger & more complicated to manage, with approx 13 billion IOT devices in operation today. An IOT governance model is an effective way to address security & privacy concern as well as legal, ethical & public relation matters. It establishes the policies, procedures & practices that defines how a company will design, build, deploy & manage an IOT system

BUSINESS DRIVERS

(1) Developing the IOT products
1.1 Time to market

(2) Developing connected features
(3) Developing business model
3.1 Market positioning
3.2 Value change
3.3 Revenue Model
(4) Commercialising the IOT products
4.1 Pricing the IOT products
4.2 Driving adoption rates
4.3 Measuring success

FUTURE OF IOT

1 By 2023, the average IOT devices would be more than 3 times as per the current.
2 IOT security expanding worldwide will be 3.11 billion largely driven by Regulatory Compliance.
3 Vacandy estimates the IOT will have $11.1 ~~billion~~ trillion by 2025.

IOT Hardware Platform

1. Raspberry pi
2. Arduino
3. Cartigle
4. Pygame
5. Adafruit
6. sparkFund

Date
23/03/23
Thursday

Date : / /
Page No.

UNIT-2

IOT Protocols

★ Protocol standardisation for IOT

① This consortium consist of 17 European org from 9 country. ① It has fragmented architecture ② not holistic approach to implement IOT has yet been proposed

③ Many island solutions do exist

M2M ↔ IOT & WSN Protocol.

④ WSN (Wireless Sensor Network) M2M (Machine-to-Machine)

④ Most M2M app are developed today in a highly customize fashion.

⑤ High level M2M architecture from M2M standardisation Task Force (MSTF) does include fixed and non cellular wireless n/w.

⑥ M2M and IOT sometimes are used interchangeably in US.

⑦ Data transfort protocol standard includes JSON (Java Script Object Notation) M2M XMN

⑧ M2M security & fraud detection

⑨ Remote management of device behind gateway & firewall

⑩ Scada & RFID protocol :

Supervisory Control And Data Aquisition (SCADA)

RadioFrequency IDentification to represent these are basically an IOT pillars the whole industrial automation arena.

⑪ IEEE created std specification called Std. C37.1 for SCADA and automation system in 2007 with the use of IED (Intelligent Electronic Devices) and IOT devices in substations and power stations we are able to achieve # n/w based industrial automation

⑫ This process is now distributed rather than centralised

⑬ functions that use to be done add control center can now be done by IED i.e. M2M b/w devices

Date :
Page No.

Due to restructuring of electrical industry Traditionally vertically integrated electrid utilitie are now replaced by many entities such as1 -

1 GENCO (Generation Company)
2 TRANSCO (Transmission company)
3 DISCO (Distribution company)
4 ISO (Independent System operator)

5/04/23 Wednesday

ISSUES WITH IOT STANDARDISATION

1. It should be noted that not everything about standardisation is positive
2. It is very critical to market development
3. It make certain innovation & inhibit change when standards are accepted by the marcet
4. They could be contradictory to each other in some cases, which is always debatable.
5. Different consortium, forums & alliances have been doing standardisation in their own limited scope
6. For eg 3GPP (Third gen partnership project) covers only cellular wireless n/w
7. Even within same segment, there are more than one consortium or forum doing standardisation without enough communication with each others.
8. Some consortium are even competing with each other
9. However, some ~~tricky~~ gray zones remain in the definition, specially which technology should be included
10. Following 2 issues for IOT standardisation in partical may never have answers

info & comm techno

10.1 IOT standardisation is a highly decentralised activity.
How can the how the n/w of extremely heterogenous std setting bodies be co-ordinated.

Date : / /
Page No.

It will become essential to allow all interested stakeholders to participate in the standardisation proces and to voice their resp requirement & concern.

10-04-23 Monday

UNIFIED DATA STANDARDS (UDS)

HTTP is the TCP/IP Protocol used to deliver web page from servers to clients whereas HTML is the formatting language used to client web pages.
HTML / HTTP combinations of data formats and exchange protocol is the foundation pillar of WWW.
Many standardisation effort have been prime to define unified data representation, protocols for IOT.
Before IOT, internet was actually an internet of docum -ent or of multimedia services.
Two pillars of internet was actually including HTML turned the internet into WWW.
We need to turn the IOT into WOT (~~wireless~~ web of thin
Protocols IEEE 802.15.4 under this protocol, it define operation of low rate wireless personal area n/w (LRWPAN). This protocol also specify physical layer and MAC for LR-WPAN.
Maintained by IEEE 802.15 working group, which define the standard in 2003. Basic framework consists of 10m communication ring with Tx rate of 250 Kbps
Physical layer provide data transmission service and interface physical layer management MAC enables transmission of MAC frame through the use of channel.

BACKNED PROTOCOL

1. This is a communication protocol for building automation and control network.
2. It provide mechanism and computerised device

information.
3. It is designed along communication of building automation and control System.
4. For application: lightning control, access control etc.

Different versions of Backnet Protocol
1. Backned / IP
2. Backned / IPV6
3. Zigbee

2/04/23 MODBUS It is a serial communication protocol originally published by modicon in 1979
It is commonly available for connecting industrial electronic devices.
Reasons for the use of Modbus in industrial environment :-
(i) Openly published and royalty free
(ii) Easy to deploy and maintain
(iii) Enables communication among many devices connected to the same network.

PROTOCOL VERSIONS
Modbus ASCII
Modbus TCP/IP
Modbus over UDP
Modbus + Zigbee (1) IEEE 802.15.4 based specification for high level communication protocol
(2) It is used to create PAN with small, low power digital radius.

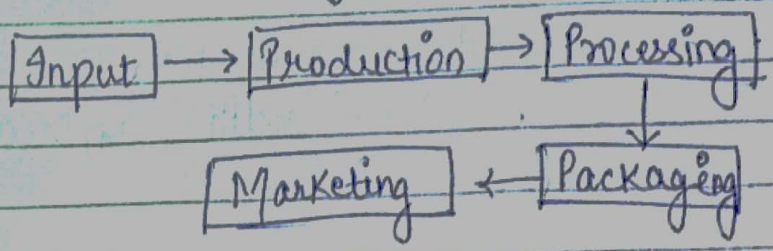
Zigbee Applications
1. Home Automation
2. Medical devices for data collection
3. Other ~~Too~~ low power, low bandwidth application

Zigbee Architecture
(1) Divided into 3 sections.

Date
19/04/23
Wednesday

Game theory
Date: / optimization
Page No.

M2M value change



1. Inputs are base raw ingredients that are turned into an product
2. Production refers to the process that the raw i/p are put through to become part of a value change
3. Processing refers to the process where a product is prepared for sale
4. Packaging refers to the process where a product can be branded as it would be recognisable to end users conv
5. Distribution / Marketing this process refers to the channel to market the product

KNX PROTOCOL

1. It is a standardised OSI base n/w communication protocol for automation
2. All the devices for the KNX installation are connected together by a two wire bus to exchange data. For eg :- sensors, actuators, system devices & components

Ass 3 Q. Draw and explain zigbee architecture.

Each end node for 'n'- devices can have multiple EPs
Each EP contains an application profile such as home automation
It can be used to control multiple devices or single device.
Zigbee Addressing Mode: Zigbee uses direct, group, & broadcast addressing for tx of information

SECURITY REQUIREMENTS IN IOT

(i) So the fundamental idea is that IOT will connect all objects around us to provide smooth communication
(iii) The challenges for global devices are Authentication, addressing embedded security
Authentication & Authorisation must be established b/w devices to achieve the security goal for IOT.
Privacy of things & security of data is one of the key challenges in IOT
Unauthorised access
Identity base verification should be done before giving the access rights
Information Corruption
Device credential must be protected from tampering
Theft of Resources
Access of shared resources over insecure channel causes theft of resources.
DoS Attack
Makes an attempt to prevent authentic users from accessing services which they are eligible for

We can control these attack
Access Control: Provides authorise access to n/w resource

2. Authentication :- Id establishment b/w communicating devices.

3. Data Confidentiality :- Protecting data from unauthorised disclosure.

4. Data Availability :- Ensuring no denial of authorise access to n/w resources.

5. Trust Management :- Decision rules needs to be evolved for trust management in IOT.

6. SECURE STORAGE :- It involves confidentiality & integrity of sensitive information stored in the system.

IOT SECURITY ARCHITECTURE ~~IN IOT~~

Sensing layer consists of actuators, devices which accept from the physical environment

N/w layer consists of internet gateways, DAS. DAS performs data aggregation & conversion function

Data processing layer is a processing unit of IOT ecosystem where data is analyze and keep process before sending it to data centres

Application layer is the last layer of IOT ecosystem Data centers or cloud is manage the stage of data where data is managed and used by end user Applications.

APPLICATION	Smart applications
DATA PROCESSING	Processing information
NETWORK	Transmission
SENSING	Data Gathering

COMPONENTS OF IOT ARCHITECTURE

1. Application & analytics components: This is the pla

2023.05.03 09:41

Date : / /
Page No.

that processes & displays the information collected by a IOT it includes analytics tool & AI, ML and

2. Integration components : These are the components that ensure the apps, tools, security and infrastructure are integrated efficiently

3. Security & Management : IOT security includes securing the physical components of a system by a firmware and embedded security provider

4. Infrastructure Components : This includes physical devices such as IOT sensors, which capture information & actuators which control the environment.

OPEN SRC ARCHITECTURE FOR IOT

The 7 high level architecture requirements for an IOT based system are

(i) Context :- It should be able to capture the context at all times 24 hrs a days 365 days / year.

(ii) Standard :- It has to use standard base communication protocol b/w IOT devices and enterprise system

(iii) Scalability :- It has to respond to ↑ load without failure proportionally.

(iv) Data Management :- It should effectively manage huge volumes of data

(v) Connectivity :- It should provide high n/w connectivity for large data payloads & continuous streaming speed.

(vi) Security :- It should use to encrypt information securely to avoid risk & vulnerability.

(vii) Inter-operability :- It should connect all the n/w

devices together in a enterprise system.

03/05/23

Why Open source architecture is important in IOT.

(1) Promote innovation

(2) Cost: Adoption of open source IOT framework involves no cost at all which encourages the community and organisation to implement IOT without hesitation

(3) Innovation:- Open source code from the communicating helps in building newer applications leading to more innovation & agility

(4) Open APIs:- Use of open source APIs for IOT framework offers the common gateway for different s/w and h/w applications to communicate with one and other.

(5) Library:- Open source IOT framework offers a wide range of libraries, ~~examples~~ SDKs, open src h/w like arduino & raspberry pi ensuring that companies remain on the cutting edge and by using these tools to customise IOT applications.

(6) Security:- Open source s/w can protect individual data by implementing really strong encryption technique.

(7) Inter-operability:- Adoption of open source solves the problem of inter-operability

CHARACTERISTICS OF IOT ARCHITECTURE

1. Loosely coupled, modular and secure
2. Platform independent
3. Scalable, flexible & can be deployed anywhere.
4. Based on open standards
5. Open & Inter-operable on the cloud
6. Application agility & integration
7.

DESIGN PRINCIPLES OF IOT ARCHITECTURE

1. Standardised integration
2. PLATFORM agnostic & PAaS
3. Data residencing and complies
4. Prefer edge intelligent over cloud computing
5. Using existing infrastructure.
6. Security by design
7. Real time processing of alarms and alerts
8. Support multiple connectivity protocols
9. Supports switch-off mode.
10. NO downtime