MCA 402C: Internet of Things

UNIT I

Fundamentals of IoT: Introduction, Definitions & Characteristics of IoT, IoT Architectures, Physical & Logical Design of IoT, Enabling Technologies in IoT, History of IoT, About Things in IoT, The Identifiers in IoT, About the Internet in IoT, IoT frameworks, IoT and M2M.

UNIT II

Sensors Networks : Definition, Types of Sensors, Types of Actuators, Examples and Working, IoT Development Boards: Arduino IDE and Board Types, RaspberriPi Development Kit, RFID Principles and components, Wireless Sensor Networks: History and Context, The node, Connecting nodes, Networking Nodes, WSN and IoT.

UNIT III

Wireless Technologies For Iot: WPAN Technologies for IoT: IEEE 802.15.4, Zigbee, HART, NFC, Z-Wave, BLE, Bacnet, Modbus. IP Based Protocols For IoT: IPv6, 6LowPAN, RPL, REST, AMPQ, CoAP, MQTT.

Edge connectivity and protocols

UNI IV

Data Handling& Analytics: Introduction, Bigdata, Types of data, Characteristics of Big data, Data handling Technologies, Flow of data, Data acquisition, Data Storage, Introduction to Hadoop. Introduction to data Analytics, Types of Data analytics, Local Analytics, Cloud analytics and applications, Edge/Fog Computing

UNIT V

Applications of IoT: Home Automation, Smart Cities, Energy, Retail Management, Logistics, Agriculture, Health and Lifestyle, Industrial IoT, Legal challenges, IoT design Ethics, IoT in Environmental Protection.

Text Books:

1. Olivier Hersent, David Boswarthick, and Omar Elloumi, — “The Internet of Things: Key Applications and Protocols”, WileyPublications

2. Vijay Madisetti and ArshdeepBahga, — “Internet of Things (A Hands-on-Approach)”, 1st Edition, VPT, 2014.

Reference Books

1. Daniel Minoli, — “Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications”, ISBN: 978-1-118-47347-4, Willy Publications

2. Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRC Press

Lecture Notes

UNIT-I

Introduction to IOT:

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.[1][2][3][4][5] Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network,[6] and be individually addressable.[7][8]

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, as well as systems, automation (including home and building automation), independently and collectively enable the Internet of things.[10] In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.[11]

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks.[12]

History[edit]

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first ARPANET-connected appliance,[13] able to report its inventory and whether newly loaded drinks were cold or not.[14] Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IOT.[15][16] In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories".[17] Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.[18]

The concept of the "Internet of things" and the term itself, first appeared in a speech by Peter T. Lewis, to the Congressional Black Caucus Foundation 15th Annual Legislative Weekend in Washington, D.C., published in September 1985.[19] According to Lewis, "The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices."

The term "Internet of things" was coined independently by Kevin Ashton of Procter & Gamble, later of MIT's Auto-ID Center, in 1999,[20] though he prefers the phrase "Internet *for* things".[21] At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things,[22] which would allow computers to manage all individual things.[23][24][25] The main theme of the Internet of things is to embed short-range mobile transceivers in various gadgets and daily necessities to enable new forms of communication between people and things, and between things themselves.[26]

In 2004 Cornelius "Pete" Peterson, CEO of NetSilicon, predicted that, "The next era of information technology will be dominated by [IoT] devices, and networked devices will ultimately gain in popularity and significance to the extent that they will far exceed the number of networked computers and workstations." Peterson believed that medical devices and industrial controls would become dominant applications of the technology.[27]

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.[28]

characteristics of internet of IoT:

According to the definition of IoT, It is the way to interconnection with the help of the internet devices that can be embedded to implement the functionality in everyday objects by enabling them to send and receive data. Today data is everything and everywhere. Hence, IoT can also be defined as the analysis of the data generate a meaning action, triggered subsequently after the interchange of data. IoT can be used to build applications for agriculture, assets tracking, energy sector, safety and security sector, defence, embedded applications, education, waste management, healthcare product, telemedicine, smart city applications, etc.

Characteristics of the Internet of Things :

There are the following characteristics of IoT as follows. Let’s discuss it one by one.

1. Connectivity –

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.

2. Intelligence and Identity –

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3. Scalability –

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4. Dynamic and Self-Adapting (Complexity) –

IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night).

5. Architecture –

IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ' products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6. Safety –

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

7. Self Configuring – This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Architecture of IoT:

Internet of Things (IoT) technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

So. here in this article we will discuss basic fundamental architecture of IoT i.e., 4 Stage IoT architecture.

4 Stage IoT architecture

So, from the above image it is clear that there is 4 layers are present that can be divided as follows: Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

1. Sensing Layer –

Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.

2. Network Layer –

Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc). Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also some times decision making based on inputted data and data management services, etc.

3. Data processing Layer –

This is processing unit of IoT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.

4. Application Layer –

This is last layer of 4 stages of IoT architecture. Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

Physical and Logical Design of IoT:

In this article we discuss Physical and Logical Design of IoT. Physical Design of IoT system refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Communication established between things and cloud based server over the Internet by various IoT protocols. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation.

Physical Design of IoT

Physical Design of IoT refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. IoT Protocols helps Communication established between things and cloud based server over the Internet.

Things

Basically Things refers to IoT Devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Things are is main part of IoT Application. IoT Devices can be various type, Sensing Devices, Smart Watches, Smart Electronics appliances, Wearable Sensors, Automobiles, and industrial machines. These devices generate data in some forms or the other which when processed by data analytics systems leads to useful information to guide further actions locally or remotely.

For example, Temperature data generated by a Temperature Sensor in Home or other place, when processed can help in determining temperature and take action according to users.

Above picture, shows a generic block diagram of IoT device. It may consist of several interfaces for connections to other devices. IoT Device has I/O interface for Sensors, Similarly for Internet connectivity, Storage and Audio/Video.

IoT Device collect data from on-board or attached Sensors and Sensed data communicated either to other device or Cloud based sever. Today many cloud servers available for especially IoT System. These Platfrom known as IoT Platform. Actually these cloud especially design for IoT purpose. So here we can analysis and processed data easily.

How it works ? For example if relay switch connected to an IoT device can turn On/Off an appliance on the commands sent to the IoT device over the Internet.

IoT Protocols

IoT protcols help to establish Communication between IoT Device (Node Device) and Cloud based Server over the Internet. It help to sent commands to IoT Device and received data from an IoT device over the Internet. An image is given below. By this image you can understand which protocols used.

Link Layer

Link layer protocols determine how data is physically sent over the network's physical layer or medium (Coxial calbe or other or radio wave). Link Layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (eg. coxial cable).

Here we explain some Link Layer Protocols:

802.3 – Ethernet : Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

WiFi : IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

Wi-Max : The standard for WiMAX technology is a standard for Wireless Metropolitan Area Networks (WMANs) that has been developed by working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access. Initially 802.16a was developed and launched, but now it has been further refined. 802.16d or 802.16-2004 was released as a refined version of the 802.16a standard aimed at fixed applications. Another version of the standard, 802.16e or 802.16-2005 was also released and aimed at the roaming and mobile markets.

LR-WPAN : A collection of standards for Low-rate wireless personal area network. The IEEE's 802.15.4 standard defines the MAC and PHY layer used by, but not limited to, networking specifications such as Zigbee®, 6LoWPAN, Thread, WiSUN and MiWi™ protocols. The standards provide low-cost and low-speed communication for power constrained devices.

2G/3G/4G- Mobile Communication : These are different types of telecommunication generations. IoT devices are based on these standards can communicate over the celluer networks.

Network Layer

Responsible for sending of IP datagrams from the source network to the destination network. Network layer performs the host addressing and packet routing. We used IPv4 and IPv6 for Host identification. IPv4 and IPv6 are hierarchical IP addrssing schemes.

IPv4 :

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s.

IPv6 : Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. In December 1998, IPv6 became a Draft Standard for the IETF, who subsequently ratified it as an Internet Standard on 14 July 2017. IPv6 uses a 128-bit address, theoretically allowing 2128, or approximately 3.4×1038 addresses. Source – wikipedia

6LoWPAN : 6LoWPAN is an acronym of IPv6 over Low-Power Wireless Personal Area Networks.6LoWPAN is the name of a concluded working group in the Internet area of the IETF. 6LoWPAN is a somewhat contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi.

Transport Layer

This layer provides functions such as error control, segmentation, flow control and congestion control. So this layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP : TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. The Internet Engineering Task Force (IETF) defines TCP in the Request for Comment (RFC) standards document number 793.

UDP : User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

Application Layer

Application layer protocols define how the applications interface with the lower layer protocols to send over ther network.

HTTP : Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests. Though often based on a TCP/IP layer, it can be used on any reliable transport layer, that is, a protocol that doesn't lose messages silently like UDP does. RUDP — the reliable update of UDP — is a suitable alternative.

CoAP : CoAP-Constrained Application Protocol is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252. It enables devices to communicate over the Internet. It is defined as Contrained Application Protocol, and is a protocol intended to be used in very simple hardware. The protocol is especially targeted for constrained hardware such as 8-bits microcontrollers, low power sensors and similar devices that can't run on HTTP or TLS. It is a simplification of the HTTP protocol running on UDP, that helps save bandwidth. It is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.

WebSocket : The WebSocket Protocol enables two-way communication between a client running untrusted code in a controlled environment to a remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The goal of this technology is to provide a mechanism for browser-based applications that need two-way communication with servers that does not rely on opening multiple HTTP connections (e.g., using XMLHttpRequest or <iframe>s and long polling).

MQTT :

MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport and useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium. For example, it has been used in sensors communicating to a broker via satellite link, over

occasional dial-up connections with healthcare providers, and in a range of home automation and small device scenarios.

MQTT protocol runs on top of the TCP/IP networking stack. When clients connect and publish/subscribe, MQTT has different message types that help with the handshaking of that process. The MQTT header is two bytes and first byte is constant. In the first byte, you specify the type of message being sent as well as the QoS level, retain, and DUP (duplication) flags. The second byte is the remaining length field.

XMPP : Extensible Messaging and Presence Protocol (XMPP) is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Originally named Jabber, the protocol was developed by the eponymous open-source community in 1999 for near real-time instant messaging (IM), presence information, and contact list maintenance. Designed to be extensible, the protocol has been used also for publish-subscribe systems, signalling for VoIP, video, file transfer, gaming, the Internet of Things (IoT) applications such as the smart grid, and social networking services.

DDS : The Data Distribution Service (DDS™) is a middleware protocol and API standard for data-centric connectivity from the Object Management Group® (OMG®). It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical Internet of Things (IoT) applications need.

In a distributed system, middleware is the software layer that lies between the operating system and applications. It enables the various components of a system to more easily communicate and share data. It simplifies the development of distributed systems by letting software developers focus on the specific purpose of their applications rather than the mechanics of passing information between applications and systems.

AMQP : The AMQP – IoT protocols consist of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model. AMQP has the following three additives, which might link into processing chains in the server to create the favored capability.

- Exchange: Receives messages from publisher primarily based programs and routes them to ‘message queues’.
- Message Queue: Stores messages until they may thoroughly process via the eating client software.
- Binding: States the connection between the message queue and the change.

Logical Design of IoT

In this article we discuss Logical design of Internet of things. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation. For understanding Logical Design of IoT, we describes given below terms.

- IoT Functional Blocks
- IoT Communication Models

- IoT Communication APIs

IoT Functional Blocks

An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.

functional blocks are:

Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.

Communication: Handles the communication for the IoT system.

Services: services for device monitoring, device control service, data publishing services and services for device discovery.

Management: this blocks provides various functions to govern the IoT system.

Security: this block secures the IoT system and by providing functions such as authentication , authorization, message and content integrity, and data security.

Application: This is an interface that the users can use to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyze the processed data.

History of IOT:

Simply stated, the Internet of Things consists of any device with an on/off switch that is connected to the Internet. The Internet of Things (IoT) involves machines communicating information over the internet, and has not been around for very long.

Machines have been providing direct communications since the telegraph (the first landline) was developed in the 1830s and 1840s. Described as “wireless telegraphy,” the first radio voice transmission took place on June 3, 1900, providing a necessary component for developing the Internet of Things. The development of computers began in the 1950s.

HAVE YOU HEARD? WE HAVE A NEW PODCAST!

Tune in weekly to hear different data experts discuss how they built their careers and share tips and tricks for those looking to follow in their footsteps.

The internet, itself a significant component of the IoT, started out as part of DARPA (Defense Advanced Research Projects Agency) in 1962, and evolved into ARPANET (Advanced Research Projects Agency Network) in 1969.

In the 1980s, commercial service providers began supporting public use of ARPANET, allowing it to evolve into our modern Internet. Satellites and landlines provide basic communications for much of the IoT.

Global Positioning Satellites (GPS) became a reality in early 1993, with the Department of Defense providing a stable, highly functional system of 24 satellites. This was quickly followed by privately owned, commercial satellites being placed in orbit, making the IIoT much more functional.

Realizing the Concept

The Internet of Things, as a concept, wasn't officially named until 1999, but one of the first examples of an IoT is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Mellon University. Local programmers would connect through the Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip to purchase one.

Kevin Ashton, MIT's Executive Director of Auto-ID Labs, coined the phrase "Internet of Things" in 1999. He was the first to describe the IoT, while making a presentation for Procter & Gamble, but the definition of the IoT has evolved over time. Mr. Ashton stated:

"Today computers, and, therefore, the Internet, are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a barcode. The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh, or past their best."

The Early 2000s

Kevin Ashton (the guy who came up with the name "Internet of Things") believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things — primarily as an inventory tracking solution.

In hindsight, Inventory tracking has become one of the more obvious advantages of the IoT.

He concluded if all devices were "tagged," computers could manage, track, and inventory them. To some extent, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes.

In 2002-2003, Walmart and the US Department of Defense were the first large organizations to embrace Ashton's model of tracking inventory using tagging, RFID, and the Internet of Things.

Ring, a doorbell that links to your smartphone, provides an excellent example of the T00nternet of Things being used at home. Ring signals you when the doorbell is pressed, and lets you see who it is, and to speak with them.

The Ring doorbell was developed in 2011 by Jamie Siminoff because he wanted to see who was at his door while he was in the garage, working. He couldn't hear the doorbell from the garage and kept missing deliveries.

An additional and important component in developing a functional IoT took place in June of 2012, when the major Internet service providers and web companies agreed to increase address space on the global Internet by enabling IPV6 for their services and products. Steve Leibson, of the Computer History Museum, stated,

"The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths."

Put another way, we are not going to run out of internet addresses anytime soon.

IoT Getting Smarter

"Smart cities" can use the IoT to reduce waste and maximize the efficient use of energy. The IoT can also be used to streamline traffic flows and locate available parking.

In 2012, The Swiss Federal Office of Energy started a pilot program called "Smart City Switzerland." They brought representatives from universities, business, and public administration together to discuss new ideas for the urban environment. Smart City Switzerland has over sixty projects underway and supports new scientific partnerships and innovation. (Smart City Switzerland has evolved into something quite impressive.)

A well-designed smart city supports all kind of sensors that are connected to the internet and provides:

- Traffic monitoring- Real-time tracking and reporting of traffic.
- Air quality monitoring- Integrated IoT sensors can identify polluters.
- Smart transportation- Smart traffic lights streamline traffic efficiency and public transport.
- Smart parking- Sensors installed in pavement, etc. to determine occupancy of the parking lot, which is communicated to drivers.
- Smart public lighting- Low energy lighting combined with timing and sensors.
- Smart buildings- When connected to the smart city by way of the internet, it becomes a part of the city infrastructure.

A smart building, by itself, uses sensors and automated processes to control the building's operations, which includes air conditioning, heating, ventilation, security, lighting, and other systems. Smart buildings are integrated systems and share vital information.

The Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) is an extension of the IoT, and uses actuators and smart sensors, which are networked together with a company's industrial applications. The goal is to give industries greater efficiency and reliability. The IIoT includes robotics and software-defined production processes.

The cloud's massive storage capacity (2002) was necessary for the modern version of the IIot to become a reality.

The IIoT came into being in roughly 2010, with several large companies developing their own systems. GE is given credit for creating the term “Tndustrial Tnternet of Things,” In 2012.

The Internet of Things Becomes a Part of Life

By the year 2013, the IoT had become a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems.

This includes almost anything you can think of, ranging from mobile phones to building maintenance to the jet engine of an airplane. Medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, can transfer dataover a network and are members of the IoT.

The IoT Goes Mobile – 2015

Smartphones are part of the IoT, and have become an important communications tool for many individuals. In 2015, they joined the IoT with a high degree of enthusiasm from marketers. The sensors within these devices are monitored by marketing departments, who send out certain promotions based on the customer and the product’s location.

The healthcare industry has also taken advantage of this trend. Devices, such as smartwatches, smartphones, and ingestible monitors can keep track of a patient’s data regarding blood pressure, heart rate, and other concerns in real time.

Cars and trucks have become members of the IoT. A connected vehicle works with other devices over wireless networks. This technology allows various “connected networks” to access and communicate with the vehicles.

Cars and trucks are already loaded with sensors and technology, including OBD (on-board diagnostics) and GPS. By maximizing their use of these technologies, businesses can extract information from their fleets about maintenance requirements, driving conditions, and routes in real-time.

Self-driving cars use the cloud to respond to adjacent cars, traffic data, maps, weather, surface conditions, etcetera. Use of the cloud helps the vehicles to monitor their surroundings and make better decisions.

Self-driving cars are new members of the IOT. The first truly self-driving vehicle appeared in the 1980s. In October of 2021, May Mobility launched a pilot program to test their self-driving software.

Human neighborhoods are now becoming part of the interconnected community called the Internet of Things.

Things In IOT:

The Value of Connected “Things” in Healthcare, Logistics and Agriculture

IoT for Healthcare: Our Bodies as “Things” connected to the Internet

“Things” in IoT can also be [“wearables” that serve medical purposes](). Devices that monitor your bodily functions and systems daily and make that data available to your doctors can function as an early warning system for health issues and a way for you to keep yourself accountable to your health goals.


Image Credit: Sensors Magazine

As [Lalit Panda]() writes in [What Is the Internet of Medical Things (IoMT)?](), “With streaming information, preventive care can reduce hospitalization and reduce the cost of acute care significantly.” However, both Panda and Kristina Podnar, in [her article](), warn of the serious risk of accidents and abuse that come with connecting our bodies to the internet. In the case of healthcare, a “thing” in the Internet of Things would be our very bodies.

IoT for Logistics: Packages and Containers As “Things” Connected to the Internet

Logistics and Supply Chain Management are all about moving things from point A to point B. Keeping tracking of those things in an ideal world isn’t terribly difficult. You send shipment X from warehouse Y to customer Z, and you know everything will work out, right? Wrong! The world is dynamic, shifting, and chaotic. Things go wrong. Everything from weather disasters to piracy can affect global shipping lanes

and cause delays and financial losses. And sometimes it's merely naturally built-in inefficiencies that cause losses and delays.

In 2018, in the UK alone, inefficiencies in the supply chain resulted in losses of about $2B, due to what one study called "a game of Chinese whispers" as packages zigzag around the world. Ericsson recently argued in an article on IoT For All that "supply chain participants are connected—just not to each other or not at the right time."

That's where the Internet of Things comes in. For Logistics and Supply Chain Applications, "things" in IoT cargo containers, trucks, port utility equipment and, most importantly, data pipelines and digital ledgers for tracking shipments reliably as they traverse the world and change hands.

Image Credit: All Things Supply Chain

IoT for Agriculture: “Things” as Tractors, Soil Sensors and Irrigation Systems

From irrigation to crop rotation to fertilization to genetic modification, we’ve been changing the way we grow and harvest food for thousands of years. Farms have grown from small, family- or community-managed organizations to vast enterprises that sprawl across thousands or even millions of acres. As populations exploded throughout the 20th century, farmers have turned to technology to meet growing demands. The 21st century is no different; farmers continue to find innovative ways to meet food supply needs in an increasingly interdependent and environmentally unstable world.

IoT is enabling a whole range of agricultural innovations. As SciForce writes on IoT For All, farmers are starting to use IoT, drones and AI to “increase the quantity and quality of products while optimizing the human labor required by production.”

The photo below shows a soil monitoring solution called “CropX” being used to help farmers better understand which fields need watering when and how soil conditions change over time—all remotely and at massive scale.


Image Credit: Smart2Zero

In this example, CropX represents a “thing” in the Internet of Things. It’s a thing that you can embed in your fields, and since it’s connected to the internet, you can gather insights from it about what’s going on in the soil feeding your crops—remotely and at massive scale, even from the comfort of your farmhouse living room!

The Best Way to Predict the Future Is to Build It

In the now distant past, every “thing” was disconnected. Then the telephone came around and enabled us to connect people and spaces across hundreds and then thousands of miles. Then we started sending not only our voices but other kinds of information across the wire, like documents, images, videos, *etc*. But we couldn’t stop by connecting only things like computers and smartphones to the internet. Why end there? Now we’re focused on connecting the myriad other objects and spaces we use for everyday life and business processes to the internet so that we can extract insights about the world around us and interact with our “things” remotely and at massive scale.

Identifiers in IoT:

identifiers play an important role in Internet of Things (IoT). Identification of the Thing itself comes immediately into my mind. Also the use of identifiers as communication addresses like IP and Ethernet MAC addresses is an obvious application. However when you dive deeper into IoT systems you will recognize many more applications for identifiers. For the design, but also for the use of IoT solutions it is therefore important to know the various usages of identifiers, the related requirements, interoperability, security and privacy issues and which standards are available for them.

These topics came up in AIOTI WG03 on IoT Standards late 2016 and we decided to analyse them further and provide a report about our findings. The starting point of our activity was a survey that we performed in spring 2017. The survey asked questions about IoT use cases, the specific purpose of identifiers, related requirements, standards and standardization gaps. It was sent to standardisation bodies, industry alliances, research projects and individual companies around the world and we received back over eighty responses. These responses were a significant input to our report, along with research and standardisation documents. They showed that identifiers are used in IoT to identify various types of entities for many purposes and within different contexts. The figure below shows an example for the different identifiers used in a fitness tracking use case.

This use case includes identifiers for:

- Things
- Communication
- User
- Data
- Location
- and Services & Applications

With the classification of identifiers and the categorization of requirements we tried to provide a structure that may help system architects and developers to understand the type of identifiers that they need for their solution and guide them in selecting the specific identifier schemes. In general no single identification scheme fits all needs. Furthermore many identification are already standardized and in use. We therefore do not define or recommend specific solutions and standards, but provide examples and summaries in order to indicate what has to be taken into account when considering identifiers in IoT.

IoT frameworks:

IoT (Internet of Things) is a network of devices which are connected to the internet for transferring and sensing the data without much human intervention, the framework used to this is termed as the IoT framework, this framework consists all the required capabilities for the cloud support and other needs which is needed to satisfy the IoT technology, few of the common IoT frameworks that are used frequently are KAA IoT, Cisco IoT Cloud Connect, ZETTA IoT, SAP IoT, IBM Watson, Hewlett Packard Enterprise, etc

What is the IoT Framework?

IoT is a key part of a large IoT ecosystem, which promotes and links all elements in the scheme. It allows device management, handles communication protocols on software and hardware, collects / analyses information, improves information flow and intelligent apps functions.

List of IoT Framework

Now we will discuss the IoT Framework one by one

1. KAA IoT

Kaa IoT is one of the most effective and rich Open Source Internet of Things Cloud Platforms, where anyone can freely implement their smart product concepts. You can manage an N number of devices connected to each other with cross-device interoperability on this platform. You can monitor your machine in actual time by providing and configuring remote devices. Kaa enables information exchange between linked devices, the IoT Cloud, information and visualization systems, as well as other elements of IoT Ecosystems

2. Cisco IoT Cloud Connect

Cisco IoT Cloud Connect provides robust, automated, and highly secure connectivity for the enterprise. IoT data management is done by the Cisco Kinetic IoT platform to extract, move and compute the data. As Cisco is very famous for its security services, it protects IoT deployment against threats with a secure IoT architecture.

3. ZETTA IoT

Zetta is nothing but a server-oriented platform developed based on the REST, NodeJS, and the Siren hypermedia-API-strip flow-based reactive programming philosophy. After being abstracted as REST APIs they are connected with cloud services. These internet services include tools for visualizing machine analytics and support such as Splunk. It builds a gero-distributed network through connectivity with systems like Heroku to endpoints like Arduino and Linux hackers.

4. Salesforce IoT

Salesforce is power by thunder. Thunder allows companies to unlock earlier unseen ideas and allows anyone to take proactive, personalized activities from any device to bring their clients closer than ever. More than 150,000 clients worldwide were held by Salesforce. Salesforce has a 19.7% market share in the globe of CRM. SAP (12.%1), Microsoft (6.2%), Oracle (9.1%) are far behind its nearest rivals. Many businesses now develop their apps or migrate to Salesforce on the Salesforce platform. This has raised demand for developers and administrators from Salesforce.

5. DeviceHive IoT

DeviceHive is another rich IoT open-source platform that is distributed under the Apache 2.0 license and can be used and changed free of charge. It provides deployment options for Docker and Kubernetes and can be downloaded and used both by public and personal cloud. You can run batch analysis and machine learning above and beyond your device information. DeviceHive supports several libraries, including Android and iOS.

6. Oracle IoT

We surely include Oracle, a worldwide software company known to offer its top level of solutions in database management, and business software, as we compare the top Internet-of-Things platforms. Oracle offers its flexible environment outstanding company possibilities to create company applications. Oracle supports the processing and builds large-scale IoT networks with very wide data. The use of advanced security systems to protect IoT systems against external threats is another worth mentioning. Since these systems usually have different devices, some of which have no security tool, it is not sufficiently justifiable to implement centralized security measures.

7. SAP IoT

The SAP Internet of Things cloud platform has everything you need to build and handle an IoT application. The SAP platform provides a convenient environment to remotely manage and monitor all connected devices of your IoT system. In the SAP Platform a remote-devices we can connect directly or through cloud service. Obviously, SAP can use IoT information to create machine learning and artificial intelligence applications while maintaining recent technological trends.

8. Microsoft Azure IoT

Without the Microsoft Azure solution, a cloud service giant with AWS and Google Cloud platform, the comparison of our IoT platform will be not complete. The Microsoft Azure IoT Suite provides preconfigured solutions and the ability to personalize and develop new solutions to meet the project requirements. The strongest safety mechanisms, superb scalability and simple integration with your current or future systems are achieved through Microsoft Azure Internet of thing Suite.

9. Google Cloud Platform – IoT framework

Things can be done by Google. Google Cloud is one of the best IoT systems available today with its end-to-end platform. Google stands out from the others because it can process the large quantity of information using Cloud IoT Core. Due to Google's Cloud Data Studio and Big Query you get advanced analysis. With the help of Google Cloud Platform, you can accelerate your business and with that, you can speed up your device.

10. IBM Watson – IoT framework

We can not expect the Big Blue to miss the chance to make a difference in the IoT segment. IBM Watson is very popular among the internet of thing platform among developers. The Bluemix hybrid cloud-supported Watson IoT platform allows developers to use IoT-applications easily. IBM Watson manages the secure communication and also data storage. Real-time data exchange also is done by IBM Watson.

11. Hewlett Packard Enterprise – IoT framework

Hewlett Packard Enterprise's universal business platform offers scalability for its customers by offering solutions to most of their problems. The platform provides cloud-based assistance or local support. In smart cities and the automobile industry, HPE universal of things platform was used

properly. The data monetization of several businesses has been carried out by HPE. Hewlett Packard Enterprise Collects analyzes information in order to grow the company. In the Hewlett Packard Enterprise M2M device management in Single point, Single seller.

12. DataV by Bsquare – IoT framework

The next cloud platform is DataV by Bsquare. The company is working with the best in the company, including Google, Amazon web services, and Microsoft. Bsquare takes its services seriously and has introduced the DataV application, the hybrid framework for managing your services. It offers a variety of services that predict and analyze all of your ecosystem problems. It Improves the condition maintenances.

13. Mindsphere by Siemens – IoT framework

Mindsphere from Siemens provides a cost-effective platform as a service that is ideal for application development. The cost-efficient platform allows you to connect all your appliances to a cloud solution. In accordance with the DIn ISO / IEC 27001 standard, Siemens claims every stored information is strictly confidential. You can choose open interfaces and local connectivity from the business. Allow you to regulate machine information in order to open fresh opportunities.

14. Ayla Network – IoT framework

Ayla networks have developed their platform as a solution for enterprises. Agile Ayla networks have been established to support customers with the smooth establishment of services, not only to develop the product. In addition to the Ayla agile platform, AMAP is an agile mobile app platform from Ayla that develops and guides consumers through app development.

15. MBED IoT Device platform

The open-source service is available on the Apache 2.0 Arm MBED computer platform. It involves cloud services, developer tools, and operating systems, that facilitate the creation and operation of business goods. The service is designed to simplify users ‘ processes. MBED OS was designed to connect all your devices as an open-source platform. The platform provides services from over 60 partners and free access to a community of 200,000 designers. You can flexibly access MBED club service

16. Amazon Web Services (AWS) IoT framework

Amazon Web Services (AWS) is an IoT platform provided by Amazon. This IoT platform provides cloud computing, database, and security services through the AWS Console. There are so many other services such as Regions, Availability Zones, and Virtual Private Clouds (VPCs). It helps to ease out the improving durability, distribution, availability of the application. It provides Registry for recognizing devices, Secure Device Gateway, Compatible Software Development Kit for devices which AWS partnered with HW manufacturers like Intel, Texas Instruments, Broadcom and Qualcomm.

17. Mocana – IoT framework

The final one on the list is the Mocana company’s safety platform. The platform seeks to provide industrial IoT devices and clouds with security. The company provides currently more than 100 companies with services.

18. RTI IoT

RTI is one of the IoT platforms that is the oldest and most pioneering provider and also it is the Most Influent Industrial of the internet of thing firm. Connext DDS is built especially for smart computers and their corresponding cyber-physical systems. Connext DDS does not require response brokers, directory services, servers, as well as administration, unlike messaging middleware designed mainly for IT systems.

7.Difference between IoT and M2M?

1. Internet of Things : IOT is known as the Internet of Things where things are said to be the communicating devices that can interact with each other using a communication media. Usually every day some new devices are being integrated which uses IoT devices for its function. These devices use various sensors and actuators for sending and receiving data over the internet. It is an ecosystem where the devices share data through a communication media known as the internet. 2. Machine to Machine : This is commonly known as Machine to machine communication. It is a concept where two or more than two machines communicate with each other without human interaction using a wired or wireless mechanism. M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.

IoT and M2M :

Basis of IoT M2M

Abbreviation Internet of Things Machine to Machine

Intelligence Devices have objects that are responsible for decision making Some degree of intelligence is observed in this.

Connection type used The connection is via Network and using various communication types. The connection is a point to point

Communication protocol used Internet protocols are used such as HTTP, FTP, and Telnet.

Traditional protocols and communication technology techniques are used

Data Sharing Data is shared between other applications that are used to improve the end-user experience. Data is shared with only the communicating parties.

Internet Internet connection is required for communication Devices are not dependent on the Internet.

Type of Communication It supports cloud communication It supports point-to-point communication.

Computer System Involves the usage of both Hardware and Software. Mostly hardware-based technology

Scope A large number of devices yet scope is large. Limited Scope for devices.

Business Type used Business 2 Business(B2B) and Business 2 Consumer(B2C) Business 2 Business (B2B)

Open API support Supports Open API integrations. There is no support for Open APIs

Examples Smart wearables, Big Data and Cloud, etc. Sensors, Data and Information, etc.

Short Questions:

1.What is the definition of IOT?

2.Explain about history of IOT?

3.What are the characteristics of IOT?

4.Explain about things in IOT?

Long Questions:

1.Explain about physical and logical design of IOT?

2.Explain about IOT frameworks and Architecture of IOT?

3.Explain about IOT and M2M in detail?

UNIT-2

Sensors and Networks

Sensor:

We live in a World of Sensors. You can find different types of Sensors in our homes, offices, cars etc. working to make our lives easier by turning on the lights by detecting our presence, adjusting the room temperature, detect smoke or fire, make us delicious coffee, open garage doors as soon as our car is near the door and many other tasks.

All these and many other automation tasks are possible because of Sensors. Before going in to the details of What is a Sensor, What are the Different Types of Sensors and Applications of these different types of Sensors, we will first take a look at a simple example of an automated system, which is possible because of Sensors (and many other components as well).

Outline

- Real Time Application of Sensors

- What is a Sensor?
- Classification of Sensors
- Different Types of Sensors
  - Temperature Sensor
  - Proximity Sensors
  - Infrared Sensor (IR Sensor)
  - Ultrasonic Sensor
  - Light Sensor
  - Smoke and Gas Sensors
  - Alcohol Sensor
  - Touch Sensor
  - Color Sensor
  - Humidity Sensor
  - Tilt Sensor

Real Time Application of Sensors

The example we are talking about here is the Autopilot System in aircrafts. Almost all civilian and military aircrafts have the feature of Automatic Flight Control system or sometimes called as Autopilot.

An Automatic Flight Control System consists of several sensors for various tasks like speed control, height monitoring, position tracking, status of doors, obstacle detection, fuel level, maneuvering and many more. A Computer takes data from all these sensors and processes them by comparing them with pre-designed values.

The computer then provides control signals to different parts like engines, flaps, rudders, motors etc. that help in a smooth flight. The combination of Sensors, Computers and Mechanics makes it possible to run the plane in Autopilot Mode.

All the parameters i.e., the Sensors (which give inputs to the Computers), the Computers (the brains of the system) and the mechanics (the outputs of the system like engines and motors) are equally important in building a successful automated system.

This is an extremely simplified version of Flight Control System. In fact, there are hundreds of individual control systems which preform unique tasks for a safe and smooth journey.

But in this tutorial, we will be concentrating on the Sensors part of a system and look at different concepts associated with Sensors (like types, characteristics, classification etc.).

What is a Sensor?

There are numerous definitions as to what a sensor is but I would like to define a Sensor as an input device which provides an output (signal) with respect to a specific physical quantity (input).

The term “input device” in the definition of a Sensor means that it is part of a bigger system which provides input to a main control system (like a Processor or a Microcontroller).

Another unique definition of a Sensor is as follows: It is a device that converts signals from one energy domain to electrical domain. The definition of the Sensor can be better understood if we take an example in to consideration.

The simplest example of a sensor is an LDR or a Light Dependent Resistor. It is a device, whose resistance varies according to intensity of light it is subjected to. When the light falling on an LDR is more, its resistance becomes very less and when the light is less, well, the resistance of the LDR becomes very high.

We can connect this LDR in a voltage divider (along with other resistor) and check the voltage drop across the LDR. This voltage can be calibrated to the amount of light falling on the LDR. Hence, a Light Sensor.

Now that we have seen what a sensor is, we will proceed further with the classification of Sensors.

Classification of Sensors

There are several classifications of sensors made by different authors and experts. Some are very simple and some are very complex. The following classification of sensors may already be used by an expert in the subject but this is a very simple classification of sensors.

In the first classification of the sensors, they are divided in to Active and Passive. Active Sensors are those which require an external excitation signal or a power signal.

Passive Sensors, on the other hand, do not require any external power signal and directly generates output response.

The other type of classification is based on the means of detection used in the sensor. Some of the means of detection are Electric, Biological, Chemical, Radioactive etc.

The next classification is based on conversion phenomenon i.e., the input and the output. Some of the common conversion phenomena are Photoelectric, Thermoelectric, Electrochemical, Electromagnetic, Thermooptic, etc.

The final classification of the sensors are Analog and Digital Sensors. Analog Sensors produce an analog output i.e., a continuous output signal (usually voltage but sometimes other quantities like Resistance etc.) with respect to the quantity being measured.

Digital Sensors, in contrast to Analog Sensors, work with discrete or digital data. The data in digital sensors, which is used for conversion and transmission, is digital in nature.

Types of Sensors:

The following is a list of different types of sensors that are commonly used in various applications. All these sensors are used for measuring one of the physical properties like Temperature, Resistance, Capacitance, Conduction, Heat Transfer etc.

1. Temperature Sensor
2. Proximity Sensor
3. Accelerometer
4. IR Sensor (Infrared Sensor)
5. Pressure Sensor
6. Light Sensor
7. Ultrasonic Sensor
8. Smoke, Gas and Alcohol Sensor
9. Touch Sensor
10. Color Sensor
11. Humidity Sensor
12. Position Sensor
13. Magnetic Sensor (Hall Effect Sensor)
14. Microphone (Sound Sensor)
15. Tilt Sensor
16. Flow and Level Sensor
17. PIR Sensor
18. Touch Sensor
19. Strain and Weight Sensor

We will see about few of the above-mentioned sensors in brief. More information about the sensors will be added subsequently. A list of projects using the above sensors is given at the end of the page.

Temperature Sensor

One of the most common and most popular sensors is the Temperature Sensor. A Temperature Sensor, as the name suggests, senses the temperature i.e., it measures the changes in the temperature.

There are different types of Temperature Sensors like Temperature Sensor ICs (like LM35, DS18B20), Thermistors, Thermocouples, RTD (Resistive Temperature Devices), etc.

Temperature Sensors can be analog or digital. In an Analog Temperature Sensor, the changes in the Temperature correspond to change in its physical property like resistance or voltage. LM35 is a classic Analog Temperature Sensor.

Coming to the Digital Temperature Sensor, the output is a discrete digital value (usually, some numerical data after converting analog value to digital value). DS18B20 is a simple Digital Temperature Sensor.

Temperature Sensors are used everywhere like computers, mobile phones, automobiles, air conditioning systems, industries etc.

A simple project using LM35 (Celsius Scale Temperature Sensor) is implemented in this project: TEMPERATURE CONTROLLED SYSTEM.

Proximity Sensors

A Proximity Sensor is a non-contact type sensor that detects the presence of an object. Proximity Sensors can be implemented using different techniques like Optical (like Infrared or Laser), Sound (Ultrasonic), Magnetic (Hall Effect), Capacitive, etc.

Some of the applications of Proximity Sensors are Mobile Phones, Cars (Parking Sensors), industries (object alignment), Ground Proximity in Aircrafts, etc.

Proximity Sensor in Reverse Parking is implemented in this Project: REVERSE PARKING SENSOR CIRCUIT.

Infrared Sensor (IR Sensor)

IR Sensors or Infrared Sensor are light based sensor that are used in various applications like Proximity and Object Detection. IR Sensors are used as proximity sensors in almost all mobile phones.

There are two types of Infrared or IR Sensors: Transmissive Type and Reflective Type. In Transmissive Type IR Sensor, the IR Transmitter (usually an IR LED) and the IR Detector (usually a Photo Diode) are positioned facing each other so that when an object passes between them, the sensor detects the object.

The other type of IR Sensor is a Reflective Type IR Sensor. In this, the transmitter and the detector are positioned adjacent to each other facing the object. When an object comes in front of the sensor, the infrared light from the IR Transmitter is reflected from the object and is detected by the IR Receiver and thus the sensor detects the object.

Different applications where IR Sensor is implemented are Mobile Phones, Robots, Industrial assembly, automobiles etc.

A small project, where IR Sensors are used to turn on street lights: STREET LIGHTS USING IR SENSORS.

Ultrasonic Sensor

An Ultrasonic Sensor is a non-contact type device that can be used to measure distance as well as velocity of an object. An Ultrasonic Sensor works based on the properties of the sound waves with frequency greater than that of the human audible range.

Using the time of flight of the sound wave, an Ultrasonic Sensor can measure the distance of the object (similar to SONAR). The Doppler Shift property of the sound wave is used to measure the velocity of an object.

Arduino based Range Finder is a simple project using Ultrasonic Sensor: PORTABLE ULTRASONIC RANGE METER.

Light Sensor

Sometimes also known as Photo Sensors, Light Sensors are one of the important sensors. A simple Light Sensor available today is the Light Dependent Resistor or LDR. The property of LDR is that its resistance is inversely proportional to the intensity of the ambient light i.e., when the intensity of light increases, its resistance decreases and vise-versa.

By using LDR is a circuit, we can calibrate the changes in its resistance to measure the intensity of Light. There are two other Light Sensors (or Photo Sensors) which are often used in complex electronic system design. They are Photo Diode and Photo Transistor. All these are Analog Sensors.

There are also Digital Light Sensors like BH1750, TSL2561, etc., which can calculate intensity of light and provide a digital equivalent value.

Check out this simple LIGHT DETECTOR USING LDR project.

Smoke and Gas Sensors

One of the very useful sensors in safety related applications are Smoke and Gas Sensors. Almost all offices and industries are equipped with several smoke detectors, which detect any smoke (due to fire) and sound an alarm.

Gas Sensors are more common in laboratories, large scale kitchens and industries. They can detect different gases like LPG, Propane, Butane, Methane (CH4), etc.

Now-a-days, smoke sensors (which often can detect smoke as well gas) are also installed in most homes as a safety measure.

The “MQ” series of sensors are a bunch of cheap sensors for detecting CO, CO2, CH4, Alcohol, Propane, Butane, LPG etc. You can use these sensors to build your own Smoke Sensor Application.

Check out this SMOKE DETECTOR ALARM CIRCUIT without using Arduino.

Alcohol Sensor

As the name suggests, an Alcohol Sensor detects alcohol. Usually, alcohol sensors are used in breathalyzer devices, which determine whether a person is drunk or not. Law enforcement personnel uses breathalyzers to catch drunk-and-drive culprits.

A simple tutorial on HOW TO MAKE ALCOHOL BREATHALYZER CIRCUIT?

Touch Sensor

We do not give much importance to touch sensors but they became an integral part of our life. Whether you know or not, all touch screen devices (Mobile Phones, Tablets, Laptops, etc.) have touch sensors in them. Another common application of touch sensor is trackpads in our laptops.

Touch Sensors, as the name suggests, detect touch of a finger or a stylus. Often touch sensors are classified into Resistive and Capacitive type. Almost all modern touch sensors are of Capacitive Types as they are more accurate and have better signal to noise ratio.

If you want to build an application with Touch Sensor, then there are low-cost modules available and using those touch sensors, you can build TOUCH DIMMER SWITCH CIRCUIT USING ARDUINO.

Color Sensor

A Color Sensor is an useful device in building color sensing applications in the field of image processing, color identification, industrial object tracking etc. The TCS3200 is a simple Color Sensor, which can detect any color and output a square wave proportional to the wavelength of the detected color.

If you are interested in building a Color Sensor Application, checkout this ARDUINO BASED COLOR DETECTOR project.

Humidity Sensor

If you see Weather Monitoring Systems, they often provide temperature as well as humidity data. So, measuring humidity is an important task in many applications and Humidity Sensors help us in achieving this.

Often all humidity sensors measure relative humidity (a ratio of water content in air to maximum potential of air to hold water). Since relative humidity is dependent on temperature of air, almost all Humidity Sensors can also measure Temperature.

Humidity Sensors are classified into Capacitive Type, Resistive Type and Thermal Conductive Type. DHT11 and DHT22 are two of the frequently used Humidity Sensors in DIY Community (the former is a resistive type while the latter is capacitive type).

Checkout this tutorial with DHT11 HUMIDITY SENSOR ON ARDUINO.

Tilt Sensor

Often used to detect inclination or orientation, Tilt Sensors are one of the simplest and inexpensive sensors out there. Previously, tilt sensors are made up of Mercury (and hence they are sometimes called as Mercury Switches) but most modern tilt sensors contain a roller ball.

A simple Arduino based title switch using tilt sensor is implemented here HOW TO MAKE A TILT SENSOR WITH ARDUINO?

In this article, we have seen about What is a Sensor, what are the classification of sensors and Different Types of Sensors along with their practical applications. In the future, I will update this article with more sensors and their applications.

Actuator:

An actuator is a machine part that initiates movements by receiving feedback from a control signal. Once it has power, the actuator creates specific motions depending on the purpose of the machine.

What Are Some Devices with Actuators?

Machines and systems have featured actuators since their popularization back in World War II. The most well-known examples of actuators include:

- Electric motors: Any part of a piece of equipment or appliance that translates electrical energy into motion, such as those found in ventilation fans, blenders, or refrigerators, contains at least one actuator. Electric cars also use actuators.

- Stepper motors: These actuators are best known for receiving digital pulses and converting them into mechanical motion. Stepper motors are often seen in robots, smart tools, or automated cutting equipment.

- Hydraulic cylinders: These are linear-motion devices that operate using a tube, piston, and rod. Many vehicles operate using hydraulic motion, such as bulldozers, backhoes, or excavators.

Types of Actuators:

Actuators can be classified by the motion they produce and the power source they use.

Motion

Actuators can create two main types of motion: linear and rotary.

Linear Actuators

Implied by their name, linear actuators are devices that produce movement within a straight path. They can either be mechanical or electrical and are mostly seen in hydraulic or pneumatic devices. Any machine, equipment, or gadget that requires some form of straight motion typically has a linear actuator.

In a simple linear actuator, there is a nut, cover, and a sliding tube. The sliding tube provides the space for the motion, whereas the nut and cover provide the interlocking movement that keeps the actuator in a straight path. Other complex linear actuators will have additional parts, but the system mentioned above is the foundation for straight movement.

Rotary Actuators

In contrast to linear actuators, rotary actuators create a circular motion. From the term “rotary,” most machines use these rotating parts to complete a turning movement. They are often used in conjunction with a linear actuator if a machine requires moving forward, backward, up, or down.

Many rotary actuators are electrically powered, but some are powered using a hydraulic or pneumatic system. You can find rotary actuators in windshield wipers, electric fans, or manufacturing machines that transport goods from one area to another.

Source of Energy

To further distinguish different types of actuators, we can also sort them according to the power source or system they use to move. Below are the most common actuators according to energy source:

Hydraulic Actuators

Hydraulic actuators operate by the use of a fluid-filled cylinder with a piston suspended at the center. Commonly, hydraulic actuators produce linear movements, and a spring is attached to one end as a part of the return motion. These actuators are widely seen in exercise equipment such as steppers or car transport carriers.

Pneumatic Actuators

Pneumatic actuators are one of the most reliable options for machine motion. They use pressurized gases to create mechanical movement. Many companies prefer pneumatic-powered actuators because they can make very precise motions, especially when starting and stopping a machine.

Examples of equipment that uses pneumatic actuators include:

- Bus brakes
- Exercise machines
- Vane motors
- Pressure sensors
- Pneumatic mailing systems

Electric Actuators

Electric actuators, as you may have guessed, require electricity to work. Well-known examples include electric cars, manufacturing machinery, and robotics equipment. Similar to pneumatic actuators, they also create precise motion as the flow of electrical power is constant.

The different types of electrical actuators include:

- Electromechanical actuators: These actuators convert electric signals into rotary or linear movements and may even be capable of a combination of both.

- Electrohydraulic actuators: This type of actuator is also powered electrically but gives movement to a hydraulic accumulator. The accumulator then provides the force for movement, usually seen in heavy industrial equipment.

Thermal and Magnetic Actuators

Thermal and magnetic actuators usually consist of shape memory alloys that can be heated to produce movement. The motion of thermal or magnetic actuators often comes from the Joule effect, but it can also occur when a coil is placed in a static magnetic field. The magnetic field causes constant motion called the Laplace-Lorentz force. Most thermal and magnetic actuators can produce a wide and powerful range of motion while remaining lightweight.

Mechanical Actuators

Some actuators are mostly mechanical, such as pulleys or rack and pinion systems. Another mechanical force is applied, such as pulling or pushing, and the actuator will leverage that single movement to produce the desired results. For instance, turning a single gear on a set of rack and pinions can mobilize an object from point A to point B. The tugging movement applied on the pulley can bring the other side upwards or towards the desired location.

Supercoiled Polymer Actuators

Supercoiled polymer actuators are a relatively new addition to the different types of actuators. They are used in robotics and prosthetic limbs as they can replicate the motion of human muscle via a coil that contracts and expands when heated or cooled.

How to Select the Right Actuator

Understanding the different types of actuators is a crucial step in making the best selection for your equipment. Since each kind has its unique purpose and energy requirements, we'll go over factors that will help you arrive at the best decision.

Power Source Availability

The first thing you have to consider is the compatibility of your power source. If you own an industrial site with an electrical source, perhaps the best choice—and the option with the most selections—would be electric actuators. If there are no electrical sources in the area, or you want a piece of fully functional equipment without electricity, you can opt for pneumatic or hydraulic types.

Required Movement

Another important factor when choosing an actuator is the range of movement that you need for your equipment. Is it linear, rotary, or an integration of both? Custom-made actuators can combine or chronologically create these motions to help you concretize the final equipment.

Precision

Some actuators are more precise than others. For example, air brakes are created through pneumatic actuators because air pressure is known to be efficient in the start and stop movements. Other actuators have a larger margin of movement variations, such as those operated through hydraulics.

Any industry that requires a high level of precision for safety and success of operation should consider actuator types that have specific movements.

Safety and Environmental Concerns

Safety is another factor to consider when choosing an actuator for your equipment. Electrical or thermal actuators should be used with caution in areas with extreme temperatures or conducting hazards. For example, operating electrical actuators close to a water body without sealing or other safety measures may create an occupational hazard.

If your company is also committed to a reduced carbon footprint, you'll need to note each actuators' environmental impact. Typically, electrical actuators have little to no carbon footprint.

Official Guidelines

There are also specific guidelines to follow for industrial actuators in certain areas. For example, locations with a high presence of combustible gases should adhere to the requirements imposed by the National Electrical Manufacturers Association (NEMA).

Maintaining Your Actuator

All equipment requires maintenance. Maintaining your actuators will help prevent major shutdowns, hazards, or loss of productivity. Here are some general tips to keep your actuators in top shape.

- Regular inspection: Performing routine visual equipment checks will identify early signs of actuator issues. A mechanic with a keen eye is necessary to inspect for wear and tear.

- Replenish and replace: Hydraulic actuators sometimes need cylinder fluid replenishment. Always double-check for leaks and signs of low hydraulic fluid levels. Replace loose or damaged nuts, bolts, coils, or screws in your actuator parts as well.

- Measure performance data: In some cases, actuators won't show external signs of a problem, but you can trace issues through performance. Automated graphs and output computation may be necessary if you want to catch deeper issues.

IOT Development board:

A development board is a printed circuit board with circuitry and hardware designed to assist experimentation with a certain microcontroller.

Well, to understand this assume you have a microcontroller that is capable of doing many cool things but to be able to use that you need to first set up a group of circuitry and hardware on your breadboard every time. I know this is kind of frustrating to our smart engineers, especially when there are circuits that are going to be the same every time, like power circuits. At the same time, many hardware circuits are quite helpful in testing and debugging like pushbuttons that is better to be prototyped.

In short, To make the engineers' life easier and more efficient with prototyping development boards are constructed.

Why not have a quick look at the typical components of a Development board. Here they are:

- Power circuit– Generally set up to run off of a 9V power supply
- Programming interface– Let you program the microcontroller from a computer
- Basic input – Usually buttons
- Basic output– Usually LEDs

- I/O pins– Used for motors, temperature sensors, LCD screens, etc.

Key Features That Must be Included in Your Development Board

Any development board you consider for an IoT project must include a few important features. Those are:

Processing power. This could be in the form of a CPU, microcontroller, FPGA, or other CPLD. A microcontroller comes in handy for programming your device as many manufacturers provide the IDE you need.

Wireless capabilities. This feature provides wireless communication without including an external transceiver module. Some of the common protocols include Bluetooth, Zigbee, WiFi, and others.

Scalability. This particular feature allows one to add more functionality to the development board? You may verify if the board communicates via GPIO, UART, SPI, or some other protocol; As this will determine how the board interacts with other devices.

Memory. Board memory is important. To store much data, you need built-in Flash memory. A decent board allows connecting a MiniSD or MicroSD card to enhance data storage.

Have An IoT App Idea In Mind? Get A Free Consultation & Wire-Frames Done From Our Experts!

IoT boards are useful hardware structures that we use to prototype a new IoT project. As we discussed above, the custom hardware results in expensive to design and manufacture, and development boards comes to rescue to avoid that.

There are several IoT prototyping boards in the market with different specifications. And here we will cover top development boards for IoT projects.

All the below mentioned IoT boards will fall into any of the below categories:

1. Microcontroller-based boards
2. System on Chip (SOC) boards
3. Single-board Computers (SBC)

Let’s get straight to the most popular IoT Development Boards:

1. Raspberry Pi
2. Omega 2
3. Particle Photon
4. Beagle bone –
5. Jetson Nano
6. ESP 32
7. Banana Pi

8. Arduino Nano 33 IoT
9. Tessel 2
10. i.MX 8

Raspberry Pi Development kit:

The raspberry pi Development Board is a small credit card size computer. That works on Linux based operating systems and is good for embedded projects. Raspberry boards can be easily plugged in to your monitor, computer or TV. It uses a standard keyboard and mouse. Even amateur users depend on it for configuring their digital media systems and surveillance cameras.

Features :

- Processor: 1.2GHz, 64-bit quad-core ARMv8 CPU
- 802.11n Wireless LAN
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Combined 3.5mm audio jack and composite video
- Camera interface (CSI)
- Display interface (DSI)
- Micro SD card slot
- videoCore IV 3D graphics core

2. Omega 2

Omega 2 is one of Onion's Linux-based WiFi development boards that allow makers of all skill levels to build connected hardware. This highly integrated board comes with a powerful processor and flexible GPIOs. The Platform lets you prototype hardware devices using familiar tools like Git, npm, pip, as well as high-level programming languages like Python, Javascript, and PHP.

Features :

- Linux Operating System, powerful processor, and flexible GPIOs.
- Compact size that easily fits into any project design.
- Modular design for a vast range of flexibility.

- Arduino compatible.
- Integrated Wi-Fi;
- Connectivity is expandable with 2G, 3G, Ethernet, Bluetooth®, Bluetooth Low Energy (BLE), GPS.
- U.FL Connector for external Wi-Fi antenna attachment.
- FCC and CE Certified.

3. Particle Photon

Particle Photon Board consists of an STM32 microcontroller, Wi-Fi, Switches, and LEDs. Simple to use, powerful, and connected to the cloud. Powered by a Cypress Wi-Fi chip alongside a powerful STM32 ARM Cortex M3 microcontroller, it is ideal for prototyping IoT projects.

Features :

- Processor: STM32F205 120Mhz ARM Cortex M3
- Real-time operating system (Free RTOS)
- Memory: 1MB flash, 128KB RAM
- Open source design
- On-board Wi-Fi module
- On-board RGB status LED.
- 18 Mixed-signal GPIO and advanced peripherals
- Soft AP setup
- B802.11b/g/n Wi-Fi
- roadcom BCM43362 Wi-Fi chip

4. Beagle Bone

The Beagle bone is a low power open-source single-board computer produced by Texas instruments. The board can boot Linux in under 10 seconds also you can start developing in less than 5 minutes with just a single USB cable.

It is a computer installed inside of a larger electronics project. The beagle board carries two rows of GPIO (general purpose Input/Output) pins mounted along each side of the board. That allow it to communicate with a wide range of servos, sensors, outputs and other hardware, making it act as the brain of large & complex projects.

Its capabilities can be extended using plug-in boards referred to as “capes”. that are easily available for LCD, motor control, VGA, prototyping, battery power, and other functionalities.

Features :

- DDR memory: 512 MB
- Ability to run Ruby, Python, and INO Sketches directly in the Cloud9 IDE,
- Ethernet: On-chip 10/100 Ethernet
- JTAG: Optional
- Memory: 4GB eMMC memory
- Power Options: Via USB or 5V DC input
- Price (USD) Per Unit: $55.00 (Suggested Retail Price)
- Processor: 1GHz AM3359 Sitara ARM Cortex-A8

5. Jetson Nano

Jetson Nano is a power-efficient and low-cost development board. Provides total performance to run modern AI workloads in a small form factor. Additionally, It has the ability for heavy workload applications like image classification, object detection, segmentation, and speech processing. It is capable to run multiple neural network apps at the same time.

Features:

- GPU: 128-core NVIDIA Maxwell™ architecture-based GPU.
- CPU: Quad-core ARM® A57.
- Video: 4K @ 30 fps
- Camera: 1/3” AR0330 CMOS Image sensor with 2.2 µm pixel.
- Memory: 4 GB 64-bit LPDDR4; 25.6 gigabytes/second.
- Connectivity: Gigabit Ethernet.
- OS Support: Linux for Tegra®.

ESP 32

ESP32 is a dual core low-footprint system development board powered by the latest ESP-WROOM-32 module that can be easily placed into a solderless breadboard. It has a pre-integrated antenna, power amplifier, low-noise amplifiers, filters, and power management module. Because of this, it’s easy to build and test circuits as well as making projects related to IoT integrating with the cloud platform.

Features :

- 2.4 GHz dual-mode Wi-Fi.
- Programmable with Arduino open-source IDE.
- 8 independent LED.

- Bluetooth chips by TSMC.
- 40nm low power technology, power, and RF.
- Easily embedded with other products.
- Strong function with support LWIP protocol.
- Supports three modes: AP, STA, and AP+STA.
- Supporting the Lua program, easily to develop.

7. Banana Pi

Banana Pi is a line of low-cost credit card-sized single-board computers(SBC). IT is a router-based development board, which efficiently runs on various open-source operating systems including OpenWRT and Android, Lubuntu, Ubuntu, Debian, and Raspbian. Well, the hardware design of banana pi was influenced by the Raspberry Pi and it is compatible with Raspberry Pi boards.

Features :

- All winner A20 Dual-core 1.0 GHz CPU
- Mali-400 MP2 with Open GL ES 2.0/1.1.
- 1 GB DDR3 memory.
- 1x Gigabit LAN
- 1x SATA interface.
- 1X MIC
- 1x USB otg and 2x USB 2.0
- HDMI out
- Composite video out
- CSI camera interface
- DSI display interface
- 26 PIN GPIO

8. Arduino Nano 33 IoT

The Arduino Nano 33 IoT is a dual-processor device that is perfect for experimentation. It offers a practical and low-cost solution for inventors seeking to add Wi-Fi connectivity to their projects with minimal previous experience in networking. The board is compatible with the Arduino IoT Cloud, where you can create IoT applications in a few simple steps

Features :

- ARM Cortex-M0 32-bit SAMD21 processor

- 14 digital I/O pins and 8 analog input pins
- Support up to 12-bit ADC/PWM and 10-bit DAC resolutions.
- Can operate as a few different USB devices: (asynchronous serial, keyboard or mouse) also referred as HID, and USB MIDI.
- Can communicate via Synchronous serial communications.
- Inbuilt real-time clock module.

9. Tessel 2

It's a kind of System on Chipboards. With WIFI capabilities, it allows you to build scripts in Node.js. The board also provides you with a connected hardware prototyping system that can be used in multiple different applications. Loaded with on-board features including two 10-pin module ports to add sensors and other external hardware, a 10/100 supported ethernet port, 2 USB ports for camera peripherals and flash storage, and a microUSB connector for power and tethered programming.

Features :

- 2 USB ports (you can connect cameras or flash storage, for example)
- 10/100 ethernet port
- 802.11 b/g/n WiFi
- 580MHz Mediatek router-on-a-chip (you can turn your Tessel 2 into an access point!)
- 48MHz SAMD21 coprocessor (for making I/O faster)
- 64MB DDR2 RAM, 32MB of flash (lots of space for your programs and stuff)

10. i.MX 8

i.MX 8 boards offer low power, flexible memory options, a wide range of high-speed interfaces, as well as industry-leading audio and video capabilities. It also comes with a pre-installed boot image flashed on one eMMC memory.

With best-in-class computing power, superior graphics performance, and sophisticated security features, i.MX boards became the next-gen technology for industrial embedded systems.

Features :

- i.MX 8M Quad Applications Processor.
- 4x Arm Cortex-A53 @ 1.5GHz.
- NXP PMIC PF4210 power management.
- LPDDR4 x32 @3200MT w/4GB, eMMC 5.0 w/16GB, MicroSD, QSPI w/256Gb memory availability.
- HDMI 2.0a Type-A , MIPI-CSI Camera mini-SAS, MIPI-DSI Display mini-SAS camera connector.

- 10/100/1000 Ethernet, USB 3.0 Type-A & C, PCIe M.2 interface, and Infrared connector.
- Linux, Android, and FreeRTOS OS support.

So, these are the top development boards that may fit for your various project requirements. And if are overwhelmed with the options and need guidelines that may assist you in finding the right development board.

RFID (radio frequency identification):

RFID (radio frequency identification) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person.

How does RFID work?

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers -- fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

What are RFID tags and smart labels?

RFID tags are made up of an integrated circuit (IC), an antenna and a substrate. The part of an RFID tag that encodes identifying information is called the RFID inlay.

There are two main types of RFID tags:

- Active RFID. An active RFID tag has its own power source, often a battery.
- Passive RFID. A passive RFID tag receives its power from the reading antenna, whose electromagnetic wave induces a current in the RFID tag's antenna.

There are also semi-passive RFID tags, meaning a battery runs the circuitry while communication is powered by the RFID reader.

Low-power, embedded non-volatile memory plays an important role in every RFID system. RFID tags typically hold less than 2,000 KB of data, including a unique identifier/serial number. Tags can be read-only or read-write, where data can be added by the reader or existing data overwritten.

The read range for RFID tags varies based on factors including type of tag, type of reader, RFID frequency, and interference in the surrounding environment or from other RFID tags and readers. Active RFID tags have a longer read range than passive RFID tags due to the stronger power source.

smart labels are simple RFID tags. These labels have an RFID tag embedded into an adhesive label and feature a barcode. They can also be used by both RFID and barcode readers. Smart labels can be printed on-demand using desktop printers, where RFID tags require more advanced equipment.

ZEBRA TECHNOLOGIES

RFID readers can be fixed (left) or mobile (right).

What are the types of RFID systems?

There are three main types of RFID systems: low frequency (LF), high frequency (HF) and ultra-high frequency (UHF). Microwave RFID is also available. Frequencies vary greatly by country and region.

- Low-frequency RFID systems. These range from 30 KHzto 500 KHz, though the typical frequency is 125 KHz. LF RFID has short transmission ranges, generally anywhere from a few inches to less than six feet.
- High-frequency RFID system These range from 3 MHzto 30 MHz, with the typical HF frequency being 13.56 MHz. The standard range is anywhere from a few inches to several feet.
- UHF RFID systems. These range from 300 MHz to 960 MHz, with the typical frequency of 433 MHz and can generally be read from 25-plus feet away.
- Microwave RFID systems. These run at 2.45 Ghzand can be read from 30-plus feet away.

The frequency used will depend on the RFID application, with actual obtained distances sometimes varying from what is expected. For example, when the U.S. State Department announced it would issue electronic passports enabled with an RFID chip, it said the chips would only be able to be read from approximately 4 inches away. However, the State Department soon received evidence that RFID readers could skim the information from the RFID tags from much farther than 4 inches -- sometimes upward of 33 feet away.

If longer read ranges are needed, using tags with additional power can boost read ranges to 300-plus feet.

Applications of RFID:

RFID dates back to the 1940s; however, it was used more frequently in the 1970s. For a long time, the high cost of the tags and readers prohibited widespread commercial use. As hardware costs have decreased, RFID adoption has also increased.

Some common uses for RFID applications include:

- pet and livestock tracking
- inventory management
- asset tracking and equipment tracking
- inventory control
- cargo and supply chain logistics
- vehicle tracking
- customer service and loss control

- improved visibility and distribution in the supply chain
- access control in security situations
- shipping
- healthcare
- manufacturing
- retail sales
- tap-and-go credit card payments

Components of RFID Technology

RFID technology consists of four components such as RFID tags, antenna, RFID receiver (transceiver) and software.

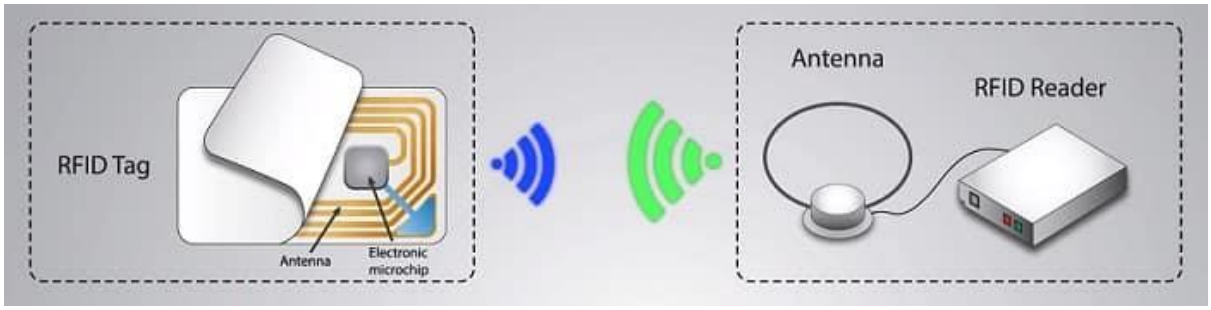


Image: Youtube

1. RFID Tag

RFID tags are small devices consists of an electronic microchip embedded inside and an antenna. The microchip has the unique identification number of the RFID tag.

Passive RFID tag does not have a power source; it will receive power from radio signals transmitted from the RFID receiver. These tags will operate when the reader is at the proximity of the tags (line of sight not required).

Antenna coil will act as power source and medium to transfer data to the reader.

Types of Tags

Passive Tags: Does not have a power source, uses power from the reader to operate.

Battery Assisted Passive Tags: Logic circuit chip uses battery power. Need RF signals from the reader to activate and function.

Active Tags: Uses a power source like battery, does not require power from source/reader.

2. Antenna

RFID antennas are designed to operate at a specific frequency for each applications in which it operates. These antennas are often mounted on the RFID reader and easily accessible for tags to tap on it.

In some handheld devices, antenna is often attached to the device. Size and shape of the antenna depends on the application and the operating frequency of the system.

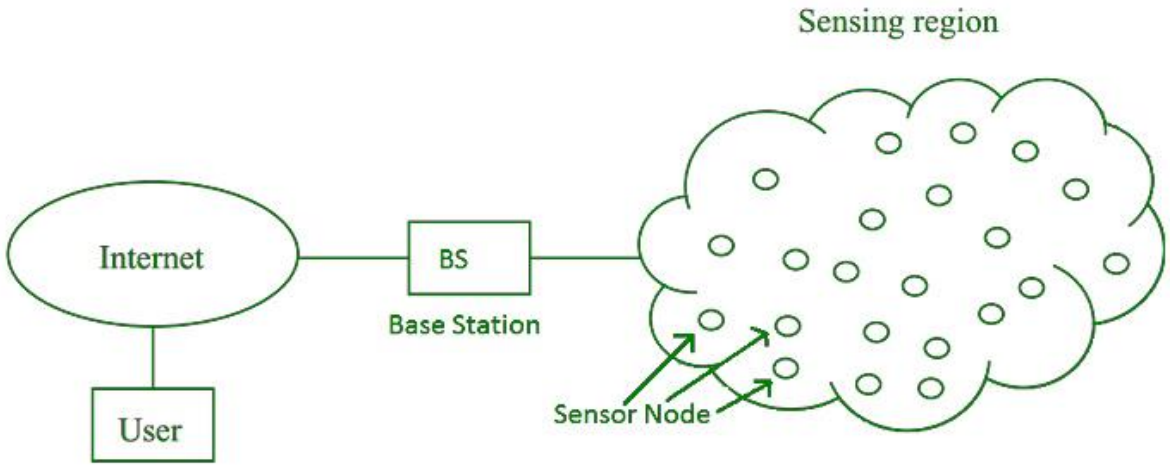
3. RFID Reader

RFID reader is one of the significant hardware component in the RFID system which read information from the RFID devices/tags and connected to the network to transfer the information to the database.

Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.
Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

Components of WSN:

1. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Connecting Nodes:

To fully unleash all the possibilities that the Internet of Things (IoT) concept enables, a very large number of devices – more than 20 billion by 2020 – will be connected to the cloud. By using cloud services to collect and process data, user experience and convenience when interacting with any particular product or system can be greatly enhanced. Directly connecting nodes to the cloud to a range of commercially available platforms – including IBM Watson, Amazon's AWS or Microsoft Azure – and selecting IP-native wired and wireless connectivity technology, help minimize the infrastructure required to access each node. At ST, we have developed a range of solutions including pre-integrated cloud connectivity protocols, provisioning and upgrade libraries as well as Software

Development Kits (SDK) to support architectures with nodes directly connected to Cloud to help developers create innovative connected devices and services.

Cellular Connected Nodes

Cellular is one of the long-range gateway-less wireless connectivity solutions for IoT, connecting devices to the cloud through telecom operator networks and infrastructure. Typical example applications using 2G, 3G, 4G (including LTE) and today's 5G

View application

Sigfox

Sigfox wireless connectivity employs a proprietary technology which uses the 868 MHz (Europe) and 902 MHz (US) frequencies in the Industrial, Scientific and Medical (ISM) radio band. It utilizes ultra-narrowband modulation to enable low-power wide-ar

View application

Wi-Fi Connected Nodes

Wi-Fi is a technology for wireless local area networking with devices based on the IEEE 802.11 standard and is a key technology within the IoT. Embedded developers can find here hardware and software development platforms to jumpstart their designs f

View application

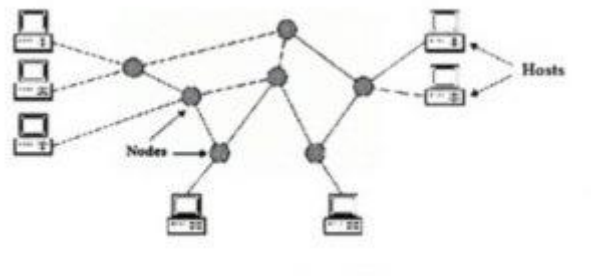
Networking Nodes:

In Data Communication Systems, a network is an interconnecting point to exchange information between various communication components connected by various communication network links. If two or more network devices are connected to each other to transfer and share information and resources within a geographical area, then it is called a network. For example, a computer network is formed with multiple computers connected to transmit, exchange, share, store data, and resources. It enables communication for entertainment, business, and research. The computer network is built by using various hardware network nodes like bridges, routers, hubs, switches, etc, and communicating links like optical fiber cables, coaxial cables, wireless networks (LAN, WAN), etc. This article gives an overview of network nodes and their types in a computer network.

What is a Node in a Computer Network?

A node within a computer network is defined as, a connecting point or redistributed point or communicating point or joint, or a transfer point where the data can be stored, received, transmitted, or created. A node can be either a computer or any device that involves receiving and sending the data inside the computer networks. It is simply called a network node. The link that connects the node of a network is known as a communication channel.

The network node is either a redistribution point or an endpoint that transmits the data with a recognizing, processing, and forwarding capability to other network nodes. To form a network connection for data transmission, 2 or multiple network nodes are needed. It depends on the type of network and the referred protocol layer.



Network Nodes

To receive access each node requires an IP address for identification. Examples of network nodes include printers, computers, modems, bridges, switches, etc. A network node is any device in the network that can transmit, process, recognize and store information to other networks.

If the node is referred to as data communication equipment, then it forms a connection for modems, hubs, bridges, switches, etc. If the network node is data terminal equipment, then it acts as an endpoint for connecting printers, handsets, telephones, computers, etc.

Any device that is connected to the network contains a unique IP address or logical address, which is referred to as a node. The device manufacturers assigned a MAC address for every node on the network to a NIC (network interface controller) for data transmission and communication. The measure of several connections made by a network node with other nodes gives the degree of connectivity.

Types of Network Nodes

The network nodes concept adopted packet switching theory to transmit and receive the data through different routes in a distributed network. There are different types of network nodes based on the application and function.

End Nodes

These are referred to as the initial point or an endpoint for communication. Examples of end nodes are computers, security, cameras, printers, and many more.

Intermediary Nodes

The nodes are located in between the initial (starting) point or an endpoint of the end nodes of the computer network. Examples of intermediary nodes are bridges, routers, switches, cell towers, etc.

Data Communications

The network nodes are the physical devices that are located in between DTE (data terminal equipment) and data communication circuits. Bridges, switches, hubs, and modems are included to execute the conversion of signals, line clocks, and coding. In data communications, devices like digital telephones, host computers, printers, routers, servers act as data terminal equipment.

Internet and intranet network nodes: these types of nodes are nothing but host computers, which are identified by an IP address. Some of the data link layer devices and WLAN access points don’t contain any IP address and they are referred to as physical network nodes or LAN nodes.

LAN and WAN network nodes: these types of network nodes are the physical devices that are involved in performing particular functions and also every node contains a specific MAC address for NIC (network interface card). The examples are modems, access points of WLAN, and PCs. If the device is offline, then there would be a loss of function of the node.

Telecommunication Nodes

These types of nodes in fixed telephone networks might be private or public to exchange the information or a computer that provides intelligent network service. While in cellular networks, include base station controllers to control multiple base stations. Since the cellular network base stations are not referred to as nodes.

Cable TV Network Nodes

These types of nodes are related to fiber optic cables, which connect businesses, homes distributed by common fiber optic receivers within a specified geographical location. The fiber optic node in cable systems determines the number of businesses and homes are connected by a particular fiber node.

Distributed Network Nodes

These types of nodes are servers, clients, and peers. In distributed networks, some virtual nodes are used to maintain data transparency.

Example of Network Nodes

The best examples of network nodes are discussed below.

Switches

The network devices that operate at the data link layer of the OSI model to forward, send, and receive the data frames/packets over the entire network are called switches. A switch is a multiple port device, in which multiple computers or network devices can be plugged in. It performs error checking and examines the destination address when the data frame arrives at any port or node of the network and forwards it with efficiency to the selected port or node.

A switch can divide the Collision domain of hosts and the broadcast domain remains the same. It supports all modes of communications such as unicast, multicast, and broadcast. It uses packet-switching technology and utilizes the MAC address to send and receive the data frames from source to destination.

The mode of transmission is full-duplex and communication is bidirectional. The switches are active devices with network management capability. Error checking is done before forwarding of data. There are 4 types of switches.

- Unmanaged switches: most widely used in home networks
- Manages switches: used complex and large networks of various organizations.
- LAN switches: connects internal LAN of a business or organization
- PoE switches (power over Ethernet switches): can receive power and data frame over the same line on the Ethernet network.

Bridges

The network devices that operate at the data link layer of the OSI model and connect two or multiple LANs to form a single larger Local Area Network (LAN) are called bridges. The process of aggregating the local area networks is known as bridging the network. It connects two or multiple segments or components of the same local area network.

They are referred to as layer 2 switches. They are usually called repeaters, which can filter the data by reading the MAC address of destination and source. They are 2 port devices, that contain a single input and output port. It can interconnect two local area networks, which are operating on the same protocol.

When multiple LANs are joined together to form a single LAN, the capacity of the network will increase. The data frame is passed to the node and then discarded, if it contains a destination MAC address in the same network. The data frame will be forwarded towards the network if it contains the destination MAC address in the connected network. If the MAC address is not available, then the bridge broadcasts the data frames to every network node. There are 2 types of bridges. They are,

- Transparent bridge: unaware of the existence of a bridge in the network and performs two processes like bridge forward and bridge learn.
- Source routing bridge: source station and the data from specifies the route to be followed.

WSN and IOT:

Wireless Sensor Networks (WSN) and the Internet of Things (IoT)

- Wireless Sensor Networks (WSN) are used to monitor and collect data from physical or environmental conditions.
    - Whereas the Internet of Things is used to connect devices and objects to the internet so they can communicate with each other and exchange data.
- Wireless sensor networks typically consist of a large number of small, low-power sensors that wirelessly transmit data to a central base station
    - whereas the Internet of Things (IoT) typically consists of a smaller number of devices that are connected to the internet via wired or wireless connections.
- Wireless sensor networks are often used for monitoring purposes in difficult or dangerous environments.

    - whereas the Internet of Things is used to connect a variety of devices and objects in more everyday settings.
- Wireless sensor networks are often designed to operate in specific environments for a specific purpose.
    - whereas the Internet of Things is designed to be more general and versatile.
- Wireless sensor networks often use proprietary protocols and technologies
    - whereas the Internet of Things relies on standard protocols such as TCP/IP.
- Wireless sensor networks are typically deployed and operated by a single organization.
    - whereas the Internet of Things is more decentralized, with a variety of organizations and individuals involved.
- Wireless sensor networks are often closed systems, with data being collected and used by the deploying organization
    - whereas the Internet of Things is more open, with data being shared and used by a variety of organizations and individuals.
- Wireless sensor networks are typically static, with sensors being deployed in a specific location and remaining in that location
    - whereas the Internet of Things is more dynamic, with devices and objects being moved around and connected to different networks.
- Wireless sensor networks are typically used for data collection and monitoring.
    - whereas the Internet of Things is used for a variety of purposes, including data collection, monitoring, control, and communication.
- The wireless sensor network market is still emerging
    - whereas the Internet of Things market is more mature.

I hope, this article would help you to know about the 10 main differences between WSN and the IoT.

The Internet of things (IoT)

1.
    1. The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.

2. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

All sensor data is further processed and analyzed in the data analyzing

Short Answer Questions:

1.What is Sensor?

2.What is Raspberripi Development kit?

3.Explain about RFID?

4.Explain about WSN(Wireless sensor networks)?

Long Answer Questions: MCA 402C: Internet of Things

UNIT I

Fundamentals of IoT: Introduction, Definitions & Characteristics of IoT, IoT Architectures, Physical & Logical Design of IoT, Enabling Technologies in IoT, History of IoT, About Things in IoT, The Identifiers in IoT, About the Internet in IoT, IoT frameworks, IoT and M2M.

UNIT II

Sensors Networks : Definition, Types of Sensors, Types of Actuators, Examples and Working, IoT Development Boards: Arduino IDE and Board Types, RaspberriPi Development Kit, RFID Principles and components, Wireless Sensor Networks: History and Context, The node,

Connecting nodes, Networking Nodes, WSN and IoT.

UNIT III

Wireless Technologies For Iot: WPAN Technologies for IoT: IEEE 802.15.4, Zigbee, HART, NFC, Z-Wave, BLE, Bacnet, Modbus. IP Based Protocols For IoT: IPv6, 6LowPAN, RPL, REST, AMPQ, CoAP, MQTT.

Edge connectivity and protocols

UNI IV

Data Handling& Analytics: Introduction, Bigdata, Types of data, Characteristics of Big data, Data handling Technologies, Flow of data, Data acquisition, Data Storage, Introduction to Hadoop. Introduction to data Analytics, Types of Data analytics, Local Analytics, Cloud analytics and applications, Edge/Fog Computing

UNIT V

Applications of IoT: Home Automation, Smart Cities, Energy, Retail Management, Logistics, Agriculture, Health and Lifestyle, Industrial IoT, Legal challenges, IoT design Ethics, IoT in Environmental Protection.

Text Books:

1. Olivier Hersent, David Boswarthick, and Omar Elloumi, — “The Internet of Things: Key Applications and Protocols”, WileyPublications

2. Vijay Madisetti and ArshdeepBahga, — “Internet of Things (A Hands-on-Approach)”, 1st Edition, VPT, 2014.

Reference Books

1. Daniel Minoli, — “Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications”, ISBN: 978-1-118-47347-4, Willy Publications

2. Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRC Press

UNIT-I

Introduction to IOT:

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.[1][2][3][4][5] Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network,[6] and be individually addressable.[7][8]

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, as well as machine learning.[9] Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and buildin g automation), independently and collectively enable the Internet of things.[10] In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with

that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.[11]

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks.[12]

History[edit]

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first ARPANET-connected appliance,[13] able to report its inventory and whether newly loaded drinks were cold or not.[14] Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IOT.[15][16] In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories".[17] Between 1993 and 1997, several companies proposed solutions

like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.[18]

The concept of the "Internet of things" and the term itself, first appeared in a speech by Peter T. Lewis, to the Congressional Black Caucus Foundation 15th Annual Legislative Weekend in Washington, D.C., published in September 1985.[19] According to Lewis, "The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices."

The term "Internet of things" was coined independently by Kevin Ashton of Procter & Gamble, later of MIT's Auto-ID Center, in 1999,[20] though he prefers the phrase "Internet *for* things".[21] At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things,[22] which would allow computers to manage all individual things.[23][24][25] The main theme of the Internet of things is to embed short-range mobile transceivers in various gadgets and daily necessities to enable new forms

of communication between people and things, and between things themselves.[26]

In 2004 Cornelius "Pete" Peterson, CEO of NetSilicon, predicted that, "The next era of information technology will be dominated by [IoT] devices, and networked devices will ultimately gain in popularity and significance to the extent that they will far exceed the number of networked computers and workstations." Peterson believed that medical devices and industrial controls would become dominant applications of the technology.[27]

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.[28]

characteristics of internet of IoT:

According to the definition of IoT, It is the way to interconnection with the help of the internet devices that can be embedded to implement the functionality in everyday objects

by enabling them to send and receive data. Today data is everything and everywhere. Hence, IoT can also be defined as the analysis of the data generate a meaning action, triggered subsequently after the interchange of data. IoT can be used to build applications for agriculture, assets tracking, energy sector, safety and security sector, defence, embedded applications, education, waste management, healthcare product, telemedicine, smart city applications, etc.

Characteristics of the Internet of Things :

There are the following characteristics of IoT as follows. Let’s discuss it one by one.

1. Connectivity –

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.

2. Intelligence and Identity –

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3. Scalability –

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4. Dynamic and Self-Adapting (Complexity) –

IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night).

5. Architecture –

IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ` products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6. Safety –

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

7. Self Configuring – This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Architecture of IoT:

Internet of Things (IoT) technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

So. here in this article we will discuss basic fundamental architecture of IoT i.e., 4 Stage IoT architecture.

4 Stage IoT architecture

So, from the above image it is clear that there is 4 layers are present that can be divided as follows: Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

1. Sensing Layer –

Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.

2. Network Layer –

Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc). Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also some times decision making based on inputted data and data management services, etc.

3. Data processing Layer –

This is processing unit of IoT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored and managed and further actions are also

prepared. So here Edge IT or edge analytics comes into picture.

4. Application Layer –

This is last layer of 4 stages of IoT architecture. Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

Physical and Logical Design of IoT:

In this article we discuss Physical and Logical Design of IoT. Physical Design of IoT system refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Communication established between things and cloud based server over the Internet by various IoT protocols. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation.

Physical Design of IoT

Physical Design of IoT refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. IoT Protocols helps Communication established between things and cloud based server over the Internet.

Things

Basically Things refers to IoT Devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Things are is main part of IoT Application. IoT Devices can be various type, Sensing Devices, Smart Watches, Smart Electronics appliances, Wearable Sensors, Automobiles, and industrial machines. These devices generate data in some forms or the other which when processed by data analytics systems leads to useful information to guide further actions locally or remotely.

For example, Temperature data generated by a Temperature Sensor in Home or other place, when processed can help in determining temperature and take action according to users.

Above picture, shows a generic block diagram of IoT device. It may consist of several interfaces for connections to other devices. IoT Device has

I/O interface for Sensors, Similarly for Internet connectivity, Storage and Audio/Video.

IoT Device collect data from on-board or attached Sensors and Sensed data communicated either to other device or Cloud based sever. Today many cloud servers available for especially IoT System. These Platfrom known as IoT Platform. Actually these cloud especially design for IoT purpose. So here we can analysis and processed data easily.

How it works ? For example if relay switch connected to an IoT device can turn On/Off an appliance on the commands sent to the IoT device over the Internet.

IoT Protocols

IoT protcols help to establish Communication between IoT Device (Node Device) and Cloud based Server over the Internet. It help to sent commands to IoT Device and received data from an IoT device over the Internet. An image is given below. By this image you can understand which protocols used.

_

Link Layer

Link layer protocols determine how data is physically sent over the network's physical layer or medium (Coxial calbe or other or radio wave). Link Layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (eg. coxial cable).

Here we explain some Link Layer Protocols:

802.3 – Ethernet : Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

WiFi : IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication

in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

Wi-Max : The standard for WiMAX technology is a standard for Wireless Metropolitan Area Networks (WMANs) that has been developed by working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access. Initially 802.16a was developed and launched, but now it has been further refined. 802.16d or 802.16-2004 was released as a refined version of the 802.16a standard aimed at fixed applications. Another version of the standard, 802.16e or 802.16-2005 was also released and aimed at the roaming and mobile markets.

LR-WPAN : A collection of standards for Low-rate wireless personal area network. The IEEE's 802.15.4 standard defines the MAC and PHY layer used by, but not limited to, networking specifications such as Zigbee®, 6LoWPAN, Thread, WiSUN and MiWi™ protocols. The standards provide low-cost and low-speed communication for power constrained devices.

2G/3G/4G- Mobile Communication : These are different types of telecommunication generations. IoT devices are based on these standards can communicate over the celluer networks.

Network Layer

Responsible for sending of IP datagrams from the source network to the destination network. Network layer performs the host addressing and packet routing. We used IPv4 and IPv6 for Host identification. IPv4 and IPv6 are hierarchical IP addrssing schemes.

IPv4 :

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s.

IPv6 : Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. In December 1998, IPv6 became a Draft Standard for the IETF, who subsequently ratified it as an Internet Standard on 14 July 2017. IPv6 uses a 128-bit address, theoretically allowing 2128, or approximately 3.4×1038 addresses. Source – wikipedia

6LoWPAN : 6LoWPAN is an acronym of IPv6 over Low-Power Wireless Personal Area Networks.6LoWPAN is the name of a concluded working group in the Internet area of the IETF. 6LoWPAN is a somewhat contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi.

Transport Layer

This layer provides functions such as error control, segmentation, flow control and congestion control. So this layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP : TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. The Internet Engineering Task Force (IETF) defines TCP in the Request for Comment (RFC) standards document number 793.

UDP : User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

Application Layer

Application layer protocols define how the applications interface with the lower layer protocols to send over ther network.

HTTP : Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests. Though often based on a TCP/IP layer, it can be used on any reliable transport layer, that is, a protocol that doesn’t lose messages silently like UDP does. RUDP — the reliable update of UDP — is a suitable alternative.

CoAP : CoAP-Constrained Application Protocol is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252. It enables devices to communicate over the Internet. It is defined as Contrained Application Protocol, and is a protocol intended to be used in very simple hardware. The protocol is especially targeted for constrained hardware such as 8-bits microcontrollers, low power sensors and similar devices that can’t run on HTTP or TLS. It is a simplification of the HTTP protocol running on

UDP, that helps save bandwidth. It is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.

WebSocket : The WebSocket Protocol enables two-way communication between a client running untrusted code in a controlled environment to a remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The goal of this technology is to provide a mechanism for browser-based applications that need two-way communication with servers that does not rely on opening multiple HTTP connections (e.g., using XMLHttpRequest or <iframe>s and long polling).

MQTT :

MQTT is a machine-to-machine (M2M)/”Internet of Things” connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport and useful for connections with remote locations where a small code

footprint is required and/or network bandwidth is at a premium. For example, it has been used in sensors communicating to a broker via satellite link, over occasional dial-up connections with healthcare providers, and in a range of home automation and small device scenarios.

MQTT protocol runs on top of the TCP/IP networking stack. When clients connect and publish/subscribe, MQTT has different message types that help with the handshaking of that process. The MQTT header is two bytes and first byte is constant. In the first byte, you specify the type of message being sent as well as the QoS level, retain, and DUP (duplication) flags. The second byte is the remaining length field.

XMPP : Extensible Messaging and Presence Protocol (XMPP) is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Originally named Jabber, the protocol was developed by the eponymous open-source community in 1999 for near real-time instant messaging (IM), presence information, and contact list maintenance. Designed to be extensible, the protocol has been used also for publish-subscribe systems, signalling for VoIP, video, file transfer, gaming, the Internet of

Things (IoT) applications such as the smart grid, and social networking services.

DDS : The Data Distribution Service (DDS™) is a middleware protocol and API standard for data-centric connectivity from the Object Management Group® (OMG®). It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical Internet of Things (IoT) applications need.

In a distributed system, middleware is the software layer that lies between the operating system and applications. It enables the various components of a system to more easily communicate and share data. It simplifies the development of distributed systems by letting software developers focus on the specific purpose of their applications rather than the mechanics of passing information between applications and systems.

AMQP : The AMQP – IoT protocols consist of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model. AMQP has the following three additives, which might link into processing chains in the server to create the favored capability.

☐ Exchange: Receives messages from publisher primarily based programs and routes them to ‘message queues’.

☐ Message Queue: Stores messages until they may thoroughly process via the eating client software.

☐ Binding: States the connection between the message queue and the change.

_____

Logical Design of IoT

In this article we discuss Logical design of Internet of things. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation. For understanding Logical Design of IoT, we describes given below terms.

☐ IoT Functional Blocks

☐ IoT Communication Models

□ IoT Communication APIs

IoT Functional Blocks

An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.

functional blocks are:

Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.

Communication: Handles the communication for the IoT system.

Services: services for device monitoring, device control service, data publishing services and services for device discovery.

Management: this blocks provides various functions to govern the IoT system.

Security: this block secures the IoT system and by providing functions such as authentication , authorization, message and content integrity, and data security.

Application: This is an interface that the users can use to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyze the processed data.

History of IOT:

Simply stated, the Internet of Things consists of any device with an on/off switch that is connected to the Internet. The Internet of Things (IoT) involves machines communicating information over the internet, and has not been around for very long.

Machines have been providing direct communications since the telegraph (the first landline) was developed in the 1830s and 1840s. Described as “wireless telegraphy,” the first radio voice transmission took place on June 3, 1900, providing a necessary component for developing the Internet of Things. The development of computers began in the 1950s.

HAVE YOU HEARD? WE HAVE A NEW PODCAST!

Tune in weekly to hear different data experts discuss how they built their careers and share tips and tricks for those looking to follow in their footsteps.

The internet, itself a significant component of the IoT, started out as part of DARPA (Defense Advanced Research Projects Agency) in 1962, and evolved into ARPANET (Advanced Research Projects Agency Network) in 1969.

In the 1980s, commercial service providers began supporting public use of ARPANET, allowing it to evolve into our modern Internet. Satellites and landlines provide basic communications for much of the IoT.

Global Positioning Satellites (GPS) became a reality in early 1993, with the Department of Defense providing a stable, highly functional system of 24 satellites. This was quickly followed by privately owned, commercial satellites being placed in orbit, making the IIoT much more functional.

Realizing the Concept

The Internet of Things, as a concept, wasn't officially named until 1999, but one of the first examples of an IoT is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Mellon University. Local programmers would connect through the Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip to purchase one.

Kevin Ashton, MIT's Executive Director of Auto-ID Labs, coined the phrase "Internet of Things" in 1999. He was the first to describe the IoT, while making a presentation for Procter & Gamble, but the definition of the IoT has evolved over time. Mr. Ashton stated:

"Today computers, and, therefore, the Internet, are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a barcode. The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss, and cost. We would know

when things needed replacing, repairing, or recalling and whether they were fresh, or past their best.”

The Early 2000s

Kevin Ashton (the guy who came up with the name “Internet of Things”) believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things — primarily as an inventory tracking solution.

In hindsight, Inventory tracking has become one of the more obvious advantages of the IoT.

He concluded if all devices were “tagged,” computers could manage, track, and inventory them. To some extent, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes.

In 2002-2003, Walmart and the US Department of Defense were the first large organizations to embrace Ashton’s model of tracking inventory using tagging, RFID, and the Internet of Things.

Ring, a doorbell that links to your smartphone, provides an excellent example of the T00nternet of Things being used at home. Ring signals you when the doorbell is pressed, and lets you see who it is, and to speak with them.

The Ring doorbell was developed in 2011 by Jamie Siminoff because he wanted to see who was at his door while he was in the garage, working. He couldn't hear the doorbell from the garage and kept missing deliveries.

An additional and important component in developing a functional IoT took place in June of 2012, when the major Internet service providers and web companies agreed to increase address space on the global Internet by enabling IPV6 for their services and products. Steve Leibson, of the Computer History Museum, stated,

"The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths."

Put another way, we are not going to run out of internet addresses anytime soon.

IoT Getting Smarter

"Smart cities" can use the IoT to reduce waste and maximize the efficient use of energy. The IoT can also be used to streamline traffic flows and locate available parking.

In 2012, The Swiss Federal Office of Energy started a pilot program called "Smart City Switzerland." They brought representatives from

universities, business, and public administration together to discuss new ideas for the urban environment. Smart City Switzerland has over sixty projects underway and supports new scientific partnerships and innovation. (Smart City Switzerland has evolved into something quite impressive.)

A well-designed smart city supports all kind of sensors that are connected to the internet and provides:

- Traffic monitoring- Real-time tracking and reporting of traffic.

- Air quality monitoring- Integrated IoT sensors can identify polluters.

- Smart transportation- Smart traffic lights streamline traffic efficiency and public transport.

- Smart parking- Sensors installed in pavement, etc. to determine occupancy of the parking lot, which is communicated to drivers.

- Smart public lighting- Low energy lighting combined with timing and sensors.

- Smart buildings- When connected to the smart city by way of the internet, it becomes a part of the city infrastructure.

A smart building, by itself, uses sensors and automated processes to control the building's operations, which includes air conditioning, heating, ventilation, security, lighting, and other systems. Smart buildings are integrated systems and share vital information.

The Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) is an extension of the IoT, and uses actuators and smart sensors, which are networked together with a company's industrial applications. The goal is to give industries greater efficiency and reliability. The IIoT includes robotics and software-defined production processes.

The cloud's massive storage capacity (2002) was necessary for the modern version of the IIot to become a reality.

The IIoT came into being in roughly 2010, with several large companies developing their own systems. GE is given credit for creating the term "Tndustrial Tnternet of Things," In 2012.

The Internet of Things Becomes a Part of Life

By the year 2013, the IoT had become a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems.

This includes almost anything you can think of, ranging from mobile phones to building maintenance to the jet engine of an airplane. Medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, can transfer dataover a network and are members of the IoT.

The IoT Goes Mobile – 2015

Smartphones are part of the IoT, and have become an important communications tool for many individuals. In 2015, they joined the IoT with a high degree of enthusiasm from marketers. The sensors within these devices are monitored by marketing departments, who send out certain promotions based on the customer and the product’s location.

The healthcare industry has also taken advantage of this trend. Devices, such as smartwatches, smartphones, and ingestible monitors can keep track of a patient’s data regarding blood pressure, heart rate, and other concerns in real time.

Cars and trucks have become members of the IoT. A connected vehicle works with other devices over wireless networks. This technology allows various “connected networks” to access and communicate with the vehicles.

Cars and trucks are already loaded with sensors and technology, including OBD (on-board diagnostics) and GPS. By maximizing their use of these technologies, businesses can extract information from their fleets about maintenance requirements, driving conditions, and routes in real-time.

Self-driving cars use the cloud to respond to adjacent cars, traffic data, maps, weather, surface conditions, etcetera. Use of the cloud helps the vehicles to monitor their surroundings and make better decisions.

Self-driving cars are new members of the IOT. The first truly self-driving vehicle appeared in the 1980s. In October of 2021, May Mobility launched a pilot program to test their self-driving software.

Human neighborhoods are now becoming part of the interconnected community called the Internet of Things.

Things In IOT:

The Value of Connected "Things" in Healthcare, Logistics and Agriculture

IoT for Healthcare: Our Bodies as "Things" connected to the Internet

"Things" in IoT can also be "wearables" that serve medical purposes. Devices that monitor your bodily functions and systems daily and make that data available to your doctors can function as an early warning system for health issues and a way for you to keep yourself accountable to your health goals.

Image Credit: Sensors Magazine

As Lalit Panda writes in What Is the Internet of Medical Things (IoMT)?, "With streaming information, preventive care can reduce hospitalization and reduce the cost of acute care significantly." However, both Panda and Kristina Podnar, in her article, warn of the serious risk of accidents and abuse that come with connecting our bodies to the internet. In the case of

healthcare, a “thing” in the Internet of Things would be our very bodies.

IoT for Logistics: Packages and Containers As “Things” Connected to the Internet

Logistics and Supply Chain Management are all about moving things from point A to point B. Keeping tracking of those things in an ideal world isn’t terribly difficult. You send shipment X from warehouse Y to customer Z, and you know everything will work out, right? Wrong! The world is dynamic, shifting, and chaotic. Things go wrong. Everything from weather disasters to piracy can affect global shipping lanes and cause delays and financial losses. And sometimes it’s merely naturally built-in inefficiencies that cause losses and delays.

In 2018, in the UK alone, inefficiencies in the supply chain resulted in losses of about $2B, due to what one study called “a game of Chinese whispers” as packages zigzag around the world. Ericsson recently argued in an article on IoT For All that “supply chain participants are connected—just not to each other or not at the right time.”

That’s where the Internet of Things comes in. For Logistics and Supply Chain Applications, “things” in IoT cargo containers, trucks, port utility equipment and, most importantly, data pipelines

and digital ledgers for tracking shipments reliably as they traverse the world and change hands.

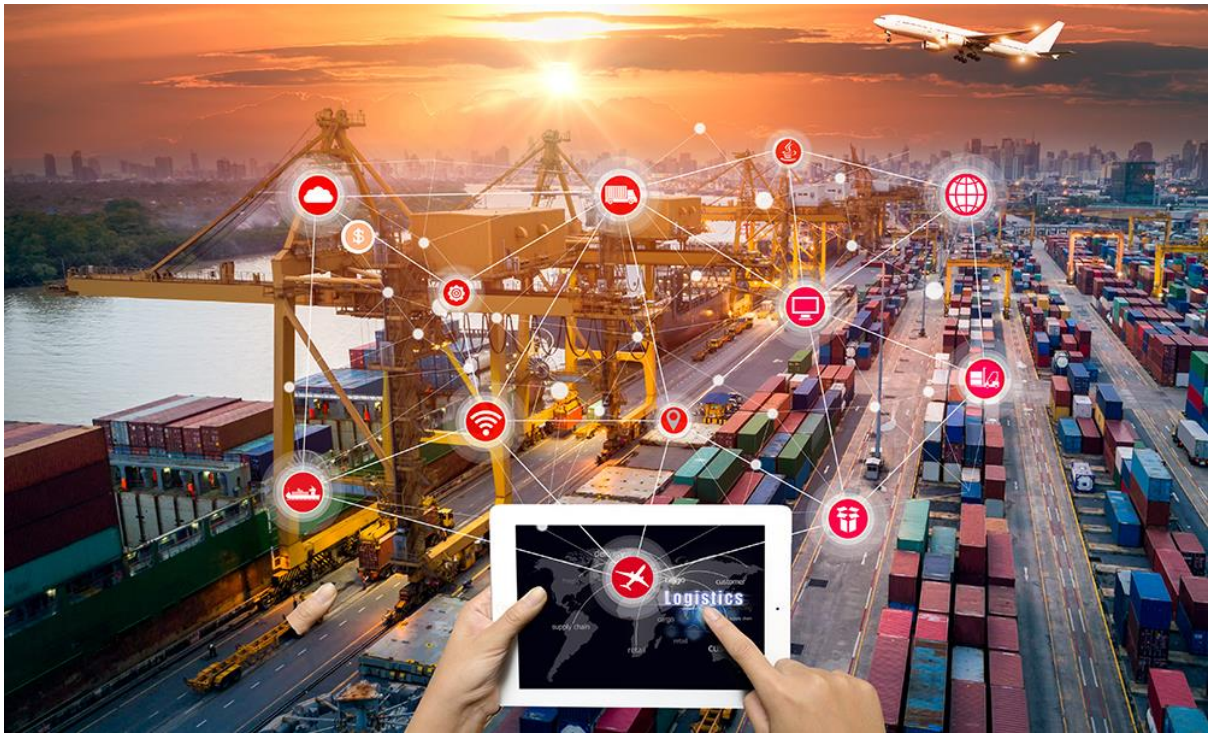


Image Credit: All Things Supply Chain

IoT for Agriculture: “Things” as Tractors, Soil Sensors and Irrigation Systems

From irrigation to crop rotation to fertilization to genetic modification, we’ve been changing the way we grow and harvest food for thousands of years. Farms have grown from small, family- or community-managed organizations to vast enterprises that sprawl across thousands or even millions of acres. As populations exploded throughout the 20th century, farmers have turned to technology to meet growing demands. The 21st century is no different; farmers

continue to find innovative ways to meet food supply needs in an increasingly interdependent and environmentally unstable world.

IoT is enabling a whole range of agricultural innovations. As SciForce writes on IoT For All, farmers are starting to use IoT, drones and AI to "increase the quantity and quality of products while optimizing the human labor required by production."

The photo below shows a soil monitoring solution called "CropX" being used to help farmers better understand which fields need watering when and how soil conditions change over time—all remotely and at massive scale.

Image Credit: Smart2Zero

In this example, CropX represents a “thing” in the Internet of Things. It’s a thing that you can embed in your fields, and since it’s connected to the internet, you can gather insights from it about what’s going on in the soil feeding your crops—remotely and at massive scale, even from the comfort of your farmhouse living room!

The Best Way to Predict the Future Is to Build It

In the now distant past, every “thing” was disconnected. Then the telephone came around and enabled us to connect people and spaces across hundreds and then thousands of miles. Then we started sending not only our voices but other kinds of information across the wire, like documents, images, videos, *etc*. But we couldn’t stop by connecting only things like computers and smartphones to the internet. Why end there? Now we’re focused on connecting the myriad other objects and spaces we use for everyday life and business processes to the internet so that we can extract insights about the world around us and interact with our “things” remotely and at massive scale.

Identifiers in IoT:

identifiers play an important role in Internet of Things (IoT). Identification of the Thing itself comes immediately into my mind. Also the use of identifiers as communication addresses like IP and Ethernet MAC addresses is an obvious application. However when you dive deeper into IoT systems you will recognize many more applications for identifiers. For the design, but also for the use of IoT solutions it is therefore important to know the various usages of identifiers, the related requirements, interoperability, security and privacy issues and which standards are available for them.

These topics came up in AIOTI WG03 on IoT Standards late 2016 and we decided to analyse them further and provide a report about our findings. The starting point of our activity was a survey that we performed in spring 2017. The survey asked questions about IoT use cases, the specific purpose of identifiers, related requirements, standards and standardization gaps. It was sent to standardisation bodies, industry alliances, research projects and individual companies around the world and we received back over eighty responses. These responses were a significant input to our report, along with research and standardisation documents. They showed that identifiers are used in IoT to identify various types of entities for many purposes and within different contexts. The figure below shows an example for the

different identifiers used in a fitness tracking use case.

This use case includes identifiers for:

- Things
- Communication
- User
- Data
- Location
- and Services & Applications

With the classification of identifiers and the categorization of requirements we tried to provide a structure that may help system architects and developers to understand the type of identifiers that they need for their solution and guide them in selecting the specific identifier schemes. In general no single identification scheme fits all needs. Furthermore many identification are already standardized and in

use. We therefore do not define or recommend specific solutions and standards, but provide examples and summaries in order to indicate what has to be taken into account when considering identifiers in IoT.

IoT frameworks:

IoT (Internet of Things) is a network of devices which are connected to the internet for transferring and sensing the data without much human intervention, the framework used to this is termed as the IoT framework, this framework consists all the required capabilities for the cloud support and other needs which is needed to satisfy the IoT technology, few of the common IoT frameworks that are used frequently are KAA IoT, Cisco IoT Cloud Connect, ZETTA IoT, SAP IoT, IBM Watson, Hewlett Packard Enterprise, etc

What is the IoT Framework?

IoT is a key part of a large IoT ecosystem, which promotes and links all elements in the scheme. It allows device management, handles communication protocols on software and hardware, collects / analyses information, improves information flow and intelligent apps functions.

List of IoT Framework

Now we will discuss the IoT Framework one by one

1. KAA IoT

Kaa IoT is one of the most effective and rich Open Source Internet of Things Cloud Platforms, where anyone can freely implement their smart product concepts. You can manage an N number of devices connected to each other with cross-device interoperability on this platform. You can monitor your machine in actual time by providing and configuring remote devices. Kaa enables information exchange between linked devices, the IoT Cloud, information and visualization systems, as well as other elements of IoT Ecosystems

2. Cisco IoT Cloud Connect

Cisco IoT Cloud Connect provides robust, automated, and highly secure connectivity for the enterprise. IoT data management is done by the Cisco Kinetic IoT platform to extract, move and compute the data. As Cisco is very famous for its security services, it protects IoT deployment against threats with a secure IoT architecture.

3. ZETTA IoT

Zetta is nothing but a server-oriented platform developed based on the REST, NodeJS, and the Siren hypermedia-API-strip flow-based reactive programming philosophy. After being abstracted as REST APIs they are connected with cloud services. These internet services include tools for visualizing machine analytics and support such as Splunk. It builds a gero-distributed network through connectivity with systems like Heroku to endpoints like Arduino and Linux hackers.

4. Salesforce IoT

Salesforce is power by thunder. Thunder allows companies to unlock earlier unseen ideas and allows anyone to take proactive, personalized activities from any device to bring their clients closer than ever. More than 150,000 clients worldwide were held by Salesforce. Salesforce has a 19.7% market share in the globe of CRM. SAP (12.%1), Microsoft (6.2%), Oracle (9.1%) are far behind its nearest rivals. Many businesses now develop their apps or migrate to Salesforce on the Salesforce platform. This has raised demand for developers and administrators from Salesforce.

5. DeviceHive IoT

DeviceHive is another rich IoT open-source platform that is distributed under the Apache 2.0 license and can be used and changed free of

charge. It provides deployment options for Docker and Kubernetes and can be downloaded and used both by public and personal cloud. You can run batch analysis and machine learning above and beyond your device information. DeviceHive supports several libraries, including Android and iOS.

6. Oracle IoT

We surely include Oracle, a worldwide software company known to offer its top level of solutions in database management, and business software, as we compare the top Internet-of-Things platforms. Oracle offers its flexible environment outstanding company possibilities to create company applications. Oracle supports the processing and builds large-scale IoT networks with very wide data. The use of advanced security systems to protect IoT systems against external threats is another worth mentioning. Since these systems usually have different devices, some of which have no security tool, it is not sufficiently justifiable to implement centralized security measures.

7. SAP IoT

The SAP Internet of Things cloud platform has everything you need to build and handle an IoT application. The SAP platform provides a convenient environment to remotely manage and

monitor all connected devices of your IoT system. In the SAP Platform a remote-devices we can connect directly or through cloud service. Obviously, SAP can use IoT information to create machine learning and artificial intelligence applications while maintaining recent technological trends.

8. Microsoft Azure IoT

Without the Microsoft Azure solution, a cloud service giant with AWS and Google Cloud platform, the comparison of our IoT platform will be not complete. The Microsoft Azure IoT Suite provides preconfigured solutions and the ability to personalize and develop new solutions to meet the project requirements. The strongest safety mechanisms, superb scalability and simple integration with your current or future systems are achieved through Microsoft Azure Internet of thing Suite.

9. Google Cloud Platform – IoT framework

Things can be done by Google. Google Cloud is one of the best IoT systems available today with its end-to-end platform. Google stands out from the others because it can process the large quantity of information using Cloud IoT Core. Due to Google’s Cloud Data Studio and Big Query you get advanced analysis. With the help of Google Cloud Platform, you can accelerate your

business and with that, you can speed up your device.

10. IBM Watson – IoT framework

We can not expect the Big Blue to miss the chance to make a difference in the IoT segment. IBM Watson is very popular among the internet of thing platform among developers. The Bluemix hybrid cloud-supported Watson IoT platform allows developers to use IoT-applications easily. IBM Watson manages the secure communication and also data storage. Real-time data exchange also is done by IBM Watson.

11. Hewlett Packard Enterprise – IoT framework

Hewlett Packard Enterprise’s universal business platform offers scalability for its customers by offering solutions to most of their problems. The platform provides cloud-based assistance or local support. In smart cities and the automobile industry, HPE universal of things platform was used properly. The data monetization of several businesses has been carried out by HPE. Hewlett Packard Enterprise Collects analyzes information in order to grow the company. In the Hewlett Packard Enterprise M2M device management in Single point, Single seller.

12. DataV by Bsquare – IoT framework

The next cloud platform is DataV by Bsquare. The company is working with the best in the company, including Google, Amazon web services, and Microsoft. Bsquare takes its services seriously and has introduced the DataV application, the hybrid framework for managing your services. It offers a variety of services that predict and analyze all of your ecosystem problems. It Improves the condition maintenances.

13. Mindsphere by Siemens – IoT framework

Mindsphere from Siemens provides a cost-effective platform as a service that is ideal for application development. The cost-efficient platform allows you to connect all your appliances to a cloud solution. In accordance with the DIn ISO / IEC 27001 standard, Siemens claims every stored information is strictly confidential. You can choose open interfaces and local connectivity from the business. Allow you to regulate machine information in order to open fresh opportunities.

14. Ayla Network – IoT framework

Ayla networks have developed their platform as a solution for enterprises. Agile Ayla networks have been established to support customers with the smooth establishment of services, not only to develop the product. In addition to the Ayla agile

platform, AMAP is an agile mobile app platform from Ayla that develops and guides consumers through app development.

15. MBED IoT Device platform

The open-source service is available on the Apache 2.0 Arm MBED computer platform. It involves cloud services, developer tools, and operating systems, that facilitate the creation and operation of business goods. The service is designed to simplify users ' processes. MBED OS was designed to connect all your devices as an open-source platform. The platform provides services from over 60 partners and free access to a community of 200,000 designers. You can flexibly access MBED club service

16. Amazon Web Services (AWS) IoT framework

Amazon Web Services (AWS) is an IoT platform provided by Amazon. This IoT platform provides cloud computing, database, and security services through the AWS Console. There are so many other services such as Regions, Availability Zones, and Virtual Private Clouds (VPCs). It helps to ease out the improving durability, distribution, availability of the application. It provides Registry for recognizing devices, Secure Device Gateway, Compatible Software Development Kit for devices which AWS

partnered with HW manufacturers like Intel, Texas Instruments, Broadcom and Qualcomm.

17. Mocana – IoT framework

The final one on the list is the Mocana company's safety platform. The platform seeks to provide industrial IoT devices and clouds with security. The company provides currently more than 100 companies with services.

18. RTI IoT

RTI is one of the IoT platforms that is the oldest and most pioneering provider and also it is the Most Influent Industrial of the internet of thing firm. Connext DDS is built especially for smart computers and their corresponding cyber-physical systems. Connext DDS does not require response brokers, directory services, servers, as well as administration, unlike messaging middleware designed mainly for IT systems.

7.Difference between IoT and M2M?

1. Internet of Things : IOT is known as the Internet of Things where things are said to be the communicating devices that can interact with each other using a communication media. Usually every day some new devices are being integrated which uses IoT devices for its function. These devices use various sensors and

actuators for sending and receiving data over the internet. It is an ecosystem where the devices share data through a communication media known as the internet. 2. Machine to Machine : This is commonly known as Machine to machine communication. It is a concept where two or more than two machines communicate with each other without human interaction using a wired or wireless mechanism. M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.

IoT and M2M :

Basis of	IoT	M2M
Abbreviation	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this.
Connection type used	The connection is via Network and using various communication types.	The connection is a point to point

Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.
	Traditional protocols and communication technology techniques are used
Data Sharing	Data is shared between other applications that are used to improve the end-user experience.
	Data is shared with only the communicating parties.
Internet	Internet connection is required for communication
	Devices are not dependent on the Internet.
Type of Communication	It supports cloud communication
	It supports point-to-point communication.
Computer System	Involves the usage of both Hardware and Software.
	Mostly hardware-based technology
Scope	A large number of devices yet scope is large.
	Limited Scope for devices.
Business Type used	Business 2 Business(B2B) and Business 2 Consumer(B2C)

	Business 2 Business (B2B)
Open API support	Supports Open API integrations.
	There is no support for Open APIs
Examples	Smart wearables, Big Data and Cloud, etc.
	Sensors, Data and Information, etc.

Short Answer Questions:

1.What is the definition of IOT?

2.Explain about history of IOT?

3.What are the characteristics of IOT?

4.Explain about things in IOT?

Long Answer Questions:

1.Explain about physical and logical design of IOT?

2.Explain about IOT frameworks and Architecture of IOT?

3.Explain about IOT and M2M in detail?

UNIT-2

Sensors and Networks

Sensor:

We live in a World of Sensors. You can find different types of Sensors in our homes, offices, cars etc. working to make our lives easier by turning on the lights by detecting our presence, adjusting the room temperature, detect smoke or fire, make us delicious coffee, open garage doors as soon as our car is near the door and many other tasks.

All these and many other automation tasks are possible because of Sensors. Before going in to the details of What is a Sensor, What are the Different Types of Sensors and Applications of these different types of Sensors, we will first take

a look at a simple example of an automated system, which is possible because of Sensors (and many other components as well).

Outline

- Real Time Application of Sensors
- What is a Sensor?
- Classification of Sensors
- Different Types of Sensors
  - Temperature Sensor
  - Proximity Sensors
  - Infrared Sensor (IR Sensor)
  - Ultrasonic Sensor
  - Light Sensor

- Smoke and Gas Sensors
- Alcohol Sensor
- Touch Sensor
- Color Sensor
- Humidity Sensor
- Tilt Sensor

Real Time Application of Sensors

The example we are talking about here is the Autopilot System in aircrafts. Almost all civilian and military aircrafts have the feature of Automatic Flight Control system or sometimes called as Autopilot.

An Automatic Flight Control System consists of several sensors for various tasks like speed control, height monitoring, position tracking, status of doors, obstacle detection, fuel level, maneuvering and many more. A Computer takes

data from all these sensors and processes them by comparing them with pre-designed values.

The computer then provides control signals to different parts like engines, flaps, rudders, motors etc. that help in a smooth flight. The combination of Sensors, Computers and Mechanics makes it possible to run the plane in Autopilot Mode.

All the parameters i.e., the Sensors (which give inputs to the Computers), the Computers (the brains of the system) and the mechanics (the outputs of the system like engines and motors) are equally important in building a successful automated system.

This is an extremely simplified version of Flight Control System. In fact, there are hundreds of individual control systems which preform unique tasks for a safe and smooth journey.

But in this tutorial, we will be concentrating on the Sensors part of a system and look at different concepts associated with Sensors (like types, characteristics, classification etc.).

What is a Sensor?

There are numerous definitions as to what a sensor is but I would like to define a Sensor as an input device which provides an output (signal)

with respect to a specific physical quantity (input).

The term “input device” in the definition of a Sensor means that it is part of a bigger system which provides input to a main control system (like a Processor or a Microcontroller).

Another unique definition of a Sensor is as follows: It is a device that converts signals from one energy domain to electrical domain. The definition of the Sensor can be better understood if we take an example in to consideration.

The simplest example of a sensor is an LDR or a Light Dependent Resistor. It is a device, whose resistance varies according to intensity of light it is subjected to. When the light falling on an LDR is more, its resistance becomes very less and when the light is less, well, the resistance of the LDR becomes very high.

We can connect this LDR in a voltage divider (along with other resistor) and check the voltage drop across the LDR. This voltage can be calibrated to the amount of light falling on the LDR. Hence, a Light Sensor.

Now that we have seen what a sensor is, we will proceed further with the classification of Sensors.

Classification of Sensors

There are several classifications of sensors made by different authors and experts. Some are very simple and some are very complex. The following classification of sensors may already be used by an expert in the subject but this is a very simple classification of sensors.

In the first classification of the sensors, they are divided in to Active and Passive. Active Sensors are those which require an external excitation signal or a power signal.

Passive Sensors, on the other hand, do not require any external power signal and directly generates output response.

The other type of classification is based on the means of detection used in the sensor. Some of the means of detection are Electric, Biological, Chemical, Radioactive etc.

The next classification is based on conversion phenomenon i.e., the input and the output. Some of the common conversion phenomena are Photoelectric, Thermoelectric, Electrochemical, Electromagnetic, Thermooptic, etc.

The final classification of the sensors are Analog and Digital Sensors. Analog Sensors produce an analog output i.e., a continuous output signal

(usually voltage but sometimes other quantities like Resistance etc.) with respect to the quantity being measured.

Digital Sensors, in contrast to Analog Sensors, work with discrete or digital data. The data in digital sensors, which is used for conversion and transmission, is digital in nature.

Types of Sensors:

The following is a list of different types of sensors that are commonly used in various applications. All these sensors are used for measuring one of the physical properties like Temperature, Resistance, Capacitance, Conduction, Heat Transfer etc.

1. Temperature Sensor

2. Proximity Sensor

3. Accelerometer

4. IR Sensor (Infrared Sensor)

5. Pressure Sensor

6. Light Sensor

7. Ultrasonic Sensor

8. Smoke, Gas and Alcohol Sensor

9. Touch Sensor

10. Color Sensor

11. Humidity Sensor

12. Position Sensor

13. Magnetic Sensor (Hall Effect Sensor)

14. Microphone (Sound Sensor)

15. Tilt Sensor

16. Flow and Level Sensor

17. PIR Sensor

18. Touch Sensor

19. Strain and Weight Sensor

We will see about few of the above-mentioned sensors in brief. More information about the sensors will be added subsequently. A list of projects using the above sensors is given at the end of the page.

Temperature Sensor

One of the most common and most popular sensors is the Temperature Sensor. A Temperature Sensor, as the name suggests, senses the temperature i.e., it measures the changes in the temperature.

There are different types of Temperature Sensors like Temperature Sensor ICs (like LM35, DS18B20), Thermistors, Thermocouples, RTD (Resistive Temperature Devices), etc.

Temperature Sensors can be analog or digital. In an Analog Temperature Sensor, the changes in the Temperature correspond to change in its physical property like resistance or voltage. LM35 is a classic Analog Temperature Sensor.

Coming to the Digital Temperature Sensor, the output is a discrete digital value (usually, some

numerical data after converting analog value to digital value). DS18B20 is a simple Digital Temperature Sensor.

Temperature Sensors are used everywhere like computers, mobile phones, automobiles, air conditioning systems, industries etc.

A simple project using LM35 (Celsius Scale Temperature Sensor) is implemented in this project: TEMPERATURE CONTROLLED SYSTEM.

Proximity Sensors

A Proximity Sensor is a non-contact type sensor that detects the presence of an object. Proximity Sensors can be implemented using different techniques like Optical (like Infrared or Laser), Sound (Ultrasonic), Magnetic (Hall Effect), Capacitive, etc.

Some of the applications of Proximity Sensors are Mobile Phones, Cars (Parking Sensors), industries (object alignment), Ground Proximity in Aircrafts, etc.

Proximity Sensor in Reverse Parking is implemented in this Project: REVERSE PARKING SENSOR CIRCUIT.

Infrared Sensor (IR Sensor)

IR Sensors or Infrared Sensor are light based sensor that are used in various applications like Proximity and Object Detection. IR Sensors are used as proximity sensors in almost all mobile phones.

There are two types of Infrared or IR Sensors: Transmissive Type and Reflective Type. In Transmissive Type IR Sensor, the IR Transmitter (usually an IR LED) and the IR Detector (usually a Photo Diode) are positioned facing each other so that when an object passes between them, the sensor detects the object.

The other type of IR Sensor is a Reflective Type IR Sensor. In this, the transmitter and the detector are positioned adjacent to each other facing the object. When an object comes in front of the sensor, the infrared light from the IR Transmitter is reflected from the object and is detected by the IR Receiver and thus the sensor detects the object.

Different applications where IR Sensor is implemented are Mobile Phones, Robots, Industrial assembly, automobiles etc.

A small project, where IR Sensors are used to turn on street lights: STREET LIGHTS USING IR SENSORS.

Ultrasonic Sensor

An Ultrasonic Sensor is a non-contact type device that can be used to measure distance as well as velocity of an object. An Ultrasonic Sensor works based on the properties of the sound waves with frequency greater than that of the human audible range.

Using the time of flight of the sound wave, an Ultrasonic Sensor can measure the distance of the object (similar to SONAR). The Doppler Shift property of the sound wave is used to measure the velocity of an object.

Arduino based Range Finder is a simple project using Ultrasonic Sensor: PORTABLE ULTRASONIC RANGE METER.

Light Sensor

Sometimes also known as Photo Sensors, Light Sensors are one of the important sensors. A simple Light Sensor available today is the Light Dependent Resistor or LDR. The property of LDR is that its resistance is inversely proportional to

the intensity of the ambient light i.e., when the intensity of light increases, its resistance decreases and vise-versa.

By using LDR is a circuit, we can calibrate the changes in its resistance to measure the intensity of Light. There are two other Light Sensors (or Photo Sensors) which are often used in complex electronic system design. They are Photo Diode and Photo Transistor. All these are Analog Sensors.

There are also Digital Light Sensors like BH1750, TSL2561, etc., which can calculate intensity of light and provide a digital equivalent value.

Check out this simple LIGHT DETECTOR USING LDR project.

Smoke and Gas Sensors

One of the very useful sensors in safety related applications are Smoke and Gas Sensors. Almost all offices and industries are equipped with several smoke detectors, which detect any smoke (due to fire) and sound an alarm.

Gas Sensors are more common in laboratories, large scale kitchens and industries. They can

detect different gases like LPG, Propane, Butane, Methane (CH4), etc.

Now-a-days, smoke sensors (which often can detect smoke as well gas) are also installed in most homes as a safety measure.

The “MQ” series of sensors are a bunch of cheap sensors for detecting CO, CO2, CH4, Alcohol, Propane, Butane, LPG etc. You can use these sensors to build your own Smoke Sensor Application.

Check out this SMOKE DETECTOR ALARM CIRCUIT without using Arduino.

Alcohol Sensor

As the name suggests, an Alcohol Sensor detects alcohol. Usually, alcohol sensors are used in breathalyzer devices, which determine whether a person is drunk or not. Law enforcement personnel uses breathalyzers to catch drunk-and-drive culprits.

A simple tutorial on HOW TO MAKE ALCOHOL BREATHALYZER CIRCUIT?

Touch Sensor

We do not give much importance to touch sensors but they became an integral part of our life. Whether you know or not, all touch screen devices (Mobile Phones, Tablets, Laptops, etc.) have touch sensors in them. Another common application of touch sensor is trackpads in our laptops.

Touch Sensors, as the name suggests, detect touch of a finger or a stylus. Often touch sensors are classified into Resistive and Capacitive type. Almost all modern touch sensors are of Capacitive Types as they are more accurate and have better signal to noise ratio.

If you want to build an application with Touch Sensor, then there are low-cost modules available and using those touch sensors, you can build TOUCH DIMMER SWITCH CIRCUIT USING ARDUINO.

Color Sensor

A Color Sensor is an useful device in building color sensing applications in the field of image processing, color identification, industrial object tracking etc. The TCS3200 is a simple Color Sensor, which can detect any color and output a

square wave proportional to the wavelength of the detected color.

If you are interested in building a Color Sensor Application, checkout this ARDUINO BASED COLOR DETECTOR project.

Humidity Sensor

If you see Weather Monitoring Systems, they often provide temperature as well as humidity data. So, measuring humidity is an important task in many applications and Humidity Sensors help us in achieving this.

Often all humidity sensors measure relative humidity (a ratio of water content in air to maximum potential of air to hold water). Since relative humidity is dependent on temperature of air, almost all Humidity Sensors can also measure Temperature.

Humidity Sensors are classified into Capacitive Type, Resistive Type and Thermal Conductive Type. DHT11 and DHT22 are two of the frequently used Humidity Sensors in DIY Community (the former is a resistive type while the latter is capacitive type).

Checkout this tutorial with DHT11 HUMIDITY SENSOR ON ARDUINO.

Tilt Sensor

Often used to detect inclination or orientation, Tilt Sensors are one of the simplest and inexpensive sensors out there. Previously, tilt sensors are made up of Mercury (and hence they are sometimes called as Mercury Switches) but most modern tilt sensors contain a roller ball.

A simple Arduino based title switch using tilt sensor is implemented here HOW TO MAKE A TILT SENSOR WITH ARDUINO?

In this article, we have seen about What is a Sensor, what are the classification of sensors and Different Types of Sensors along with their practical applications. In the future, I will update this article with more sensors and their applications.

Actuator:

An actuator is a machine part that initiates movements by receiving feedback from a control signal. Once it has power, the actuator creates

specific motions depending on the purpose of the machine.

What Are Some Devices with Actuators?

Machines and systems have featured actuators since their popularization back in World War II. The most well-known examples of actuators include:

- Electric motors: Any part of a piece of equipment or appliance that translates electrical energy into motion, such as those found in ventilation fans, blenders, or refrigerators, contains at least one actuator. Electric cars also use actuators.

- Stepper motors: These actuators are best known for receiving digital pulses and converting them into mechanical motion. Stepper motors are often seen in robots, smart tools, or automated cutting equipment.

- Hydraulic cylinders: These are linear-motion devices that operate using a tube, piston, and rod. Many

vehicles operate using hydraulic motion, such as bulldozers, backhoes, or excavators.

Types of Actuators:

Actuators can be classified by the motion they produce and the power source they use.

Motion

Actuators can create two main types of motion: linear and rotary.

Linear Actuators

Implied by their name, linear actuators are devices that produce movement within a straight path. They can either be mechanical or electrical and are mostly seen in hydraulic or pneumatic devices. Any machine, equipment, or gadget that requires some form of straight motion typically has a linear actuator.

In a simple linear actuator, there is a nut, cover, and a sliding tube. The sliding tube provides the space for the motion, whereas the nut and cover provide the interlocking movement that keeps the actuator in a straight path. Other complex linear actuators will have additional parts, but

the system mentioned above is the foundation for straight movement.

Rotary Actuators

In contrast to linear actuators, rotary actuators create a circular motion. From the term “rotary,” most machines use these rotating parts to complete a turning movement. They are often used in conjunction with a linear actuator if a machine requires moving forward, backward, up, or down.

Many rotary actuators are electrically powered, but some are powered using a hydraulic or pneumatic system. You can find rotary actuators in windshield wipers, electric fans, or manufacturing machines that transport goods from one area to another.

Source of Energy

To further distinguish different types of actuators, we can also sort them according to the power source or system they use to move. Below are the most common actuators according to energy source:

Hydraulic Actuators

Hydraulic actuators operate by the use of a fluid-filled cylinder with a piston suspended at the

center. Commonly, hydraulic actuators produce linear movements, and a spring is attached to one end as a part of the return motion. These actuators are widely seen in exercise equipment such as steppers or car transport carriers.

Pneumatic Actuators

Pneumatic actuators are one of the most reliable options for machine motion. They use pressurized gases to create mechanical movement. Many companies prefer pneumatic-powered actuators because they can make very precise motions, especially when starting and stopping a machine.

Examples of equipment that uses pneumatic actuators include:

- Bus brakes
- Exercise machines
- Vane motors
- Pressure sensors
- Pneumatic mailing systems

Electric Actuators

Electric actuators, as you may have guessed, require electricity to work. Well-known examples include electric cars, manufacturing machinery, and robotics equipment. Similar to pneumatic actuators, they also create precise motion as the flow of electrical power is constant.

The different types of electrical actuators include:

- Electromechanical actuators: These actuators convert electric signals into rotary or linear movements and may even be capable of a combination of both.

- Electrohydraulic actuators: This type of actuator is also powered electrically but gives movement to a hydraulic accumulator. The accumulator then provides the force for movement, usually seen in heavy industrial equipment.

Thermal and Magnetic Actuators

Thermal and magnetic actuators usually consist of shape memory alloys that can be heated to produce movement. The motion of thermal or magnetic actuators often comes from the Joule effect, but it can also occur when a coil is placed in a static magnetic field. The magnetic field causes constant motion called the Laplace-Lorentz force. Most thermal and magnetic actuators can produce a wide and powerful range of motion while remaining lightweight.

Mechanical Actuators

Some actuators are mostly mechanical, such as pulleys or rack and pinion systems. Another mechanical force is applied, such as pulling or pushing, and the actuator will leverage that single movement to produce the desired results. For instance, turning a single gear on a set of rack and pinions can mobilize an object from point A to point B. The tugging movement applied on the pulley can bring the other side upwards or towards the desired location.

Supercoiled Polymer Actuators

Supercoiled polymer actuators are a relatively new addition to the different types of actuators. They are used in robotics and prosthetic limbs as they can replicate the motion of human muscle via a coil that contracts and expands when heated or cooled.

How to Select the Right Actuator

Understanding the different types of actuators is a crucial step in making the best selection for your equipment. Since each kind has its unique purpose and energy requirements, we'll go over factors that will help you arrive at the best decision.

Power Source Availability

The first thing you have to consider is the compatibility of your power source. If you own an industrial site with an electrical source, perhaps the best choice—and the option with the most selections—would be electric actuators. If there are no electrical sources in the area, or you want a piece of fully functional equipment without electricity, you can opt for pneumatic or hydraulic types.

Required Movement

Another important factor when choosing an actuator is the range of movement that you need for your equipment. Is it linear, rotary, or an integration of both? Custom-made actuators can combine or chronologically create these motions to help you concretize the final equipment.

Precision

Some actuators are more precise than others. For example, air brakes are created through pneumatic actuators because air pressure is known to be efficient in the start and stop movements. Other actuators have a larger margin of movement variations, such as those operated through hydraulics.

Any industry that requires a high level of precision for safety and success of operation should consider actuator types that have specific movements.

Safety and Environmental Concerns

Safety is another factor to consider when choosing an actuator for your equipment. Electrical or thermal actuators should be used with caution in areas with extreme temperatures or conducting hazards. For example, operating electrical actuators close to a water body without sealing or other safety measures may create an occupational hazard.

If your company is also committed to a reduced carbon footprint, you'll need to note each actuators' environmental impact. Typically, electrical actuators have little to no carbon footprint.

Official Guidelines

There are also specific guidelines to follow for industrial actuators in certain areas. For example, locations with a high presence of combustible gases should adhere to the requirements imposed by the National Electrical Manufacturers Association (NEMA).

Maintaining Your Actuator

All equipment requires maintenance. Maintaining your actuators will help prevent major shutdowns, hazards, or loss of productivity. Here are some general tips to keep your actuators in top shape.

- Regular inspection: Performing routine visual equipment checks will identify early signs of actuator issues. A mechanic with a keen eye is necessary to inspect for wear and tear.

- Replenish and replace: Hydraulic actuators sometimes need cylinder fluid replenishment. Always double-check for leaks and signs of low hydraulic fluid levels. Replace loose or damaged nuts, bolts, coils, or screws in your actuator parts as well.

- Measure performance data: In some cases, actuators won’t show external signs of a problem, but you can trace issues through performance. Automated graphs and output computation may be necessary if you want to catch deeper issues.

IOT Development board:

A development board is a printed circuit board with circuitry and hardware designed to assist experimentation with a certain microcontroller.

Well, to understand this assume you have a microcontroller that is capable of doing many cool things but to be able to use that you need to first set up a group of circuitry and hardware on your breadboard every time. I know this is kind of frustrating to our smart engineers, especially when there are circuits that are going to be the same every time, like power circuits. At the same time, many hardware circuits are quite helpful in testing and debugging like pushbuttons that is better to be prototyped.

In short, To make the engineers’ life easier and more efficient with prototyping development boards are constructed.

Why not have a quick look at the typical components of a Development board. Here they are:

- Power circuit– Generally set up to run off of a 9V power supply
- Programming interface– Let you program the microcontroller from a computer
- Basic input – Usually buttons
- Basic output– Usually LEDs
- I/O pins– Used for motors, temperature sensors, LCD screens, etc.

Key Features That Must be Included in Your Development Board

Any development board you consider for an IoT project must include a few important features. Those are:

Processing power. This could be in the form of a CPU, microcontroller, FPGA, or other CPLD. A

microcontroller comes in handy for programming your device as many manufacturers provide the IDE you need.

Wireless capabilities. This feature provides wireless communication without including an external transceiver module. Some of the common protocols include Bluetooth, Zigbee, WiFi, and others.

Scalability. This particular feature allows one to add more functionality to the development board? You may verify if the board communicates via GPIO, UART, SPI, or some other protocol; As this will determine how the board interacts with other devices.

Memory. Board memory is important. To store much data, you need built-in Flash memory. A decent board allows connecting a MiniSD or MicroSD card to enhance data storage.

Have An IoT App Idea In Mind? Get A Free Consultation & Wire-Frames Done From Our Experts!

IoT boards are useful hardware structures that we use to prototype a new IoT project. As we discussed above, the custom hardware results in expensive to design and manufacture, and

development boards comes to rescue to avoid that.

There are several IoT prototyping boards in the market with different specifications. And here we will cover top development boards for IoT projects.

All the below mentioned IoT boards will fall into any of the below categories:

1. Microcontroller-based boards
2. System on Chip (SOC) boards
3. Single-board Computers (SBC)

Let’s get straight to the most popular IoT Development Boards:

1. Raspberry Pi
2. Omega 2
3. Particle Photon
4. Beagle bone –

5. Jetson Nano

6. ESP 32

7. Banana Pi

8. Arduino Nano 33 IoT

9. Tessel 2

10. i.MX 8

Raspberry Pi Development kit:

The raspberry pi Development Board is a small credit card size computer. That works on Linux based operating systems and is good for embedded projects. Raspberry boards can be easily plugged in to your monitor, computer or TV. It uses a standard keyboard and mouse. Even amateur users depend on it for configuring their digital media systems and surveillance cameras.

Features :

- Processor: 1.2GHz, 64-bit quad-core ARMv8 CPU

- 802.11n Wireless LAN
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Combined 3.5mm audio jack and composite video
- Camera interface (CSI)
- Display interface (DSI)
- Micro SD card slot
- videoCore IV 3D graphics core

2. Omega 2

Omega 2 is one of Onion’s Linux-based WiFi development boards that allow makers of all skill levels to build connected hardware. This highly integrated board comes with a powerful processor and flexible GPIOs. The Platform lets you prototype hardware devices using familiar tools like Git, npm, pip, as well as high-level programming languages like Python, Javascript, and PHP.

Features :

- Linux Operating System, powerful processor, and flexible GPIOs.
- Compact size that easily fits into any project design.
- Modular design for a vast range of flexibility.
- Arduino compatible.
- Integrated Wi-Fi;

- Connectivity is expandable with 2G, 3G, Ethernet, Bluetooth®, Bluetooth Low Energy (BLE), GPS.

- U.FL Connector for external Wi-Fi antenna attachment.

- FCC and CE Certified.

3. Particle Photon

Particle Photon Board consists of an STM32 microcontroller, Wi-Fi, Switches, and LEDs. Simple to use, powerful, and connected to the cloud. Powered by a Cypress Wi-Fi chip alongside a powerful STM32 ARM Cortex M3 microcontroller, it is ideal for prototyping IoT projects.

Features :

- Processor: STM32F205 120Mhz ARM Cortex M3

- Real-time operating system (Free RTOS)

- Memory: 1MB flash, 128KB RAM
- Open source design
- On-board Wi-Fi module
- On-board RGB status LED.
- 18 Mixed-signal GPIO and advanced peripherals
- Soft AP setup
- B802.11b/g/n Wi-Fi
- roadcom BCM43362 Wi-Fi chip

4. Beagle Bone

The Beagle bone is a low power open-source single-board computer produced by Texas instruments. The board can boot Linux in under 10 seconds also you can start developing in less than 5 minutes with just a single USB cable.

It is a computer installed inside of a larger electronics project. The beagle board carries two rows of GPIO (general purpose Input/Output) pins mounted along each side of the board. That allow it to communicate with a wide range of servos, sensors, outputs and other hardware, making it act as the brain of large & complex projects.

Its capabilities can be extended using plug-in boards referred to as “capes”. that are easily available for LCD, motor control, VGA, prototyping, battery power, and other functionalities.

Features :

- DDR memory: 512 MB
- Ability to run Ruby, Python, and INO Sketches directly in the Cloud9 IDE,
- Ethernet: On-chip 10/100 Ethernet
- JTAG: Optional
- Memory: 4GB eMMC memory

- Power Options: Via USB or 5V DC input
- Price (USD) Per Unit: $55.00 (Suggested Retail Price)
- Processor: 1GHz AM3359 Sitara ARM Cortex-A8

5. Jetson Nano

Jetson Nano is a power-efficient and low-cost development board. Provides total performance to run modern AI workloads in a small form factor. Additionally, It has the ability for heavy workload applications like image classification, object detection, segmentation, and speech processing. It is capable to run multiple neural network apps at the same time.

Features:

- GPU: 128-core NVIDIA Maxwell™ architecture-based GPU.
- CPU: Quad-core ARM® A57.
- Video: 4K @ 30 fps

- Camera: 1/3” AR0330 CMOS Image sensor with 2.2 µm pixel.
- Memory: 4 GB 64-bit LPDDR4; 25.6 gigabytes/second.
- Connectivity: Gigabit Ethernet.
- OS Support: Linux for Tegra®.

ESP 32

ESP32 is a dual core low-footprint system development board powered by the latest ESP-WROOM-32 module that can be easily placed into a solderless breadboard. It has a pre-integrated antenna, power amplifier, low-noise amplifiers, filters, and power management module. Because of this, it’s easy to build and test circuits as well as making projects related to IoT integrating with the cloud platform.

Features :

- 2.4 GHz dual-mode Wi-Fi.

- Programmable with Arduino open-source IDE.
- 8 independent LED.
- Bluetooth chips by TSMC.
- 40nm low power technology, power, and RF.
- Easily embedded with other products.
- Strong function with support LWIP protocol.
- Supports three modes: AP, STA, and AP+STA.
- Supporting the Lua program, easily to develop.

7. Banana Pi

Banana Pi is a line of low-cost credit card-sized single-board computers(SBC). IT is a router-based development board, which efficiently runs

on various open-source operating systems including OpenWRT and Android, Lubuntu, Ubuntu, Debian, and Raspbian. Well, the hardware design of banana pi was influenced by the Raspberry Pi and it is compatible with Raspberry Pi boards.

Features :

- All winner A20 Dual-core 1.0 GHz CPU
- Mali-400 MP2 with Open GL ES 2.0/1.1.
- 1 GB DDR3 memory.
- 1x Gigabit LAN
- 1x SATA interface.
- 1X MIC
- 1x USB otg and 2x USB 2.0
- HDMI out

- Composite video out
- CSI camera interface
- DSI display interface
- 26 PIN GPIO

8. Arduino Nano 33 IoT

The Arduino Nano 33 IoT is a dual-processor device that is perfect for experimentation. It offers a practical and low-cost solution for inventors seeking to add Wi-Fi connectivity to their projects with minimal previous experience in networking. The board is compatible with the Arduino IoT Cloud, where you can create IoT applications in a few simple steps

Features :

- ARM Cortex-M0 32-bit SAMD21 processor
- 14 digital I/O pins and 8 analog input pins

- Support up to 12-bit ADC/PWM and 10-bit DAC resolutions.

- Can operate as a few different USB devices: (asynchronous serial, keyboard or mouse) also referred as HID, and USB MIDI.

- Can communicate via Synchronous serial communications.

- Inbuilt real-time clock module.

9. Tessel 2

It’s a kind of System on Chipboards. With WIFI capabilities, it allows you to build scripts in Node.js. The board also provides you with a connected hardware prototyping system that can be used in multiple different applications. Loaded with on-board features including two 10-pin module ports to add sensors and other external hardware, a 10/100 supported ethernet port, 2 USB ports for camera peripherals and flash storage, and a microUSB connector for power and tethered programming.

Features :

- 2 USB ports (you can connect cameras or flash storage, for example)
- 10/100 ethernet port
- 802.11 b/g/n WiFi
- 580MHz Mediatek router-on-a-chip (you can turn your Tessel 2 into an access point!)
- 48MHz SAMD21 coprocessor (for making I/O faster)
- 64MB DDR2 RAM, 32MB of flash (lots of space for your programs and stuff)

10. i.MX 8

i.MX 8 boards offer low power, flexible memory options, a wide range of high-speed interfaces, as well as industry-leading audio and video capabilities. It also comes with a pre-installed boot image flashed on one eMMC memory.

With best-in-class computing power, superior graphics performance, and sophisticated security features, i.MX boards became the next-gen technology for industrial embedded systems.

Features :

- i.MX 8M Quad Applications Processor.
- 4x Arm Cortex-A53 @ 1.5GHz.
- NXP PMIC PF4210 power management.
- LPDDR4 x32 @3200MT w/4GB, eMMC 5.0 w/16GB, MicroSD, QSPI w/256Gb memory availability.
- HDMI 2.0a Type-A , MIPI-CSI Camera mini-SAS, MIPI-DSI Display mini-SAS camera connector.
- 10/100/1000 Ethernet, USB 3.0 Type-A & C, PCIe M.2 interface, and Infrared connector.
- Linux, Android, and FreeRTOS OS support.

So, these are the top development boards that may fit for your various project requirements. And if are overwhelmed with the options and need guidelines that may assist you in finding the right development board.

RFID (radio frequency identification):

RFID (radio frequency identification) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person.

How does RFID work?

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers -- fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors

including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

What are RFID tags and smart labels?

RFID tags are made up of an integrated circuit (IC), an antenna and a substrate. The part of an RFID tag that encodes identifying information is called the RFID inlay.

There are two main types of RFID tags:

- Active RFID. An active RFID tag has its own power source, often a battery.

- Passive RFID. A passive RFID tag receives its power from the reading antenna, whose electromagnetic wave induces a current in the RFID tag's antenna.

There are also semi-passive RFID tags, meaning a battery runs the circuitry while communication is powered by the RFID reader.

Low-power, embedded non-volatile memory plays an important role in every RFID system. RFID tags typically hold less than 2,000 KB of data, including a unique identifier/serial number.

Tags can be read-only or read-write, where data can be added by the reader or existing data overwritten.

The read range for RFID tags varies based on factors including type of tag, type of reader, RFID frequency, and interference in the surrounding environment or from other RFID tags and readers. Active RFID tags have a longer read range than passive RFID tags due to the stronger power source.

smart labels are simple RFID tags. These labels have an RFID tag embedded into an adhesive label and feature a barcode. They can also be used by both RFID and barcode readers. Smart labels can be printed on-demand using desktop printers, where RFID tags require more advanced equipment.

ZEBRA TECHNOLOGIES

RFID readers can be fixed (left) or mobile (right).

What are the types of RFID systems?

There are three main types of RFID systems: low frequency (LF), high frequency (HF) and ultra-high frequency (UHF). Microwave RFID is also

available. Frequencies vary greatly by country and region.

- Low-frequency RFID systems. These range from 30 KHzto 500 KHz, though the typical frequency is 125 KHz. LF RFID has short transmission ranges, generally anywhere from a few inches to less than six feet.

- High-frequency RFID system These range from 3 MHzto 30 MHz, with the typical HF frequency being 13.56 MHz. The standard range is anywhere from a few inches to several feet.

- UHF RFID systems. These range from 300 MHz to 960 MHz, with the typical frequency of 433 MHz and can generally be read from 25-plus feet away.

- Microwave RFID systems. These run at 2.45 Ghzand can be read from 30-plus feet away.

The frequency used will depend on the RFID application, with actual obtained distances sometimes varying from what is expected. For example, when the U.S. State Department announced it would issue electronic passports enabled with an RFID chip, it said the chips would only be able to be read from

approximately 4 inches away. However, the State Department soon received evidence that RFID readers could skim the information from the RFID tags from much farther than 4 inches -- sometimes upward of 33 feet away.

If longer read ranges are needed, using tags with additional power can boost read ranges to 300-plus feet.

Applications of RFID:

RFID dates back to the 1940s; however, it was used more frequently in the 1970s. For a long time, the high cost of the tags and readers prohibited widespread commercial use. As hardware costs have decreased, RFID adoption has also increased.

Some common uses for RFID applications include:

- pet and livestock tracking
- inventory management
- asset tracking and equipment tracking

- inventory control
- cargo and supply chain logistics
- vehicle tracking
- customer service and loss control
- improved visibility and distribution in the supply chain
- access control in security situations
- shipping
- healthcare
- manufacturing
- retail sales
- tap-and-go credit card payments

Components of RFID Technology

RFID technology consists of four components such as RFID tags, antenna, RFID receiver (transceiver) and software.

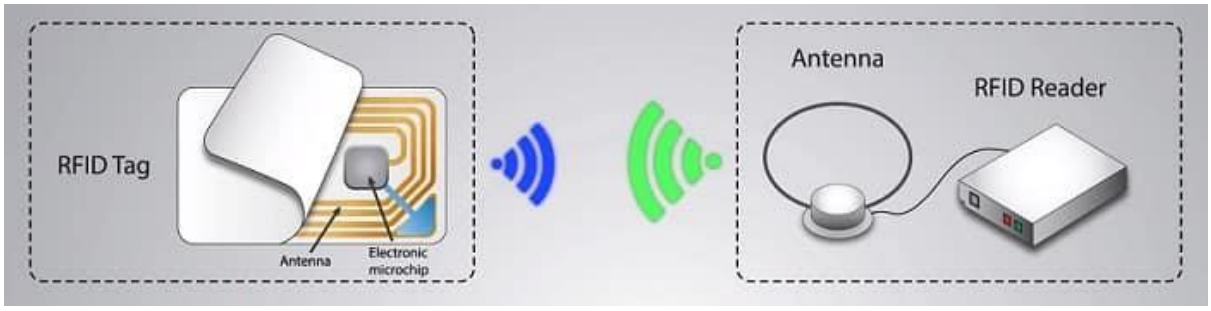


Image: Youtube

1. RFID Tag

RFID tags are small devices consists of an electronic microchip embedded inside and an antenna. The microchip has the unique identification number of the RFID tag.

Passive RFID tag does not have a power source; it will receive power from radio signals transmitted from the RFID receiver. These tags will operate when the reader is at the proximity of the tags (line of sight not required).

Antenna coil will act as power source and medium to transfer data to the reader.

Types of Tags

Passive Tags: Does not have a power source, uses power from the reader to operate.

Battery Assisted Passive Tags: Logic circuit chip uses battery power. Need RF signals from the reader to activate and function.

Active Tags: Uses a power source like battery, does not require power from source/reader.

2. Antenna

RFID antennas are designed to operate at a specific frequency for each applications in which it operates. These antennas are often mounted on the RFID reader and easily accessible for tags to tap on it.

In some handheld devices, antenna is often attached to the device. Size and shape of the

antenna depends on the application and the operating frequency of the system.

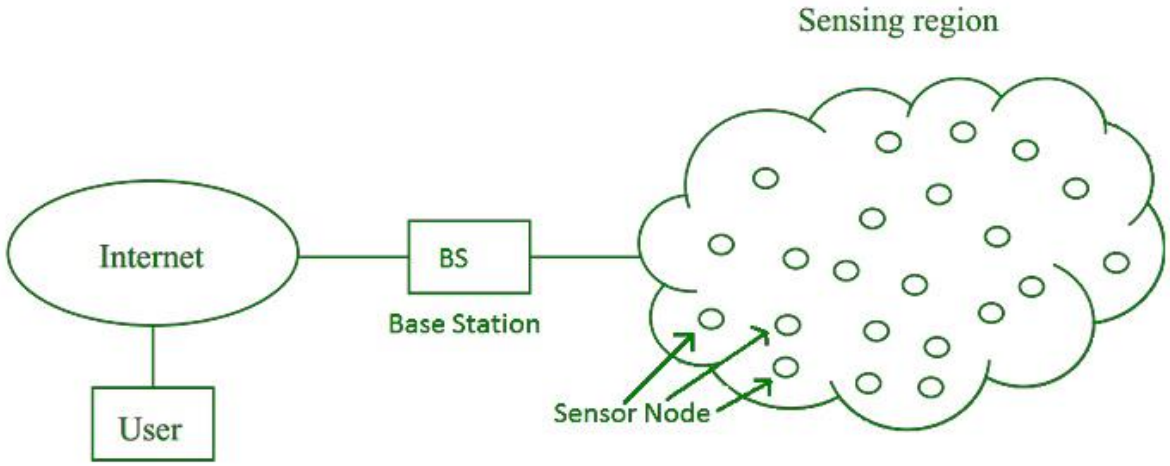
3. RFID Reader

RFID reader is one of the significant hardware component in the RFID system which read information from the RFID devices/tags and connected to the network to transfer the information to the database.

Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.
Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

8. Internet of Things (IOT)
9. Surveillance and Monitoring for security, threat detection
10. Environmental temperature, humidity, and air pressure
11. Noise Level of the surrounding

12. Medical applications like patient monitoring

13. Agriculture

14. Landslide Detection

Challenges of WSN:

9.Quality of Service

10. Security Issue

11. Energy Efficiency

12. Network Throughput

13. Performance

14. Ability to cope with node failure

15. Cross layer optimisation

16. Scalability to large scale of deployment

Components of WSN:

5. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.

6. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

7. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

8. **Evaluation Software:**
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Connecting Nodes:

To fully unleash all the possibilities that the Internet of Things (IoT) concept enables, a very large number of devices – more than 20 billion by 2020 – will be connected to the cloud. By using cloud services to collect and process data, user experience and convenience when interacting with any particular product or system can be greatly enhanced. Directly connecting nodes to the cloud to a range of commercially available platforms – including IBM Watson, Amazon's AWS or Microsoft Azure – and selecting IP-native wired and wireless connectivity technology, help minimize the infrastructure required to access each node. At ST, we have developed a range of solutions including pre-integrated cloud connectivity protocols, provisioning and upgrade libraries as well as Software Development Kits (SDK) to support architectures with nodes directly connected to Cloud to help developers create innovative connected devices and services.

Cellular Connected Nodes

Cellular is one of the long-range gateway-less wireless connectivity solutions for IoT, connecting devices to the cloud through telecom operator networks and infrastructure. Typical

example applications using 2G, 3G, 4G (including LTE) and today’s 5G

View application

Sigfox

Sigfox wireless connectivity employs a proprietary technology which uses the 868 MHz (Europe) and 902 MHz (US) frequencies in the Industrial, Scientific and Medical (ISM) radio band. It utilizes ultra-narrowband modulation to enable low-power wide-ar

View application

Wi-Fi Connected Nodes

Wi-Fi is a technology for wireless local area networking with devices based on the IEEE 802.11 standard and is a key technology within the IoT. Embedded developers can find here hardware and software development platforms to jumpstart their designs f

View application

Networking Nodes:

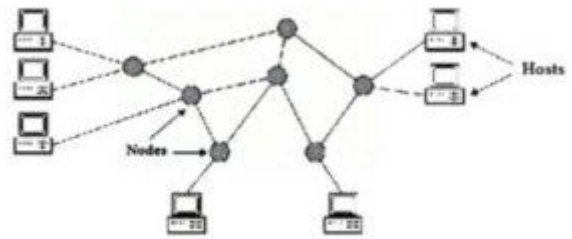
In Data Communication Systems, a network is an interconnecting point to exchange information between various communication components connected by various communication network links. If two or more network devices are connected to each other to transfer and share information and resources within a geographical area, then it is called a network. For example, a computer network is formed with multiple computers connected to transmit, exchange, share, store data, and resources. It enables communication for entertainment, business, and research. The computer network is built by using various hardware network nodes like bridges, routers, hubs, switches, etc, and communicating links like optical fiber cables, coaxial cables, wireless networks (LAN, WAN), etc. This article gives an overview of network nodes and their types in a computer network.

What is a Node in a Computer Network?

A node within a computer network is defined as, a connecting point or redistributed point or communicating point or joint, or a transfer point where the data can be stored, received, transmitted, or created. A node can be either a computer or any device that involves receiving and sending the data inside the computer networks. It is simply called a network node. The

link that connects the node of a network is known as a communication channel.

The network node is either a redistribution point or an endpoint that transmits the data with a recognizing, processing, and forwarding capability to other network nodes. To form a network connection for data transmission, 2 or multiple network nodes are needed. It depends on the type of network and the referred protocol layer.



Network Nodes

To receive access each node requires an IP address for identification. Examples of network nodes include printers, computers, modems, bridges, switches, etc. A network node is any device in the network that can transmit, process, recognize and store information to other networks.

If the node is referred to as data communication equipment, then it forms a connection for modems, hubs, bridges, switches, etc. If the

network node is data terminal equipment, then it acts as an endpoint for connecting printers, handsets, telephones, computers, etc.

Any device that is connected to the network contains a unique IP address or logical address, which is referred to as a node. The device manufacturers assigned a MAC address for every node on the network to a NIC (network interface controller) for data transmission and communication. The measure of several connections made by a network node with other nodes gives the degree of connectivity.

Types of Network Nodes

The network nodes concept adopted packet switching theory to transmit and receive the data through different routes in a distributed network. There are different types of network nodes based on the application and function.

End Nodes

These are referred to as the initial point or an endpoint for communication. Examples of end nodes are computers, security, cameras, printers, and many more.

Intermediary Nodes

The nodes are located in between the initial (starting) point or an endpoint of the end nodes of the computer network. Examples of intermediary nodes are bridges, routers, switches, cell towers, etc.

Data Communications

The network nodes are the physical devices that are located in between DTE (data terminal equipment) and data communication circuits. Bridges, switches, hubs, and modems are included to execute the conversion of signals, line clocks, and coding. In data communications, devices like digital telephones, host computers, printers, routers, servers act as data terminal equipment.

Internet and intranet network nodes: these types of nodes are nothing but host computers, which are identified by an IP address. Some of the data link layer devices and WLAN access points don’t contain any IP address and they are referred to as physical network nodes or LAN nodes.

LAN and WAN network nodes: these types of network nodes are the physical devices that are involved in performing particular functions and also every node contains a specific MAC address for NIC (network interface card). The examples are modems, access points of WLAN, and PCs. If

the device is offline, then there would be a loss of function of the node.

Telecommunication Nodes

These types of nodes in fixed telephone networks might be private or public to exchange the information or a computer that provides intelligent network service. While in cellular networks, include base station controllers to control multiple base stations. Since the cellular network base stations are not referred to as nodes.

Cable TV Network Nodes

These types of nodes are related to fiber optic cables, which connect businesses, homes distributed by common fiber optic receivers within a specified geographical location. The fiber optic node in cable systems determines the number of businesses and homes are connected by a particular fiber node.

Distributed Network Nodes

These types of nodes are servers, clients, and peers. In distributed networks, some virtual nodes are used to maintain data transparency.

Example of Network Nodes

The best examples of network nodes are discussed below.

Switches

The network devices that operate at the data link layer of the OSI model to forward, send, and receive the data frames/packets over the entire network are called switches. A switch is a multiple port device, in which multiple computers or network devices can be plugged in. It performs error checking and examines the destination address when the data frame arrives at any port or node of the network and forwards it with efficiency to the selected port or node.

A switch can divide the Collision domain of hosts and the broadcast domain remains the same. It supports all modes of communications such as unicast, multicast, and broadcast. It uses packet-switching technology and utilizes the MAC address to send and receive the data frames from source to destination.

The mode of transmission is full-duplex and communication is bidirectional. The switches are active devices with network management capability. Error checking is done before forwarding of data. There are 4 types of switches.

- Unmanaged switches: most widely used in home networks
- Manages switches: used complex and large networks of various organizations.
- LAN switches: connects internal LAN of a business or organization
- PoE switches (power over Ethernet switches): can receive power and data frame over the same line on the Ethernet network.

Bridges

The network devices that operate at the data link layer of the OSI model and connect two or multiple LANs to form a single larger Local Area Network (LAN) are called bridges. The process of aggregating the local area networks is known as bridging the network. It connects two or multiple segments or components of the same local area network.

They are referred to as layer 2 switches. They are usually called repeaters, which can filter the data by reading the MAC address of destination and source. They are 2 port devices, that contain a single input and output port. It can interconnect two local area networks, which are operating on the same protocol.

When multiple LANs are joined together to form a single LAN, the capacity of the network will increase. The data frame is passed to the node and then discarded, if it contains a destination MAC address in the same network. The data frame will be forwarded towards the network if it contains the destination MAC address in the connected network. If the MAC address is not available, then the bridge broadcasts the data frames to every network node. There are 2 types of bridges. They are,

- Transparent bridge: unaware of the existence of a bridge in the network and performs two processes like bridge forward and bridge learn.

- Source routing bridge: source station and the data from specifies the route to be followed.

WSN and IOT:

Wireless Sensor Networks (WSN) and the Internet of Things (IoT)

- Wireless Sensor Networks (WSN) are used to monitor and collect data from physical or environmental conditions.
    - Whereas the Internet of Things is used to connect devices and objects to the

internet so they can communicate with each other and exchange data.

- Wireless sensor networks typically consist of a large number of small, low-power sensors that wirelessly transmit data to a central base station
    - whereas the Internet of Things (IoT) typically consists of a smaller number of devices that are connected to the internet via wired or wireless connections.
- Wireless sensor networks are often used for monitoring purposes in difficult or dangerous environments.
    - whereas the Internet of Things is used to connect a variety of devices and objects in more everyday settings.
- Wireless sensor networks are often designed to operate in specific environments for a specific purpose.
    - whereas the Internet of Things is designed to be more general and versatile.
- Wireless sensor networks often use proprietary protocols and technologies

    - whereas the Internet of Things relies on standard protocols such as TCP/IP.

- Wireless sensor networks are typically deployed and operated by a single organization.
    - whereas the Internet of Things is more decentralized, with a variety of organizations and individuals involved.

- Wireless sensor networks are often closed systems, with data being collected and used by the deploying organization
    - whereas the Internet of Things is more open, with data being shared and used by a variety of organizations and individuals.

- Wireless sensor networks are typically static, with sensors being deployed in a specific location and remaining in that location
    - whereas the Internet of Things is more dynamic, with devices and objects being moved around and connected to different networks.

- Wireless sensor networks are typically used for data collection and monitoring.

    - whereas the Internet of Things is used for a variety of purposes, including data collection, monitoring, control, and communication.

- The wireless sensor network market is still emerging
    - whereas the Internet of Things market is more mature.

I hope, this article would help you to know about the 10 main differences between WSN and the IoT.

[The Internet of things (IoT)]

2.

    1. The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.

    2. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

All sensor data is further processed and analyzed in the data analyzing

Short Answer Questions:

1.What is Sensor?

2.What is Raspberripi Development kit?

3.Explain about RFID?

4.Explain about WSN(Wireless sensor networks)?

Long Answer Questions:

1.What are the types of sensors and actuators?

2.Explain about connecting nodes and network nodes in detail?

3.Explain about RFID principles and components?

4.Explain about IOT Development Boards?

UNIT-3

WIRELESS TECHNOLOGIES FOR IOT

WPAN Technologies For IoT/M2M:

A PAN (also known as a WPAN) is a network used for communication among intelligent gadgets that are physically close to a person (including smartphones, tablets, body monitors, and so on). PANs can be used to support wireless body area networks (WBANs) (also known as wireless medical body area networks (WMBANs) and medical body area network systems (MBANSs). Still, they can also be used to support other applications. Medical uses include vital sign monitoring, respiration monitoring, electrocardiography (ECG), pH monitoring, glucose monitoring, disability assistance, muscular tension monitoring, and artificial limb support, among others. WBANs' nonmedical applications include video streaming, data transfer, entertainment, and gaming.

A PAN's range is usually a few meters. The gadgets in question are sometimes referred to as short-range devices (SRDs). PANs can be used to communicate among personal devices (intrapersonal communication) or to connect to a higher-level network, such as the Internet. The following table highlights a rough comparison of three wireless technologies, highlighting the features of BANs/WBANs. WBAN technology can, to varying degrees, meet the following significant needs that the healthcare industry considers essential.

S.No.	Sr.No	WBAN	WSN	Cellular Wireless Networks
01.	Traffic	Application-specific	Sporadic/cyclic, modest data rate	Multimedia, high data rate
02.	Topology	Dynamic	Random, dynamic	Few infrastructures changes
03.	Configuration/ maintenance	Some flexibility Specialists are needed	Self-configurable, unattended operation	Managed by large organizations/ carriers
04.	Standardization	Multiple (IEEE) standards especiall	Relatively little standardization	Multiple international standards, ITU-T, ETSI, etc.

S.No.	Sr.No	WBAN	WSN	Cellular Wireless Networks
		y at lower layers		

The following are the key wireless technologies and concepts that support IoT/M2M applications:

- **3GPP:** 3GPP brings together six telecommunications standard bodies, known as “organisational partners,” and offers a stable environment for their members to generate the reports and specifications that define 3GPP technologies. These technologies are constantly advancing through what has come to be recognised as commercial cellular/mobile system generations.3GPP was originally the standards collaboration that was advancing Global System for Mobile Communication (GSM) platforms toward 3G. However, 3GPP has been the main point for mobile systems beyond 3G since the completion of the initial LTE and the Evolved Packet Core (EPC) specifications. 3GPP Release 10 and later are compliant with the most recent ITU-R specifications for IMT-

Advanced “Systems beyond 3G.” The standard currently enables high-mobility communication at speeds of up to 100 Mbps and low-mobility communication at speeds of up to 1 Gbps. The original mission of 3GPP was to develop Technical Specifications and Technical Reports for a 3G Mobile System based on evolved GSM CNs and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) in both frequency division duplex (FDD) and time division duplex (TDD) modes). The scope was later expanded to encompass the upkeep and development of GSM Technical Specifications and Technical Reports, as well as advanced radio access technologies (e.g., GPRS and EDGE). All GSM (including GPRS and EDGE), W-CDMA, and LTE (including LTE-Advanced) specifications are included in the term “3GPP specification”.

- **3GPP2 (Third-Generation Partnership Project 2):** 3GPP2 is a collaborative 3G telecommunications specification-setting project that includes North American and Asian interests in developing global specifications for ANSI/TIA/EIA-41 Cellular Radio telecommunication Intersystem Operations network evolution to 3G, as well as global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 encompasses

HS, broadband, and Internet protocol (IP)-based mobile systems with network-to-network interconnection and feature/service transparency, global roaming, and location-independent services, thanks to the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" effort.

- **6LoWPAN: IPv6 over low-power area networks (IEEE 802.15.4):** 6LoWPAN Based on RFC 4944, 6LoWPAN is currently a generally acknowledged method for running IP on 802.15.4.TinyOS, Contiki, and protocols such as ISA100 and ZigBee SE 2.0 all support it. RFC 4944 disguises 802.15.4 as an IPv6 link. It provides simple encapsulation and efficient 100-byte packet representation. It covers themes such as:
    - The first approach to stateless header compression
    - Datagram tag/datagram offset
    - Mesh forwarding
    - Identify originator/final destination
    - Minimal use of complex MAC layer concepts

- **ANT/ANT+:** Dynastream’s sensor company created ANTTM, a low-power proprietary wireless technology, in 2004. The technology runs on the 2.4 GHz frequency band. ANT devices can run for years on a single coin cell. The purpose of ANT is to connect sports and fitness sensors to a display device. ANT+TM expands the ANT protocol and allows devices to communicate in a controlled network. As a prerequisite for adopting ANT+ branding, ANT+ recently launched a new certification process.

- **Bluetooth:** Bluetooth is a Personal Area Network (PAN) technology that is based on IEEE 802.15.1. It is a short-range wireless communication specification for portable personal devices that was created by Ericsson. The Bluetooth SIG made their specifications public in the late 1990s, at which point the IEEE 802.15 Group took over and established a vendor-independent standard based on the Bluetooth work. IEEE 802.15 sublayers include

    - RF layer
    - baseband layer
    - link manager
    - L2CAP

- Bluetooth has progressed through four iterations, with all Bluetooth standards remaining downwardly compatible. BLE is a subset of Bluetooth v4.0 that includes a completely new protocol stack for the speedy establishment of basic links.BLE is an alternative to the “power management” features introduced as part of the standard Bluetooth protocols in Bluetooth v1.0 to v3.0 (Bluetooth is a trademark of the Bluetooth Alliance, a commercial organisation that certifies the interoperability of specific devices designed to the respective IEEE standard).

- **EDGE (Enhanced Data Rates for Global Evolution):** GSMTM radio access technology has been improved to deliver faster bit rates for data applications, both circuit and packet-switched. EDGE is accomplished as an upgrade to the existing GSM PHY layer, rather than as a distinct, standalone specification, by updates to the existing layer 1 specifications. EDGE, in addition to improving data rates, is transparent to the service offerings at the upper levels, although it is an enabler for HS circuit-switched data (HSCSD) and upgraded GPRS (EGPRS). For example, GPRS can provide a data rate of 115 Kbps, while EDGE can raise this to 384 Kbps. This is comparable to the rate for early Wideband Code Division

Multiple Access (W-CDMA) implementations, prompting some parties to view EDGE as a 3G technology rather than a 2G (EDGE systems can meet the ITU's IMT-2000 specifications with a capability of 384 Kbps).EDGE is commonly seen as a link between the two generations: a sort of 2.5G.

- **LTE (Long Term Evolution):** LTE is a 3GPP initiative to transition UMTS technology to 4G. LTE can be considered as an architecture framework and a set of auxiliary mechanisms aimed at delivering smooth IP communication between UE and the packet (IPv4, IPv6) data network during mobility with no disruption to end-user applications. In contrast to previous-generation cellular networks' circuit-switched models, LTE is designed to offer solely packet-switched services.

- **NFC (Near Field Communication):** A set of standards for devices such as PDAs, cellphones, and tablets that enable the establishment of wireless communication when they are within a few inches of each other. These standards cover communications protocols as well as data interchange formats; they are based on existing RFID standards such as ISO/IEC 14443 and FeliCa (a contactless RFID smart card technology developed by Sony that is

used in electronic money cards in Japan, for example). ISO/IEC 18092, as well as other standards defined by the NFC Forum, are examples of NFC standards. NFC standards enable two-way communication between endpoints (previous generation systems were exclusively one-way). Unpowered NFC-based tags can also be read by NFC devices, hence this technology can be used in place of prior one-way systems. NFC applications include contactless transactions.

- **Satellite systems:** Satellite communication is so important in commercial, TV/media, government, and military communications, because of their inherent multicast/broadcast capabilities, mobility features, and worldwide reach, dependability, and capacity to respond rapidly Open-space and/or adverse environment connectivity Satellite communications is a LOS one-way or two-way RF transmission. a transmission system made of a transmitting station (uplink) A satellite system that serves as a signal regenerator.

UMTS (Universal Mobile Telecommunications System) :

UMTS is a 3G mobile cellular technology that supports voice and data (IP) networks and is

based on the GSM standard produced by the 3GPP.

- **Very small aperture terminal (VSAT):** A complete end-user terminal (usually with a tiny 4–5 ft antenna) meant to communicate with other terminals in a satellite-delivered data IP-based network, typically in a "star" arrangement via a hub. These services typically include contention and/or traffic engineering. The hub or network operator will control the system and present charges based on data throughput or another type of usage. VSATs are used in a wide range of remote applications and are designed to be low-cost.

- **Wi-Fi:** WLANs based on the IEEE 802.11 family of protocols, including 802.11a, 802.11b, 802.11g, and 802.11n.

- **WiMAX:** The WiMAX Forum, which was founded in June 2001 to promote adherence and interoperability of the IEEE 802.16 standard, defines WiMAX as Worldwide Interoperability for Microwave Access. WiMAX is defined by the WiMAX Forum as "a standards-based technology that enables the delivery of last-mile wireless broadband connectivity as an alternative to cable and DSL."

- **Wireless Meter-Bus (M-Bus):** The Wireless M-Bus standard (EN 13757–4:2005)specifies the communication between water, gas, heat, and electric metres and is becoming increasingly popular in Europe for smart metering or AMI applications. Wireless M-Bus will operate in the 868 MHz band (from 868 MHz to 870 MHz); this band offers good trade-offs between RF range and antenna size. Chip manufacturers, such as Texas Instruments, typically offer both single-chip (SoC) and two-chip solutions for Wireless M-Bus.

- **ZigBee RF4CE specification:** The purpose-driven specification was created for basic, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities provided by ZigBee 2007. Because ZigBee RF4CE has lower memory size requirements, it can be implemented at a lower cost. The straightforward device-to-device topology facilitates development and testing, resulting in a shorter time to market. ZigBee RF4CE is a multivendor interoperable consumer electronics solution that features a simple, resilient, and low-cost communication network enabling two-way wireless connectivity. The Alliance independently tests platforms that implement this specification through the ZigBee Certified programme and

maintains a list of ZigBee Compliant Platforms that enable ZigBee RF4CE.

- **ZigBee specification:** Based on IEEE 802.15.4, the basic ZigBee specification defines ZigBee's smart, cost-effective, and energy-efficient mesh network. It is a self-configuring, self-healing network of redundant, low-cost, very low-power nodes that enable ZigBee's unrivalled flexibility, mobility, and use. ZigBee comes in two feature sets: ZigBee PRO and ZigBee. Both feature sets govern how ZigBee mesh networks work. The most extensively used specification, ZigBee PRO, is designed for low power consumption and to enable huge networks with thousands of devices. (The ZigBee Alliance, a commercial group that validates the compatibility of individual devices designed to the corresponding IEEE standard, owns the trademark ZigBee.)

- **Z-wave:** Z-wave is a wireless ecosystem that promises to connect household electronics and the user through Remote Control (RC). It employs low-power radio waves that easily penetrate walls, floors, and cabinets. Z-wave control can be added to practically any electronic equipment.

IoT protocols:

The benefit and value of IoT comes from enabling the components to communicate; this ability to communicate is what moves data from endpoint devices through the IoT pipeline to central servers.

This communication happens via IoT protocols, which ensure that data sent from endpoint devices, such as sensors, is received and understood by the next and subsequent steps in the connected environment, whether the next step for that data is to another endpoint device or a gateway or an application.

Although protocols as a collective group are essential to making IoT work, protocols aren't all created equal. Not all protocols work, or work well, in every circumstance, according to Bill Ray, analyst and senior research director at Gartner.

Ray noted that some protocols work well for IoT use in buildings, some are well suited for IoT deployments spread among buildings and others work well for national or global IoT use cases.

How many protocols are there in IoT?

There are multiple IoT protocols available, with each one offering certain capabilities or combinations of features that make it preferable over other options for specific IoT deployments.

Each IoT protocol enables either device-to-device, device-to-gateway or device-to-cloud/data center communication -- or combinations of those communications.

Factors such as geographic and special location, power consumption needs, battery-operated options, the presence of physical barriers and cost determine which protocol is optimal in an IoT deployment.

What are the different layers of IoT architecture?

Networking systems are built as a stack of technologies; these are frequently visualized in a

reference model -- a type of framework -- that technologists use to conceptualize how data is communicated over the entire stack.

The most well-known one is the Open Systems Interconnection (OSI) model, which lists seven layers. From bottom to top, the layers are the following:

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

IoT is also expressed in a multilayer model. Although some use the OSI seven-layer model, others in use include the following:

- **three-layer model:** perception, network and application
- **four-layer model:** perception, support, network and application

- **five-layer model:** perception, transport, processing, application and business, *or* physical, data link, network, transport and application

Internet protocols in use generally vary by layer. As such, an IoT ecosystem could have multiple protocols, with different protocols enabling communication at different layers and with some protocols bridging across layers, said Scott Young, principal research advisor for infrastructure at Info-Tech Research Group.

For example, Bluetooth and wireless support communication at the lowest layers, while Data Distribution Service (DDS) and MQTT work in the application layer.

Most common protocols

Technologists can select from multiple communication protocols when building a network to serve their IoT ecosystem. The most common include the following.

1. AMQP

Short for Advanced Message Queuing Protocol, AMQP is an open standard protocol used for more message-oriented middleware. As such, it enables messaging interoperability between systems, regardless of the message brokers or

platforms being used. It offers security and interoperability, as well as reliability, even at a distance or over poor networks. It supports communications, even when systems aren't simultaneously available.

2. Bluetooth and BLE

Bluetooth is a short-range wireless technology that uses short-wavelength, ultrahigh-frequency radio waves. It had most commonly been used for audio streaming, but it has also become a significant enabler of wireless and connected devices. As a result, this low-power, low-range connectivity option is a go-to for both personal area networks and IoT deployments.

Another option is Bluetooth Low Energy, known as either Bluetooth LE or BLE, which is a new version optimized for IoT connections. True to its name, BLE consumes less power than standard Bluetooth, which makes it particularly appealing in many use cases, such as health and fitness trackers and smart home devices on the consumer side and for in-store navigation on the commercial side.

3. Cellular

Cellular is one of the most widely available and well-known options available for IoT applications, and it is one of the best options for deployments

where communications range over longer distances. Although 2G and 3G legacy cellular standards are now being phased out, telecommunications companies are rapidly expanding the reach of newer high-speed standards -- namely, 4G/LTE and 5G. Cellular provides high bandwidth and reliable communication. It's capable of sending high quantities of data, which is an important capability for many IoT deployments. However, those features come at a price: higher cost and power consumption than other options.

4. CoAP

The Internet Engineering Task Force Constrained RESTful Environments Working Group in 2013 launched CoAP, for Constrained Application Protocol, having designed it to work with HTTP-based IoT systems. CoAP relies on User Datagram Protocol to establish secure communications and enable data transmission between multiple points. Often used for machine-to-machine (M2M) applications, CoAP enables constrained devices to join an IoT environment, even with the presence of low bandwidth, low availability and/or low-energy devices.

5. DDS

Object Management Group (OMG) developed Data Distribution Service for real-time systems.

OMG describes DDS as "a middleware protocol and API standard for data-centric connectivity," explaining that "it integrates the components of a system together, providing low-latency data connectivity, extreme reliability and a scalable architecture that business and mission-critical IoT applications need." This M2M standard enables high-performance and highly scalable real-time data exchange using a publish-subscribe pattern.

6. LoRa and LoRaWAN

LoRa, for long range, is a noncellular wireless technology that, as its name describes, offers long-range communication capabilities. It's low power with secure data transmission for M2M applications and IoT deployments. A proprietary technology, it's now part of Semtech's radio frequency platform. The LoRa Alliance, of which Semtech was a founding member, is now the governing body of LoRa technology. The LoRa Alliance also designed and now maintains LoRaWAN, an open cloud-based protocol that enables IoT devices to communicate LoRa.

7. LWM2M

OMA SpecWorks describes its Lightweight M2M (LWM2M) as "a device management protocol designed for sensor networks and the demands of an M2M environment." This communication

protocol was designed specifically for remote device management and telemetry in IoT environments and other M2M applications; as such, it's a good option for low-power devices with limited processing and storage capabilities.

8. MQTT

Developed in 1999 and first known as Message Queuing Telemetry Transport, it's now just MQTT. There is no longer any message queueing in this protocol. MQTT uses a publish-subscribe architecture to enable M2M communication. Its simple messaging protocol works with constrained devices and enables communication between multiple devices. It was designed to work in low-bandwidth situations, such as for sensors and mobile devices on unreliable networks. That capability makes it a commonly preferred option for connecting devices with a small code footprint, as well as for wireless networks with varying levels of latency stemming from bandwidth constraints or unreliable connections. MQTT, which started as a proprietary protocol, is now the leading open source protocol for connecting IoT and industrial IoT devices.

9. Wi-Fi

Given its pervasiveness in home, commercial and industrial buildings, Wi-Fi is a frequently used IoT

protocol. It offers fast data transfer and is capable of processing large amounts of data. Wi-Fi is particularly well suited within LAN environments, with short- to medium-range distances. Moreover, Wi-Fi's multiple standards -- the most common in homes and some businesses being 802.11n -- give technologists options for deployment. However, many Wi-Fi standards, including the one commonly used in homes, is too power-consuming for some IoT use cases, particularly low-power/battery-powered devices. That limits Wi-Fi as an option for some deployments. Additionally, Wi-Fi's low range and low scalability also limit its feasibility for use in many IoT deployments.

10. XMPP

Dating back to the early 2000s when the Jabber open source community first designed its Extensible Messaging and Presence Protocol for real-time human-to-human communication, XMPP is now used for M2M communication in lightweight middleware and for routing XML data. XMPP supports the real-time exchange of structured but extensible data between multiple entities on a network, and it's most often used for consumer-oriented IoT deployments, such as smart appliances. It's an open source protocol supported by the XMPP Standards Foundation.

11. Zigbee

Zigbee is a mesh network protocol that was designed for building and home automation applications, and it's one of the most popular mesh protocols in IoT environments. A short-range and low-power protocol, Zigbee can be used to extend communication over multiple devices. It has a longer range than BLE, but it has a lower data rate than BLE. Overseen by the Zigbee Alliance, it offers a flexible, self-organizing mesh, ultralow power and a library of applications.

12. Z-Wave

Another proprietary option, Z-Wave is a wireless mesh network communication protocol built on low-power radio frequency technology. Like Bluetooth and Wi-Fi, Z-Wave lets smart devices communicate with encryption, thereby providing a level of security to the IoT deployment. It's commonly used for home automation products and security systems, as well as in commercial applications, such as energy management technologies. It operates on 908.42 MHz radio frequency in the U.S.; although, its frequencies vary country by country. Z-Wave is supported by the Z-Wave Alliance, a member consortium focused on expanding the technology and interoperability of devices that use Z-Wave.

Choosing the right IoT protocol

No single IoT communications protocol is best, nor is any one right for every deployment.

Rather, enterprise technologists must determine which protocol will be best for their organizations based on the unique circumstances of their planned IoT deployments, said Scott Laliberte, managing director and global leader of the Emerging Technology Group with the consulting firm Protiviti. Those determinations should weigh a range of factors, from the power needs of the connected devices and the location of those devices, to the geographic size and features where the deployment will be situated, to the deployment's security requirements.

Edge connectivity and Protocol:

Edge Computing Architecture

An Edge Computing Architecture comprises of the following components

Data source/devices

The data sources in an edge computing environment can be applications capturing data, sensors, appliances, or any data capturing device. Data generated by these devices is different depending upon the source. Data sources vary from one another depending upon their functionalities and locations. The various edge devices capture data and communicate via IoT protocols, sending data to the edge gateways. The protocols used for the data transfer can be Ethernet, Bluetooth, Wi-Fi, NFC, ZigBee, etc. In short every data generating device will be considered as an edge device.

Edge gateway

An edge gateway acts as a node between edge devices and a core network. A core network comprises devices powerful enough to pre-process data. Edge gateways are employed to provide interfaces to wired and radio-based transmissions.

The various standards used are:

- **Z-Wave:** Z-Wave is used for 30 meters point-to-point communication and is specified for applications that involve small transmissions like household appliance control applications. Z-Wave functions in ISM bands (around 900 MHz) and allows a transmission rate of 40 kbps. Z-wave is

considered to be the best possible option available for household appliances communication.

- **LTE-A (Long Term Evolution—Advanced):** This communication protocol comprises of a set of various protocols meant for communication that fall under Machine-Type signals and IoT based architectures. In terms of service cost and scalability, it outperforms other cellular solutions.

- **EPC-global:** Electronic Product Code is used in the supply chain management to identify items, as a unique identification number stored on an RFID tag. The architecture uses RFID technologies along with easy to use RFID tags as well as readers for information sharing.This architecture is recognized as a promising technique for the future of the IoT because of the features of openness, scalability, etc

- **Bluetooth Low Energy:** Bluetooth Low-Energy (BLE) or Bluetooth Smart makes use of radio signals with short-range and a minimum power requirement. It operates at a range that is nearly about ten times more than classic Bluetooth technology. Its latency factor compared to classic Bluetooth technology is 15 times less. The transmission

power between 0.01 mW to 10 mW is feasible for its operation.

Protocols used

The Various Protocols used in this Layer

CoAP

CoAP is an application layer protocol for edge devices and applications, created by IETF Constrained RESTful Environments (CoRE) working group. The CoAP proposes a transfer protocol based on Representational State Transfer (REST) on top of HTTP functionalities. REST is a cacheable connection protocol that relies on the stateless client-server architecture. It represents a proper way to exchange data between clients and servers on top of HTTP. It is used in mobile-based social network applications and it makes complexity less by using HTTP methods(get, post, put, and delete).

MQTT

MQTT is used to make a connection between embedded devices, networks with services as well as middleware. The connection operation is based on a routing mechanism and makes MQTT as the best possible connection protocol for both IoT and M2M. MQTT is built on top of the TCP protocol and is suitable for devices with low

resource availability, unreliable or low bandwidth links. MQTT simply consists of three components, subscriber, publisher, and a broker.

AMQP

AMQP focuses on message-oriented environments and is an open standard application layer protocol. It provides reliable Communication through message delivery guarantee primitives which include at-most-once, at-least-once and exactly-once delivery. TCP is used as a reliable protocol for message exchange.

Edge

an edge-computing architecture simply means the edge of the network. The devices present at the edge of the network vary based upon the functionalities. A mobile phone can be employed at the edge. A router can be employed at the edge of the network etc. Edge comprises of those devices which can perform temporary data processing and temporary storage before sending the actual data to the cloud for further storage and processing. The communication between an edge device and an edge is facilitated by an edge gateway. Edge provides data computing capabilities nearer to the source of data. Edge is a demarcation between the core network and the rest of the network

in an edge computing environment. It just acts as an interface to connect the edge architecture with either fog domain or cloud environment. The devices which are employed at the edge should be capable of providing storage and computing services. The edge of a network can be at a distance from the actual edge device. In most of the cases, depending upon the response time and bandwidth available, the edge can be just a hop distance from the main edge device, collecting the data.

Short Answer Questions:

1.What is WPAN technology?

2.Explain about Zigbee,HART?

3.Explain about REST,AMPQ protocols?

4.What are the IP based protocols?

Long Answer Questions:

1.Explain about WPAN technologies in detail?

2.What are the IP based protocols and explain in detail?

3.Explain about Edge connectivity and protocols?

1.What are the types of sensors and actuators?

2.Explain about connecting nodes andsss network nodes in detail?

3.Explain about RFID principles and components?

4.Explain about IOT Development Boards?

UNIT-3

WIRELESS TECHNOLOGIES FOR IOT

WPAN Technologies For IoT/M2M:

A PAN (also known as a WPAN) is a network used for communication among intelligent gadgets that are physically close to a person (including smartphones, tablets, body monitors, and so on). PANs can be used to support wireless body area networks (WBANs) (also known as wireless medical body area networks (WMBANs) and medical body area network systems (MBANSs). Still, they can also be used to support other applications.

Medical uses include vital sign monitoring, respiration monitoring, electrocardiography (ECG), pH monitoring, glucose monitoring, disability assistance, muscular tension monitoring, and artificial limb support, among others. WBANs' nonmedical applications include video streaming, data transfer, entertainment, and gaming.

A PAN's range is usually a few meters. The gadgets in question are sometimes referred to as short-range devices (SRDs). PANs can be used to communicate among personal devices (intrapersonal communication) or to connect to a higher-level network, such as the Internet. The following table highlights a rough comparison of three wireless technologies, highlighting the features of BANs/WBANs. WBAN technology can, to varying degrees, meet the following significant needs that the healthcare industry considers essential.

S.No.	Sr.No	WBAN	WSN	Cellular Wireless Networks
01.	Traffic	Application-specific	Sporadic/cyclic, modest data rate	Multimedia, high data rate
02.	Topology	Dynamic	Random, dynamic	Few infrastructures changes
03.	Configuration/ maintenance	Some flexibility Specialists are needed	Self-configurable, unattended operation	Managed by large organizations/ carriers
04.	Standardization	Multiple (IEEE) standards especially at lower layers	Relatively little standardization	Multiple international standards, ITU-T, ETSI, etc.

The following are the key wireless technologies and concepts that support IoT/M2M applications:

- **3GPP:** 3GPP brings together six telecommunications standard bodies, known as "organisational partners," and offers a stable environment for their members to generate the reports and specifications that define 3GPP technologies. These technologies are constantly advancing through what has come to be recognised as commercial cellular/mobile system generations.3GPP was originally the standards collaboration that was advancing Global System for Mobile Communication (GSM) platforms toward 3G. However, 3GPP has been the main point for mobile systems beyond 3G since the completion of the initial LTE and the Evolved Packet Core (EPC) specifications. 3GPP Release 10 and later are compliant with the most recent ITU-R specifications for IMT-Advanced "Systems beyond 3G." The standard currently enables high-mobility communication at speeds of up to 100 Mbps and low-mobility communication at speeds of up to 1 Gbps. The original mission of 3GPP was to develop Technical Specifications and Technical Reports for a 3G

Mobile System based on evolved GSM CNs and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) in both frequency division duplex (FDD) and time division duplex (TDD) modes). The scope was later expanded to encompass the upkeep and development of GSM Technical Specifications and Technical Reports, as well as advanced radio access technologies (e.g., GPRS and EDGE). All GSM (including GPRS and EDGE), W-CDMA, and LTE (including LTE-Advanced) specifications are included in the term "3GPP specification".

- **3GPP2 (Third-Generation Partnership Project 2):** 3GPP2 is a collaborative 3G telecommunications specification-setting project that includes North American and Asian interests in developing global specifications for ANSI/TIA/EIA-41 Cellular Radio telecommunication Intersystem Operations network evolution to 3G, as well as global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 encompasses HS, broadband, and Internet protocol (IP)-based mobile systems with network-to-network interconnection and feature/service transparency, global roaming, and location-independent services, thanks to the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" effort.
- **6LoWPAN: IPv6 over low-power area networks (IEEE 802.15.4):** 6LoWPAN Based on RFC 4944, 6LoWPAN is currently a generally acknowledged method for running IP on 802.15.4.TinyOS, Contiki, and protocols such as ISA100 and ZigBee SE 2.0 all support it. RFC 4944 disguises 802.15.4 as an IPv6 link. It provides simple encapsulation and efficient 100-byte packet representation. It covers themes such as:
    - The first approach to stateless header compression
    - Datagram tag/datagram offset
    - Mesh forwarding
    - Identify originator/final destination
    - Minimal use of complex MAC layer concepts
- **ANT/ANT+:** Dynastream's sensor company created ANTTM, a low-power proprietary wireless technology, in 2004. The technology runs on the 2.4 GHz frequency band. ANT devices can run for years on a single coin cell. The purpose of ANT is to connect sports and fitness sensors to a display device. ANT+TM expands the ANT protocol and allows devices to communicate in a controlled network. As a prerequisite for adopting ANT+ branding, ANT+ recently launched a new certification process.
- **Bluetooth:** Bluetooth is a Personal Area Network (PAN) technology that is based on IEEE 802.15.1. It is a short-range wireless communication specification for portable personal devices that was created by Ericsson. The Bluetooth SIG made their specifications public in the late 1990s, at which point the IEEE 802.15 Group took over and established a vendor-independent standard based on the Bluetooth work. IEEE 802.15 sublayers include
    - RF layer
    - baseband layer
    - link manager
    - L2CAP

- Bluetooth has progressed through four iterations, with all Bluetooth standards remaining downwardly compatible. BLE is a subset of Bluetooth v4.0 that includes a completely new protocol stack for the speedy establishment of basic links.BLE is an alternative to the “power management” features introduced as part of the standard Bluetooth protocols in Bluetooth v1.0 to v3.0 (Bluetooth is a trademark of the Bluetooth Alliance, a commercial organisation that certifies the interoperability of specific devices designed to the respective IEEE standard).
- **EDGE (Enhanced Data Rates for Global Evolution):** GSMTM radio access technology has been improved to deliver faster bit rates for data applications, both circuit and packet-switched. EDGE is accomplished as an upgrade to the existing GSM PHY layer, rather than as a distinct, standalone specification, by updates to the existing layer 1 specifications. EDGE, in addition to improving data rates, is transparent to the service offerings at the upper levels, although it is an enabler for HS circuit-switched data (HSCSD) and upgraded GPRS (EGPRS). For example, GPRS can provide a data rate of 115 Kbps, while EDGE can raise this to 384 Kbps. This is comparable to the rate for early Wideband Code Division Multiple Access (W-CDMA) implementations, prompting some parties to view EDGE as a 3G technology rather than a 2G (EDGE systems can meet the ITU’s IMT-2000 specifications with a capability of 384 Kbps).EDGE is commonly seen as a link between the two generations: a sort of 2.5G.
- **LTE (Long Term Evolution):** LTE is a 3GPP initiative to transition UMTS technology to 4G. LTE can be considered as an architecture framework and a set of auxiliary mechanisms aimed at delivering smooth IP communication between UE and the packet (IPv4, IPv6) data network during mobility with no disruption to end-user applications. In contrast to previous-generation cellular networks’ circuit-switched models, LTE is designed to offer solely packet-switched services.
- **NFC (Near Field Communication):** A set of standards for devices such as PDAs, cellphones, and tablets that enable the establishment of wireless communication when they are within a few inches of each other. These standards cover communications protocols as well as data interchange formats; they are based on existing RFID standards such as ISO/IEC 14443 and FeliCa (a contactless RFID smart card technology developed by Sony that is used in electronic money cards in Japan, for example). ISO/IEC 18092, as well as other standards defined by the NFC Forum, are examples of NFC standards. NFC standards enable two-way communication between endpoints (previous generation systems were exclusively one-way). Unpowered NFC-based tags can also be read by NFC devices, hence this technology can be used in place of prior one-way systems. NFC applications include contactless transactions.
- **Satellite systems:** Satellite communication is so important in commercial, TV/media, government, and military communications, because of their inherent multicast/broadcast capabilities, mobility features, and worldwide reach, dependability, and capacity to respond rapidly Open-space and/or adverse environment connectivity Satellite communications is a LOS one-way or two-way RF transmission. a transmission system made of a transmitting station (uplink) A satellite system that serves as a signal regenerator.

UMTS (Universal Mobile Telecommunications System) :

UMTS is a 3G mobile cellular technology that supports voice and data (IP) networks and is based on the GSM standard produced by the 3GPP.

- **Very small aperture terminal (VSAT):** A complete end-user terminal (usually with a tiny 4–5 ft antenna) meant to communicate with other terminals in a satellite-delivered data IP-based network, typically in a "star" arrangement via a hub. These services typically include contention and/or traffic engineering. The hub or network operator will control the system and present charges based on data throughput or another type of usage. VSATs are used in a wide range of remote applications and are designed to be low-cost.
- **Wi-Fi:** WLANs based on the IEEE 802.11 family of protocols, including 802.11a, 802.11b, 802.11g, and 802.11n.
- **WiMAX:** The WiMAX Forum, which was founded in June 2001 to promote adherence and interoperability of the IEEE 802.16 standard, defines WiMAX as Worldwide Interoperability for Microwave Access. WiMAX is defined by the WiMAX Forum as "a standards-based technology that enables the delivery of last-mile wireless broadband connectivity as an alternative to cable and DSL."
- **Wireless Meter-Bus (M-Bus):** The Wireless M-Bus standard (EN 13757–4:2005)specifies the communication between water, gas, heat, and electric metres and is becoming increasingly popular in Europe for smart metering or AMI applications. Wireless M-Bus will operate in the 868 MHz band (from 868 MHz to 870 MHz); this band offers good trade-offs between RF range and antenna size. Chip manufacturers, such as Texas Instruments, typically offer both single-chip (SoC) and two-chip solutions for Wireless M-Bus.
- **ZigBee RF4CE specification:** The purpose-driven specification was created for basic, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities provided by ZigBee 2007. Because ZigBee RF4CE has lower memory size requirements, it can be implemented at a lower cost. The straightforward device-to-device topology facilitates development and testing, resulting in a shorter time to market. ZigBee RF4CE is a multivendor interoperable consumer electronics solution that features a simple, resilient, and low-cost communication network enabling two-way wireless connectivity. The Alliance independently tests platforms that implement this specification through the ZigBee Certified programme and maintains a list of ZigBee Compliant Platforms that enable ZigBee RF4CE.
- **ZigBee specification:** Based on IEEE 802.15.4, the basic ZigBee specification defines ZigBee's smart, cost-effective, and energy-efficient mesh network. It is a self-configuring, self-healing network of redundant, low-cost, very low-power nodes that enable ZigBee's unrivalled flexibility, mobility, and use. ZigBee comes in two feature sets: ZigBee PRO and ZigBee. Both feature sets govern how ZigBee mesh networks work. The most extensively used specification, ZigBee PRO, is designed for low power consumption and to enable huge networks with thousands of devices. (The ZigBee Alliance, a commercial group that validates the compatibility of individual devices designed to the corresponding IEEE standard, owns the trademark ZigBee.)

- **Z-wave:** Z-wave is a wireless ecosystem that promises to connect household electronics and the user through Remote Control (RC). It employs low-power radio waves that easily penetrate walls, floors, and cabinets. Z-wave control can be added to practically any electronic equipment.

IoT protocols:

The benefit and value of IoT comes from enabling the components to communicate; this ability to communicate is what moves data from endpoint devices through the IoT pipeline to central servers.

This communication happens via IoT protocols, which ensure that data sent from endpoint devices, such as sensors, is received and understood by the next and subsequent steps in the connected environment, whether the next step for that data is to another endpoint device or a gateway or an application.

Although protocols as a collective group are essential to making IoT work, protocols aren't all created equal. Not all protocols work, or work well, in every circumstance, according to Bill Ray, analyst and senior research director at Gartner.

Ray noted that some protocols work well for IoT use in buildings, some are well suited for IoT deployments spread among buildings and others work well for national or global IoT use cases.

How many protocols are there in IoT?

There are multiple IoT protocols available, with each one offering certain capabilities or combinations of features that make it preferable over other options for specific IoT deployments.

Each IoT protocol enables either device-to-device, device-to-gateway or device-to-cloud/data center communication -- or combinations of those communications.

Factors such as geographic and special location, power consumption needs, battery-operated options, the presence of physical barriers and cost determine which protocol is optimal in an IoT deployment.

What are the different layers of IoT architecture?

Networking systems are built as a stack of technologies; these are frequently visualized in a reference model -- a type of framework -- that technologists use to conceptualize how data is communicated over the entire stack.

The most well-known one is the Open Systems Interconnection (OSI) model, which lists seven layers. From bottom to top, the layers are the following:

8. Physical
9. Data link
10. Network
11. Transport
12. Session
13. Presentation
14. Application

IoT is also expressed in a multilayer model. Although some use the OSI seven-layer model, others in use include the following:

- **three-layer model:** perception, network and application
- **four-layer model:** perception, support, network and application
- **five-layer model:** perception, transport, processing, application and business, *or* physical, data link, network, transport and application

Internet protocols in use generally vary by layer. As such, an IoT ecosystem could have multiple protocols, with different protocols enabling communication at different layers and with some protocols bridging across layers, said Scott Young, principal research advisor for infrastructure at Info-Tech Research Group.

For example, Bluetooth and wireless support communication at the lowest layers, while Data Distribution Service (DDS) and MQTT work in the application layer.

Most common protocols

Technologists can select from multiple communication protocols when building a network to serve their IoT ecosystem. The most common include the following.

1. AMQP

Short for Advanced Message Queuing Protocol, AMQP is an open standard protocol used for more message-oriented middleware. As such, it enables messaging interoperability between systems, regardless of the message brokers or platforms being used. It offers security and interoperability, as well as reliability, even at a distance or over poor networks. It supports communications, even when systems aren't simultaneously available.

2. Bluetooth and BLE

Bluetooth is a short-range wireless technology that uses short-wavelength, ultrahigh-frequency radio waves. It had most commonly been used for audio streaming, but it has also become a significant enabler of wireless and connected devices. As a result, this low-power, low-range connectivity option is a go-to for both personal area networks and IoT deployments.

Another option is Bluetooth Low Energy, known as either Bluetooth LE or BLE, which is a new version optimized for IoT connections. True to its name, BLE consumes less power than standard Bluetooth, which makes it particularly appealing in many use cases, such as health and fitness trackers and smart home devices on the consumer side and for in-store navigation on the commercial side.

3. Cellular

Cellular is one of the most widely available and well-known options available for IoT applications, and it is one of the best options for deployments where communications range over longer distances. Although 2G and 3G legacy cellular standards are now being phased out, telecommunications companies are rapidly expanding the reach of newer high-speed standards -- namely, 4G/LTE and 5G. Cellular provides high bandwidth and reliable communication. It's capable of sending high quantities of data, which is an important capability for many IoT deployments. However, those features come at a price: higher cost and power consumption than other options.

4. CoAP

The Internet Engineering Task Force Constrained RESTful Environments Working Group in 2013 launched CoAP, for Constrained Application Protocol, having designed it to work with HTTP-based IoT systems. CoAP relies on User Datagram Protocol to establish secure communications and enable data transmission between multiple points. Often used for machine-to-machine (M2M) applications, CoAP enables constrained devices to join an IoT environment, even with the presence of low bandwidth, low availability and/or low-energy devices.

5. DDS

Object Management Group (OMG) developed Data Distribution Service for real-time systems. OMG describes DDS as "a middleware protocol and API standard for data-centric connectivity," explaining that "it integrates the components of a system together, providing low-latency data connectivity, extreme reliability and a scalable architecture that business and mission-critical IoT applications need." This M2M standard enables high-performance and highly scalable real-time data exchange using a publish-subscribe pattern.

6. LoRa and LoRaWAN

LoRa, for long range, is a noncellular wireless technology that, as its name describes, offers long-range communication capabilities. It's low power with secure data transmission for M2M applications and IoT deployments. A proprietary technology, it's now part of Semtech's radio frequency platform. The LoRa Alliance, of which Semtech was a founding member, is now the governing body of LoRa technology. The LoRa

Alliance also designed and now maintains LoRaWAN, an open cloud-based protocol that enables IoT devices to communicate LoRa.

7. LWM2M

OMA SpecWorks describes its Lightweight M2M (LWM2M) as "a device management protocol designed for sensor networks and the demands of an M2M environment." This communication protocol was designed specifically for remote device management and telemetry in IoT environments and other M2M applications; as such, it's a good option for low-power devices with limited processing and storage capabilities.

8. MQTT

Developed in 1999 and first known as Message Queuing Telemetry Transport, it's now just MQTT. There is no longer any message queueing in this protocol. MQTT uses a publish-subscribe architecture to enable M2M communication. Its simple messaging protocol works with constrained devices and enables communication between multiple devices. It was designed to work in low-bandwidth situations, such as for sensors and mobile devices on unreliable networks. That capability makes it a commonly preferred option for connecting devices with a small code footprint, as well as for wireless networks with varying levels of latency stemming from bandwidth constraints or unreliable connections. MQTT, which started as a proprietary protocol, is now the leading open source protocol for connecting IoT and industrial IoT devices.

9. Wi-Fi

Given its pervasiveness in home, commercial and industrial buildings, Wi-Fi is a frequently used IoT protocol. It offers fast data transfer and is capable of processing large amounts of data. Wi-Fi is particularly well suited within LAN environments, with short- to medium-range distances. Moreover, Wi-Fi's multiple standards -- the most common in homes and some businesses being 802.11n -- give technologists options for deployment. However, many Wi-Fi standards, including the one commonly used in homes, is too power-consuming for some IoT use cases, particularly low-power/battery-powered devices. That limits Wi-Fi as an option for some deployments. Additionally, Wi-Fi's low range and low scalability also limit its feasibility for use in many IoT deployments.

10. XMPP

Dating back to the early 2000s when the Jabber open source community first designed its Extensible Messaging and Presence Protocol for real-time human-to-human communication, XMPP is now used for M2M communication in lightweight middleware and for routing XML data. XMPP supports the real-time exchange of structured but extensible data between multiple entities on a network, and it's most often used for consumer-oriented IoT deployments, such as smart appliances. It's an open source protocol supported by the XMPP Standards Foundation.

11. Zigbee

Zigbee is a mesh network protocol that was designed for building and home automation applications, and it's one of the most popular mesh protocols in IoT environments. A short-range and low-power protocol, Zigbee can be used to extend communication over multiple devices. It has a longer range than BLE, but it has a lower data rate than BLE. Overseen by the Zigbee Alliance, it offers a flexible, self-organizing mesh, ultralow power and a library of applications.

12. Z-Wave

Another proprietary option, Z-Wave is a wireless mesh network communication protocol built on low-power radio frequency technology. Like Bluetooth and Wi-Fi, Z-Wave lets smart devices communicate with encryption, thereby providing a level of security to the IoT deployment. It's commonly used for home automation products and security systems, as well as in commercial applications, such as energy management technologies. It operates on 908.42 MHz radio frequency in the U.S.; although, its frequencies vary country by country. Z-Wave is supported by the Z-Wave Alliance, a member consortium focused on expanding the technology and interoperability of devices that use Z-Wave.

Choosing the right IoT protocol

No single IoT communications protocol is best, nor is any one right for every deployment.

Rather, enterprise technologists must determine which protocol will be best for their organizations based on the unique circumstances of their planned IoT deployments, said Scott Laliberte, managing director and global leader of the Emerging Technology Group

with the consulting firm Protiviti. Those determinations should weigh a range of factors, from the power needs of the connected devices and the location of those devices, to the geographic size and features where the deployment will be situated, to the deployment's security requirements.

Edge connectivity and Protocol:

Edge Computing Architecture

An Edge Computing Architecture comprises of the following components

Data source/devices

The data sources in an edge computing environment can be applications capturing data, sensors, appliances, or any data capturing device. Data generated by these devices is different depending upon the source. Data sources vary from one another depending upon their functionalities and locations. The various edge devices capture data and communicate via IoT protocols, sending data to the edge gateways. The protocols used for the data transfer can be Ethernet, Bluetooth, Wi-Fi, NFC, ZigBee, etc. In short every data generating device will be considered as an edge device.

Edge gateway

An edge gateway acts as a node between edge devices and a core network. A core network comprises devices powerful enough to pre-process data. Edge gateways are employed to provide interfaces to wired and radio-based transmissions.

The various standards used are:

- **Z-Wave:** Z-Wave is used for 30 meters point-to-point communication and is specified for applications that involve small transmissions like household appliance control applications. Z-Wave functions in ISM bands (around 900 MHz) and allows a transmission rate of 40 kbps. Z-

wave is considered to be the best possible option available for household appliances communication.

- **LTE-A (Long Term Evolution—Advanced):** This communication protocol comprises of a set of various protocols meant for communication that fall under Machine-Type signals and IoT based architectures. In terms of service cost and scalability, it outperforms other cellular solutions.
- **EPC-global:** Electronic Product Code is used in the supply chain management to identify items, as a unique identification number stored on an RFID tag. The architecture uses RFID technologies along with easy to use RFID tags as well as readers for information sharing.This architecture is recognized as a promising technique for the future of the IoT because of the features of openness, scalability, etc
- **Bluetooth Low Energy:** Bluetooth Low-Energy (BLE) or Bluetooth Smart makes use of radio signals with short-range and a minimum power requirement. It operates at a range that is nearly about ten times more than classic Bluetooth technology. Its latency factor compared to classic Bluetooth technology is 15 times less. The transmission power between 0.01 mW to 10 mW is feasible for its operation.

Protocols used

The Various Protocols used in this Layer

CoAP

CoAP is an application layer protocol for edge devices and applications, created by IETF Constrained RESTful Environments (CoRE) working group. The CoAP proposes a transfer protocol based on Representational State Transfer (REST) on top of HTTP functionalities. REST is a cacheable connection protocol that relies on the stateless client-server architecture. It represents a proper way to exchange data between clients and servers on top of HTTP. It is used in mobile-based social

network applications and it makes complexity less by using HTTP methods(get, post, put, and delete).

MQTT

MQTT is used to make a connection between embedded devices, networks with services as well as middleware. The connection operation is based on a routing mechanism and makes MQTT as the best possible connection protocol for both IoT and M2M. MQTT is built on top of the TCP protocol and is suitable for devices with low resource availability, unreliable or low bandwidth links. MQTT simply consists of three components, subscriber, publisher, and a broker.

AMQP

AMQP focuses on message-oriented environments and is an open standard application layer protocol. It provides reliable Communication through message delivery guarantee primitives which include at-most-once, at-least-once and exactly-once delivery. TCP is used as a reliable protocol for message exchange.

Edge

an edge-computing architecture simply means the edge of the network. The devices present at the edge of the network vary based upon the functionalities. A mobile phone can be employed at the edge. A router can be employed at the edge of the network etc. Edge comprises of those devices which can perform temporary data processing and temporary storage before sending the actual data to the cloud for further storage and processing. The communication between an edge device and an edge is facilitated by an edge gateway. Edge provides data computing capabilities nearer to the source of data. Edge is a demarcation between the core network and the rest of the network in an edge computing environment. It just acts as an interface to connect the edge architecture with either fog domain or cloud environment. The devices which are employed at the edge should be capable of providing storage and computing services. The edge of a network can be at a distance

from the actual edge device. In most of the cases, depending upon the response time and bandwidth available, the edge can be just a hop distance from the main edge device, collecting the data.

Short Answer Questions:

1.What is WPAN technology?

2.Explain about Zigbee,HART?

3.Explain about REST,AMPQ protocols?

4.What are the IP based protocols?

Long Answer Questions:

1.Explain about WPAN technologies in detail?

2.What are the IP based protocols and explain in detail?

3.Explain about Edge connectivity and protocols?

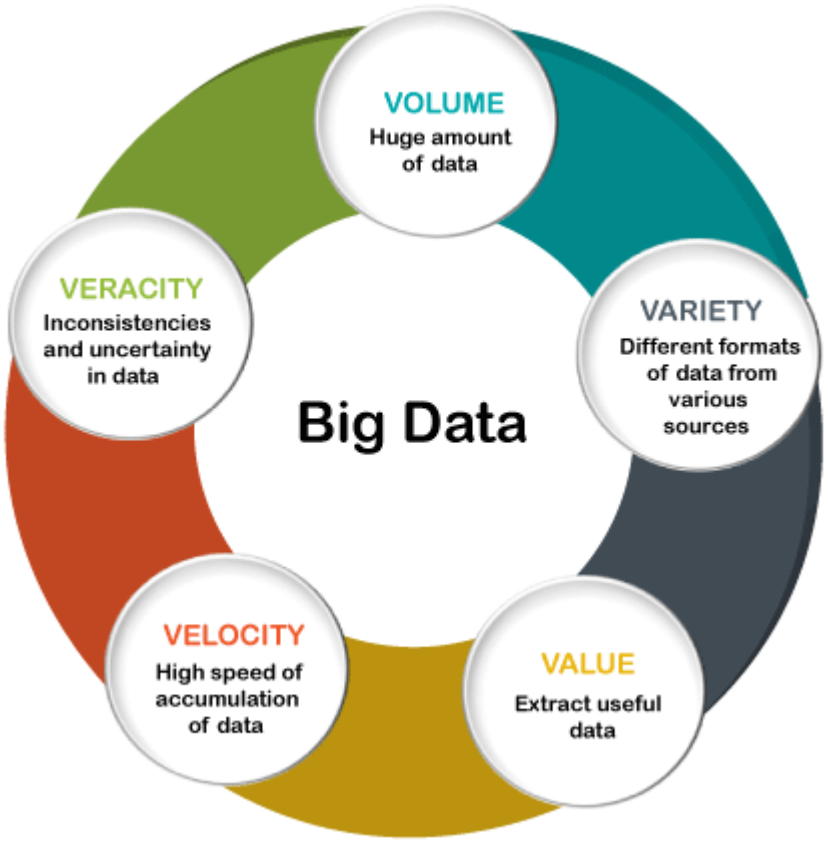
Unit 3

Data handling & Analytics

There are five v's of Big Data that explains the characteristics.

5 V's of Big Data

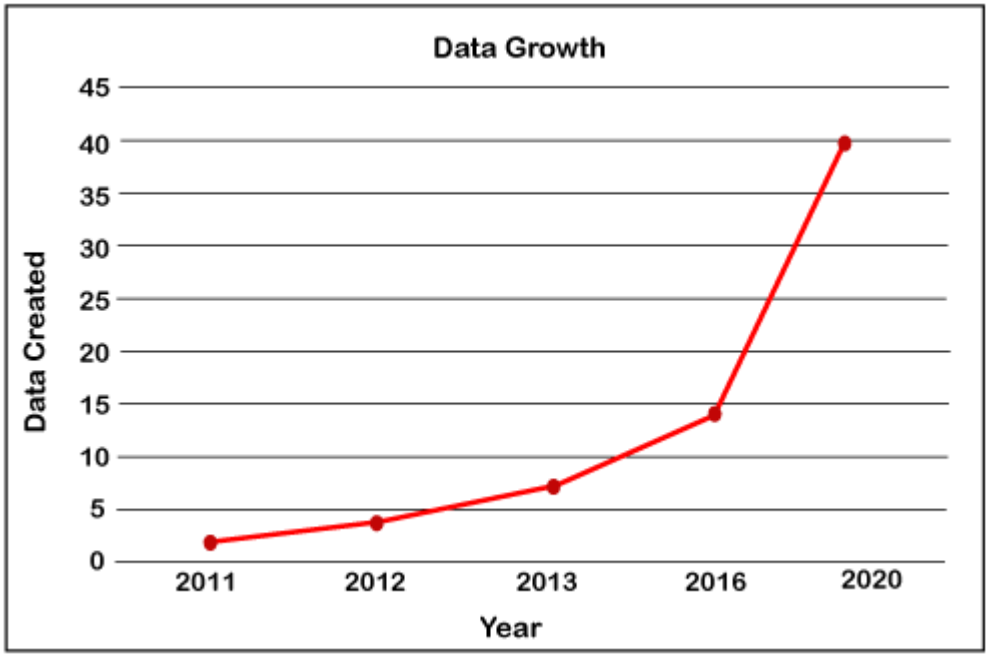
- **Volume**
- **Veracity**
- **Variety**
- **Value**
- **Velocity**



Volume

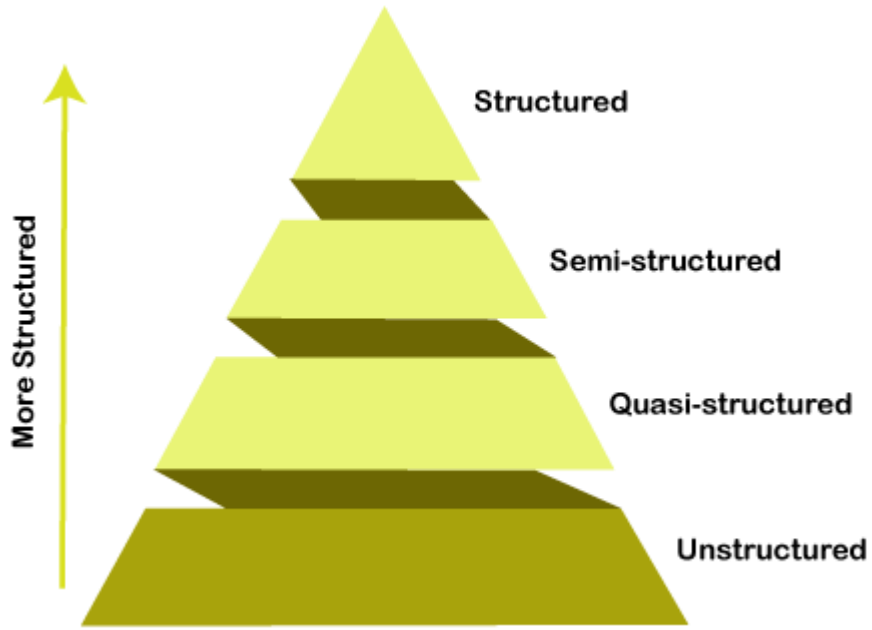
The name Big Data itself is related to an enormous size. Big Data is a vast 'volumes' of data generated from many sources daily, such as **business processes, machines, social media platforms, networks, human interactions,** and many more.

Facebook can generate approximately a **billion** messages, **4.5 billion** times that the "**Like**" button is recorded, and more than **350 million** new posts are uploaded each day. Big data technologies can handle large amounts of data.



Variety

Big Data can be **structured, unstructured, and semi-structured** that are being collected from different sources. Data will only be collected from **databases** and **sheets** in the past, But these days the data will comes in array forms, that are **PDFs, Emails, audios, SM posts, photos, videos,** etc.



The data is categorized as below:

a. **Structured data:** In Structured schema, along with all the required columns. It is in a tabular form. Structured Data is stored in the relational database management system.

b. **Semi-structured:** In Semi-structured, the schema is not appropriately defined, e.g., **JSON, XML, CSV, TSV**, and **email**. OLTP (**Online Transaction Processing**) systems are built to work with semi-structured data. It is stored in relations, i.e., **tables**.

c. **Unstructured Data**: All the **unstructured files, log files, audio files**, and **image** files are included in the unstructured data. Some organizations have much data available, but they did not know how to **derive** the value of data since the data is raw.

d. **Quasi-structured Data:**The data format contains textual data with inconsistent data formats that are formatted with effort and time with some tools.

Example: Web server logs, i.e., the log file is created and maintained by some server that contains a list of **activities**.

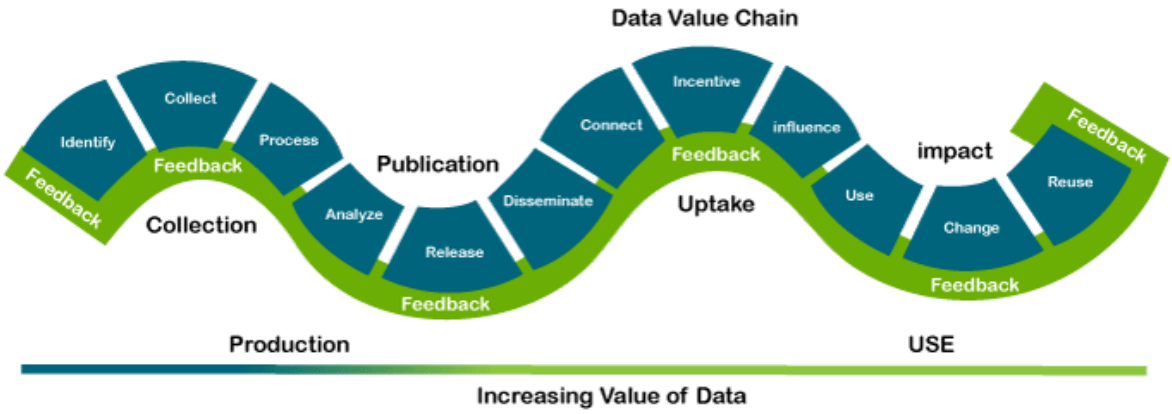
Veracity

Veracity means how much the data is reliable. It has many ways to filter or translate the data. Veracity is the process of being able to handle and manage data efficiently. Big Data is also essential in business development.

For example, **Facebook posts** with hashtags.

Value

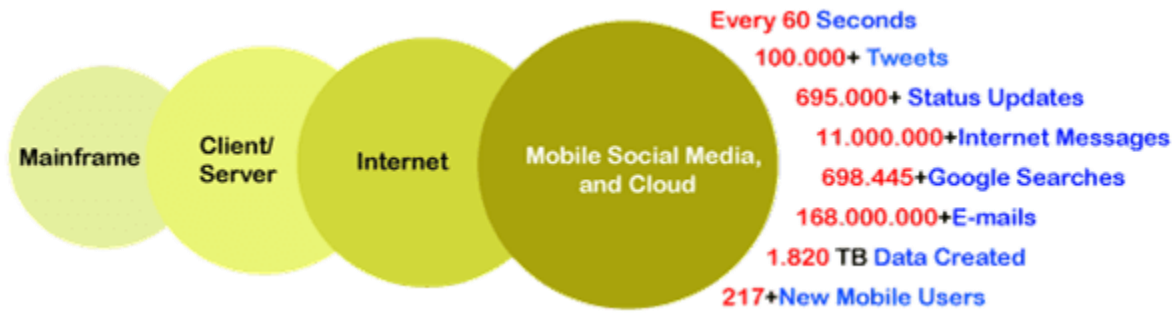
Value is an essential characteristic of big data. It is not the data that we process or store. It is **valuable** and **reliable** data that we **store, process**, and also **analyze**.



Velocity

Velocity plays an important role compared to others. Velocity creates the speed by which the data is created in **real-time**. It contains the linking of incoming **data sets speeds, rate of change**, and **activity bursts**. The primary aspect of Big Data is to provide demanding data rapidly.

Big data velocity deals with the speed at the data flows from sources like **application logs, business processes, networks, and social media sites, sensors, mobile devices,** etc.



- Data handling and technologies

Big Data Technologies

Before big data technologies were introduced, the data was managed by general programming languages and basic structured query languages. However, these languages were not efficient enough to handle the data because there has been continuous growth in each organization's information and data and the domain. That is why it became very important to handle such huge data and introduce an efficient and stable technology that takes care of all the client and large organizations' requirements and needs, responsible for data production and control. Big data technologies, the buzz word we get to hear a lot in recent times for all such needs.

In this article, we are discussing the leading technologies that have expanded their branches to help Big Data reach greater heights. Before we discuss big data technologies, let us first understand briefly about Big Data Technology.

What is Big Data Technology?

Big data technology is defined as software-utility. This technology is primarily designed to analyze, process and extract information from a large data set and a huge set of extremely complex structures. This is very difficult for traditional data processing software to deal with.

Among the larger concepts of rage in technology, big data technologies are widely associated with many other technologies such as deep learning, machine learning, artificial intelligence (AI), and Internet of Things (IoT) that are massively augmented. In combination with these technologies, big data technologies are focused on analyzing and handling large amounts of real-time data and batch-related data.

Types of Big Data Technology

Before we start with the list of big data technologies, let us first discuss this technology's board classification. Big Data technology is primarily classified into the following two types:

Operational Big Data Technologies

This type of big data technology mainly includes the basic day-to-day data that people used to process. Typically, the operational-big data includes daily basis data such as online transactions, social media platforms, and the data from any particular organization or a firm, which is usually needed for analysis using the software based on big data technologies. The data can also be referred to as raw data used as the input for several Analytical Big Data Technologies.

Some specific examples that include the Operational Big Data Technologies can be listed as below:

- Online ticket booking system, e.g., buses, trains, flights, and movies, etc.
- Online trading or shopping from e-commerce websites like Amazon, Flipkart, Walmart, etc.
- Online data on social media sites, such as Facebook, Instagram, Whatsapp, etc.
- The employees' data or executives' particulars in multinational companies.

Analytical Big Data Technologies

Analytical Big Data is commonly referred to as an improved version of Big Data Technologies. This type of big data technology is a bit complicated when compared with operational-big data. Analytical big data is mainly used when performance criteria are in use, and important real-time business decisions are made based on reports created by analyzing operational-real data. This means that the actual investigation of big data that is important for business decisions falls under this type of big data technology.

Some common examples that involve the Analytical Big Data Technologies can be listed as below:

- Stock marketing data
- Weather forecasting data and the time series analysis
- Medical health records where doctors can personally monitor the health status of an individual
- Carrying out the space mission databases where every information of a mission is very important

Top Big Data Technologies

We can categorize the leading big data technologies into the following four sections:

- Data Storage
- Data Mining
- Data Analytics
- Data Visualization

Data Storage

Let us first discuss leading Big Data Technologies that come under Data Storage:

- **Hadoop**: When it comes to handling big data, Hadoop is one of the leading technologies that come into play. This technology is based entirely on map-reduce architecture and is mainly used to process batch information. Also, it is capable

enough to process tasks in batches. The Hadoop framework was mainly introduced to store and process data in a distributed data processing environment parallel to commodity hardware and a basic programming execution model. Apart from this, Hadoop is also best suited for storing and analyzing the data from various machines with a faster speed and low cost. That is why Hadoop is known as one of the core components of big data technologies. The **Apache Software Foundation** introduced it in Dec 2011. Hadoop is written in Java programming language.

- **MongoDB**: MongoDB is another important component of big data technologies in terms of storage. No relational properties and RDBMS properties apply to MongoDb because it is a NoSQL database. This is not the same as traditional RDBMS databases that use structured query languages. Instead, MongoDB uses schema documents. The structure of the data storage in MongoDB is also different from traditional RDBMS databases. This enables MongoDB to hold massive amounts of data. It is based on a simple cross-platform document-oriented design. The database in MongoDB uses documents similar to JSON with the schema. This ultimately helps operational data storage options, which can be seen in most financial organizations. As a result, MongoDB is replacing traditional mainframes and offering the flexibility to handle a wide range of high-volume data-types in distributed architectures. **MongoDB Inc.** introduced MongoDB in Feb 2009. It is written with a combination of C++, Python, JavaScript, and Go language.
- **RainStor**: RainStor is a popular database management system designed to manage and analyze organizations' Big Data requirements. It uses deduplication strategies that help manage storing and handling vast amounts of data for reference. RainStor was designed in 2004 by a **RainStor Software Company**. It operates just like SQL. Companies such as Barclays and Credit Suisse are using RainStor for their big data needs.
- **Hunk**: Hunk is mainly helpful when data needs to be accessed in remote Hadoop clusters using virtual indexes. This helps us to use the spunk search processing language to analyze data. Also, Hunk allows us to report and visualize vast amounts of data from Hadoop and NoSQL data sources. Hunk was introduced in 2013 by **Splunk Inc**. It is based on the Java programming language.
- **Cassandra**: Cassandra is one of the leading big data technologies among the list of top NoSQL databases. It is open-source, distributed and has extensive column storage options. It is freely available and provides high availability without fail. This

ultimately helps in the process of handling data efficiently on large commodity groups. Cassandra's essential features include fault-tolerant mechanisms, scalability, MapReduce support, distributed nature, eventual consistency, query language property, tunable consistency, and multi-datacenter replication, etc. Cassandra was developed in 2008 by the **Apache Software Foundation** for the Facebook inbox search feature. It is based on the Java programming language.

Data Mining

Let us now discuss leading Big Data Technologies that come under Data Mining:

- Hadoop

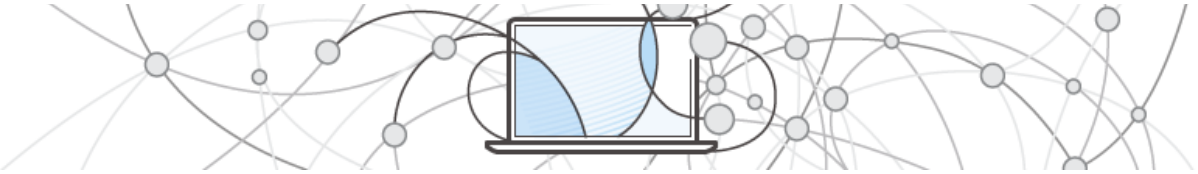
What is Hadoop?

Apache Hadoop is an open source framework that is used to efficiently store and process large datasets ranging in size from gigabytes to petabytes of data. Instead of using one large computer to store and process the data, Hadoop allows clustering multiple computers to analyze massive datasets in parallel more quickly.

Hadoop consists of four main modules:

- Hadoop Distributed File System (HDFS) – A distributed file system that runs on standard or low-end hardware. HDFS provides better data throughput than traditional file systems, in addition to high fault tolerance and native support of large datasets.

- Yet Another Resource Negotiator (YARN) – Manages and monitors cluster nodes and resource usage. It schedules jobs and tasks.
- MapReduce – A framework that helps programs do the parallel computation on data. The map task takes input data and converts it into a dataset that can be computed in key value pairs. The output of the map task is consumed by reduce tasks to aggregate output and provide the desired result.
- Hadoop Common – Provides common Java libraries that can be used across all modules.



How Hadoop Works

Hadoop makes it easier to use all the storage and processing capacity in cluster servers, and to execute distributed processes against huge amounts of data. Hadoop provides the building blocks on which other services and applications can be built.

Applications that collect data in various formats can place data into the Hadoop cluster by using an API operation to connect to the NameNode. The NameNode tracks the file directory structure and placement of “chunks” for each file, replicated across DataNodes. To run a job to query the data, provide a MapReduce job made up of many map and reduce tasks that run against the data in HDFS spread across the DataNodes. Map tasks run on each node against the input files supplied, and reducers run to aggregate and organize the final output.

The Hadoop ecosystem has grown significantly over the years due to its extensibility. Today, the Hadoop ecosystem includes

many tools and applications to help collect, store, process, analyze, and manage big data. Some of the most popular applications are:

- Spark – An open source, distributed processing system commonly used for big data workloads. Apache Spark uses in-memory caching and optimized execution for fast performance, and it supports general batch processing, streaming analytics, machine learning, graph databases, and ad hoc queries.
- Presto – An open source, distributed SQL query engine optimized for low-latency, ad-hoc analysis of data. It supports the ANSI SQL standard, including complex queries, aggregations, joins, and window functions. Presto can process data from multiple data sources including the Hadoop Distributed File System (HDFS) and Amazon S3.
- Hive – Allows users to leverage Hadoop MapReduce using a SQL interface, enabling analytics at a massive scale, in addition to distributed and fault-tolerant data warehousing.
- HBase – An open source, non-relational, versioned database that runs on top of Amazon S3 (using EMRFS) or the Hadoop Distributed File System (HDFS). HBase is a massively scalable, distributed big data store built for random, strictly consistent, real-time access for tables with billions of rows and millions of columns.
- Zeppelin – An interactive notebook that enables interactive data exploration.

Running Hadoop on AWS

Amazon EMR is a managed service that lets you process and analyze large datasets using the latest versions of big data processing frameworks such as Apache Hadoop, Spark, HBase, and Presto on fully customizable clusters.

- Easy to use: You can launch an Amazon EMR cluster in minutes. You don't need to worry about node provisioning, cluster setup, Hadoop configuration, or cluster tuning.
- Low cost: Amazon EMR pricing is simple and predictable: You pay an hourly rate for every instance hour you use and you can leverage Spot Instances for greater savings.
- Elastic: With Amazon EMR, you can provision one, hundreds, or thousands of compute instances to process data at any scale.
- Transient: You can use EMRFS to run clusters on-demand based on HDFS data stored persistently in Amazon S3. As jobs finish, you can shut down a cluster and have the data saved in Amazon S3. You pay only for the compute time that the cluster is running.
- Secure: Amazon EMR uses all common security characteristics of AWS services:
  - Identity and Access Management (IAM) roles and policies to manage permissions.
  - Encryption in-transit and at-rest to help you protect your data and meet compliance standards, such as HIPAA.
  - Security groups to control inbound and outbound network traffic to your cluster nodes.
  - AWS CloudTrail: Audit all Amazon EMR PI calls made in your account to provide security analysis, resource change tracking, and compliance auditing.

- Data analytics

Types of Data Analytics

Data analytics is broken down into four basic types.

1. **Descriptive analytics:** This describes what has happened over a given period of time. Have the number of views gone up? Are sales stronger this month than last?
2. **Diagnostic analytics:** This focuses more on why something happened. This involves more diverse data inputs and a bit of hypothesizing. Did the weather affect beer sales? Did that latest marketing campaign impact sales?
3. **Predictive analytics:** This moves to what is likely going to happen in the near term. What happened to sales the last time we had a hot summer? How many weather models predict a hot summer this year?
4. **Prescriptive analytics:** This suggests a course of action. If the likelihood of a hot summer is measured as an average of these five weather models is above 58%, we should add an evening shift to the brewery and rent an additional tank to increase output.

Data analytics underpins many quality control systems in the financial world, including the ever-popular Six Sigma program. If you aren't properly measuring something—whether it's your weight or the number of defects per million in a production line—it is nearly impossible to optimize it.

Some of the sectors that have adopted the use of data analytics include the travel and hospitality industry, where turnarounds can be quick. This industry can collect customer data and figure out where the problems, if any, lie and how to fix them.

Healthcare combines the use of high volumes of structured and unstructured data and uses data analytics to make quick decisions. Similarly, the retail industry uses copious amounts of data to meet the ever-changing demands of shoppers. The information retailers collect and analyze can help them identify trends, recommend products, and increase profits.

As of December 2021, the average total for a data analyst in the United States was just over $93,000.2

Data Analytics Techniques

There are several different analytical methods and techniques data analysts can use to process data and extract information. Some of the most popular methods are listed below.

- **Regression analysis** entails analyzing the relationship between dependent variables to determine how a change in one may affect the change in another.

- **Factor analysis** entails taking a large data set and shrinking it to a smaller data set. The goal of this maneuver is to attempt to discover hidden trends that would otherwise have been more difficult to see.
- **Cohort analysis** is the process of breaking a data set into groups of similar data, often broken into a customer demographic. This allows data analysts and other users of data analytics to further dive into the numbers relating to a specific subset of data.
- **Monte Carlo simulations** model the probability of different outcomes happening. Often used for risk mitigation and loss prevention, these simulations incorporate multiple values and variables and often have greater forecasting capabilities than other data analytics approaches.
- **Time series analysis** tracks data over time and solidifies the relationship between the value of a data point and the occurrence of the data point. This data analysis technique is usually used to spot cyclical trends or to project financial forecasts.

Data Analytics Tools

In addition to a broad range of mathematical and statistical approaches to crunching numbers, data analytics has rapidly evolved in technological capabilities. Today, data analysts have a broad range of software tools to help acquire data, store information, process data, and report findings.

Data analytics has always had loose ties to spreadsheets and Microsoft Excel. Now, data analysts also often interact with raw programming languages to transform and manipulate databases. Open-source languages such as Python are often utilized. More specific tools for data analytics like R can be used for statistical analysis or graphical modeling.

Data analysts also have help when reporting or communicating findings. Both Tableau and Power BI are data visualization and analysis tools to compile information, perform data analytics, and distribute results via dashboards and reports.

Other tools are also emerging to assist data analysts. SAS is an analytics platform that can assist with data mining, while Apache Spark is an open-source platform useful for processing large sets of data. Data analysts now have a broad range of technological capabilities to further enhance the value they deliver to their company.

Why Is Data Analytics Important?

Data analytics is important because it helps businesses optimize their performances. Implementing it into the business model means companies can help reduce costs by identifying more efficient ways of doing business. A company can also use data analytics to make better business decisions and help analyze customer trends and satisfaction, which can lead to new—and better—products and services.

What Are the 4 Types of Data Analytics?

Data analytics is broken down into four basic types. Descriptive analytics describes what has happened over a given period. Diagnostic analytics focuses more on why something happened. Predictive analytics moves to what is likely going to happen in the near term. Finally, prescriptive analytics suggests a course of action.

Who Is Using Data Analytics?

Data analytics has been adopted by several sectors, such as the travel and hospitality industry, where turnarounds can be quick. This industry can collect customer data and figure out where the problems, if any, lie and how to fix them. Healthcare is another sector that combines the use of high volumes of structured and unstructured data and data analytics can help in making quick decisions. Similarly, the retail industry uses copious amounts of data to meet the ever-changing demands of shoppers.

The Bottom Line

In a world increasingly becoming reliant on information and gathering statistics, data analytics helps individuals and organizations make sure of their data. Using a variety of tools and techniques, a set of raw numbers can be transformed into informative, educational insights that drive decision-making and thoughtful management.

ARTICLE SOURCES

Related Terms

Predictive Analytics: Definition, Model Types, and Uses

Predictive analytics is the use of statistics and modeling techniques to determine future performance based on current and historical data.

more

What Is Prescriptive Analytics? How It Works and Examples

Prescriptive analytics makes use of machine learning to help businesses decide a course of action, based on a computer program's

- Loacal analytics

Local analysis method is **the simplest method of determining connections**. Taking a small neighborhood into consideration, for example 3*3 or 5*5, we connect the similar points in this neighborhood to form a boundary of some common properties.

- Edge/Fog computing

Now we know that fog computing is an extra layer between the edge layer and the cloud layer. What are the benefits of having that extra layer? The initial benefit is efficiency of data traffic and a reduction in latency. By implementing a fog layer, the data that the cloud receives for your specific embedded application is a lot less cluttered. Where a cloud would have to first weed through a pile of unnecessary data before taking any action or returning results, it can now act directly upon the data that it receives from the fog layer.

When looking at the bigger picture, there are a lot more benefits. The amount of storage you would need for your cloud application would be a lot lower. That is because the cloud would only store and process relevant data. The data transfer would be faster as well. That is because the volume of data being sent to the cloud is significantly reduced.

What are the disadvantages of Fog Computing?

One thing that should be clear, is that fog computing can't replace edge computing. However, edge computing can definitely live without fog computing. Thus, the downside is that fog computing requires an investment. It is a more complex system that needs to be integrated with your current infrastructure. This costs money, time, but also knowledge about the best solution for your infrastructure. Fog computing isn't an ideal solution in every scenario. But, for some applications, the benefits may be attractive for those currently using a direct edge to cloud data architecture.

Do you use the same Hardware in both Fog Computing and Edge Computing?

In terms of hardware and the type of computers you can use, you can easily use an Edge Server for the same purpose as a Fog Server. The difference is in where

and how data is being collected and processed, not necessarily the hardware features and capabilities. If you take the Karbon 700 Expanded High-Performance Rugged Edge Computer for example, which was initially designed for Edge Computing, it would be just as suitable for Fog Computing. Of course, every project is unique. It's important to have a clear view of your overall project requirements when selecting and configuring any hardware solution.

Fog computing vs Edge computing in a nutshell

In a nutshell, edge computing is data computation that happens at the network's edge, in close proximity to the physical location creating the data. On the other hand, fog computing acts as a mediator between the edge and the cloud for various purposes, such as data filtering. In the end, fog computing can't replace edge computing, while edge computing can live without fog computing in many applications.

- Short answers

  What are Characteristics of big data?

  What is Data handling Technologies?

  What is Flow of data?

  Explain Data analytics, types of data analytics?

  What is Loacal analtics?

- Long answers

  Explain data storage ?

  Write about Hadoop?

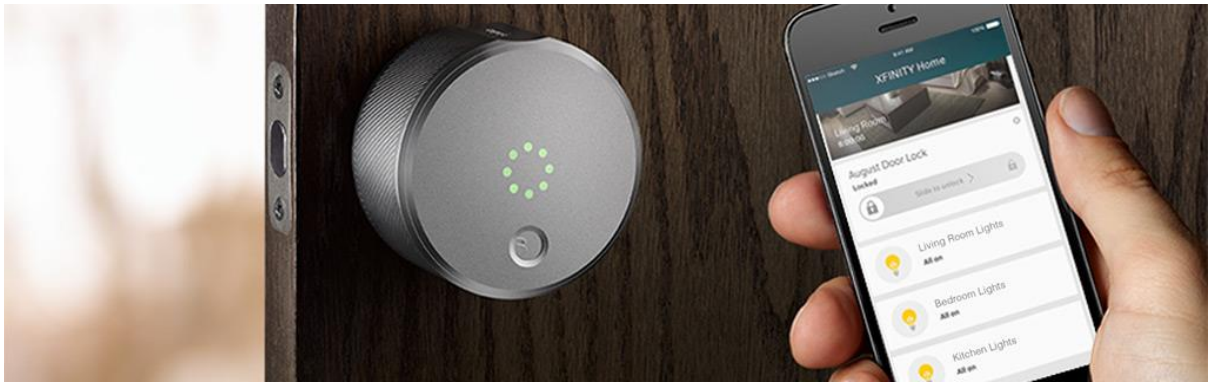
  Write about edge/fog computing?

Unit 5

Applications of iot

- What is home automation?

What is Home Automation?



- Share on Facebook
- Share on Twitter
- Share on E-Mail

“Home automation” refers to the automatic and electronic control of household features, activity, and appliances. In simple terms, it means you can easily control the utilities and features of your home via the Internet to make life more convenient and secure, and even spend less on household bills. Read on to find answers to some of the most common questions about home automation technology, and get a few ideas for home automation solutions to incorporate in your home.

How does home automation work?

Home automation is a network of hardware, communication, and electronic interfaces that work to integrate everyday devices with one another via the Internet. Each device has sensors and is connected through WiFi, so you can manage them from your smartphone or tablet whether you’re at home, or miles away. This allows you to turn on the lights, lock the front door, or even turn down the heat, no matter where you are.

There are three main elements of a home automation system: sensors, controllers, and actuators.

- Sensors can monitor changes in daylight, temperature, or motion detection. Home automation systems can then adjust those settings (and more) to your preferences.
- Controllers refer to the devices — personal computers, tablets or smartphones — used to send and receive messages about the status of automated features in your home.

- Actuators may be light switches, motors, or motorized valves that control the actual mechanism, or function, of a home automation system. They are programmed to be activated by a remote command from a controller.

What features are available through home automation systems?

Home automation systems offer a variety of services and functions. Some of the more common features available through these platforms include:

- Fire and carbon monoxide monitoring
- Remote lighting control
- Thermostat control
- Appliance control
- Home automation security systems and cameras
- Live video surveillance
- Alarm systems
- Real-time text and email alerts
- Digital personal assistant integration
- Keyless entry
- Voice-activated control

What are the benefits of home automation?

The purpose of a home automation system is to streamline how your home functions. Consider some of these benefits:

- Remote access: Control your home from mobile devices, including your laptop, tablet, or smartphone.
- Comfort: Use home automation to make your home a more comfortable, livable space. Preprogram your thermostat with your preferred settings so that your home is always at a comfortable temperature, set up smart speakers to play music when you get home from work, or adjust your lights to soften or brighten based on the time of day.
- Convenience: Program devices to turn on automatically at certain times, or access their settings remotely from anywhere with an Internet connection. When you don't have to remember to lock the door behind you or switch off the lights, you can turn your attention to more important things.
- Increased safety: Smart fire detectors, carbon monoxide monitors, pressure sensors, and other home automation security features can help protect your home from disaster.
- Energy efficiency: Home automation allows you to be more mindful of your power

- Industrial of iot

Industrial IoT (IIoT) brings machines, cloud computing, analytics, and people together to improve the performance and productivity of industrial processes. With IIoT, industrial companies can digitize processes, transform business models, and improve performance and productivity, while decreasing waste. These asset intensive companies operating in a range of industries such as manufacturing, energy, agriculture, transportation and utilities, are working on IoT projects that connect billions of devices and deliver value across a variety of use cases including predictive quality and maintenance analytics, asset condition monitoring, and process optimization.

A typical industrial facility has thousands of sensors generating data. With IIoT, manufacturers, for example, can combine machine data from a single line, factory, or a network of sites, such as manufacturing plants, assembly facilities, and refineries, to proactively improve performance by identifying potential bottlenecks, failures, gaps in production processes, and quality issues before they happen. Combining data from a network of sites can also result in a more efficient control of material flow, early detection and identification and elimination of production or supply bottlenecks, and the optimized operation of machinery and equipment in all facilities.
AWS IoT for the Industrial Internet of Things (1:56)

Leading companies choose AWS IoT, see how Volkswagen are building the Industrial Cloud (7:57)

Industrial IoT Use Cases

Predictive Quality

Predictive quality analytics extracts actionable insights from industrial data sources such as manufacturing equipment, environmental conditions, and human observations to optimize the quality of factory output. Using AWS IoT, industrial manufacturers can build predictive quality models which help them build better products. Higher quality products increase customer satisfaction and reduce product recalls.

See the infographic »

See the Reference Architecture »

Asset Condition Monitoring

Asset condition monitoring captures the state of your machines and equipment to determine asset performance. With AWS IoT, you can capture all IoT data, such as temperature, vibration, and error codes that indicate if equipment is performing optimally. With increased visibility, you can maximize the utilization and investment of your asset.

See the infographic »

See the Reference Architecture »

Predictive Maintenance

Predictive maintenance analytics captures the state of industrial equipment to identify potential breakdowns before they impact production, resulting in an increase in equipment lifespan, worker safety, and the supply chain optimization. With AWS IoT, you can continuously monitor and infer equipment status, health

- Applications of iot

In a world where home automation is being explored more and more by the day, perhaps you have always dreamed of residing in a fully connected household that offers a level of control and comfort that is quite beyond the imagination. The secret to how this dream home (actually a giant sensor) works? The internet of things!

The internet of things (IoT) is essentially a set of physical objects including sensors, software, and other technological devices to connect and exchange data with other devices and systems.

A rising number of digital devices share data by communicating via the internet, wherever you are in the world. What's more, these devices can be controlled remotely with ease through a user interface or even a smartphone. Do read this blog to get the lowdown on what IoT is all about.

In today's blog, I'd like to share some glimpses into the applications of IoT in smart homes and smart cities. Let's delve in and get started with the role IoT plays in smart homes!

- Applications of iot in retail management,logistics

Here's a big number: $1.6 trillion. That's how much the Internet-of-Things-enabled market could be worth by 2025. As more and more businesses adopt IoT technology, one highly affected area has been the sector of retail. IoT is being used to improve a variety of products and services across the retail and commerce industry — from warehousing and equipment maintenance to supply chain management and, of course, shopping itself.

TOP IOT IN RETAIL EXAMPLES

- Personalized retail marketing and content delivery.
- Optimal staffing level indicators.
- Cashierless payment systems.
- Movement tracking systems for optimal store setup.
- IoT-enabled warehouse robots.

- Wireless shipment tracking devices.
- Real-time condition monitoring of goods.
- Inventory management tools.
- In-store buyer behavior tracking.

"With the growth of the internet of things, customers will enjoy an increasingly connected or 'smart' shopping experience through a network of connections linking the physical and digital worlds into an ecosystem of devices, including vehicles, stores and software," Walmart CEO Doug McMillon has written. "The internet of things, drones, delivery robots, 3D-printing and self-driving cars will allow retailers to further automate and optimize supply chains too. Both sides of the equation – demand and supply – will change dramatically."

These retail and retail adjacent sectors are being transformed by the ongoing and ever-evolving IoT revolution.

- Iot design Ethics

Ethical Design of Internet of Things (IoT)

This post is for Professor Darakhshan Mir's class of Computer and Society. The post is based on the reading material [1][2] and the discussion in class.

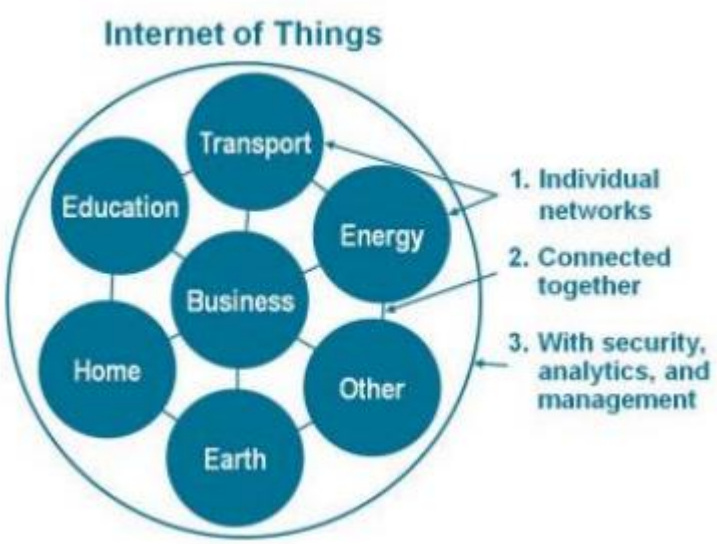


Figure 1. IoT Can Be Viewed as a Network of Networks. [1]

Introduction

The term **Internet of Things (IoT)** represents electrical or electronic devices, of varying sizes and capabilities, that are connected to the Internet. As applications and usage of the Internet expand on a daily basis, IoT appears as a new approach to incorporate the Internet into the generality of personal, professional and societal life. As shown in Figure 1, IoT has a wide scope of applications and can be used to interconnect various disparate networks [1].

The fast development of IoT technique and its widespread has brought privacy risks due to the large amount of data collected and processed by the "Things". Baldini's work [2] introduces the concept of **Ethical Design** as a new approach for users's interaction with IoT. Ethical Design of IoT allows users to select specific sets of policies, which can be tailored according to users' capabilities and to

the contexts where they operate, and thus provides a wider control over personal data and the IoT services.

In this post, I discuss the model and main challenges for Ethical Design of IoT, followed by the ethical analysis of privacy risks of IoT and potential problems with the Ethical Design model.

Discussion

Challenges for IoT

The main challenge of IoT is the trade-off between businesses needs to collect and process data and rights to privacy [2]. The economic incentives for data protection of the user are not directed to the user; instead it is limited to the businesses creating the IoT applications and devices. And the developers and manufacturers would prefer the IoT applications to collect users' data rather than to protect it because of the benefits of data collection, and the cost of implementing data protection solutions. Therefore, the poor application of security and privacy for IoT services is not because of technical reasons, but comes from the economic conflict between different stakeholders: users and entrepreneurs.

In addition, the IoT users' choices respect to privacy and other ethical issues are affected by multiple factors [2]. By the work of Acquisti and Grossklags [4], incomplete information on the consequences of an action, for instance the consequence of data disclosure, can hamper the privacy decision of users. Also the psychological biases may force users to make wrong decisions. For

example, the perception of immediate benefits (e.g., free access to an IoT service) can bring long-term negative impact (e.g., increase of privacy risk).

Model of Ethical Design

The concept of **Ethical Design** refers to the IoT products which are designed and deployed to empower users in controlling and protecting their personal data. There are many choices in IoT implementation, such as what kind of data can be accessed, collected or used by the company, and what specific functionality is preferred. Such choices are normally embedded in the algorithm of IoT products as a result of the decision of programmers and developers, and Ethical Design would make these decisions directly available to the user [2]. In this way, users would be able to establish and freely shape their value-laden choices while interacting within the IoT. Figure 2 below is a sample Graphical User Interface (GUI) for an Ethical Design of a security IoT system. It shows that the health information (e.g., heart rate) of users is usually “protected” and restricted only to authenticated and authorized doctors, and is available only in emergency situations.

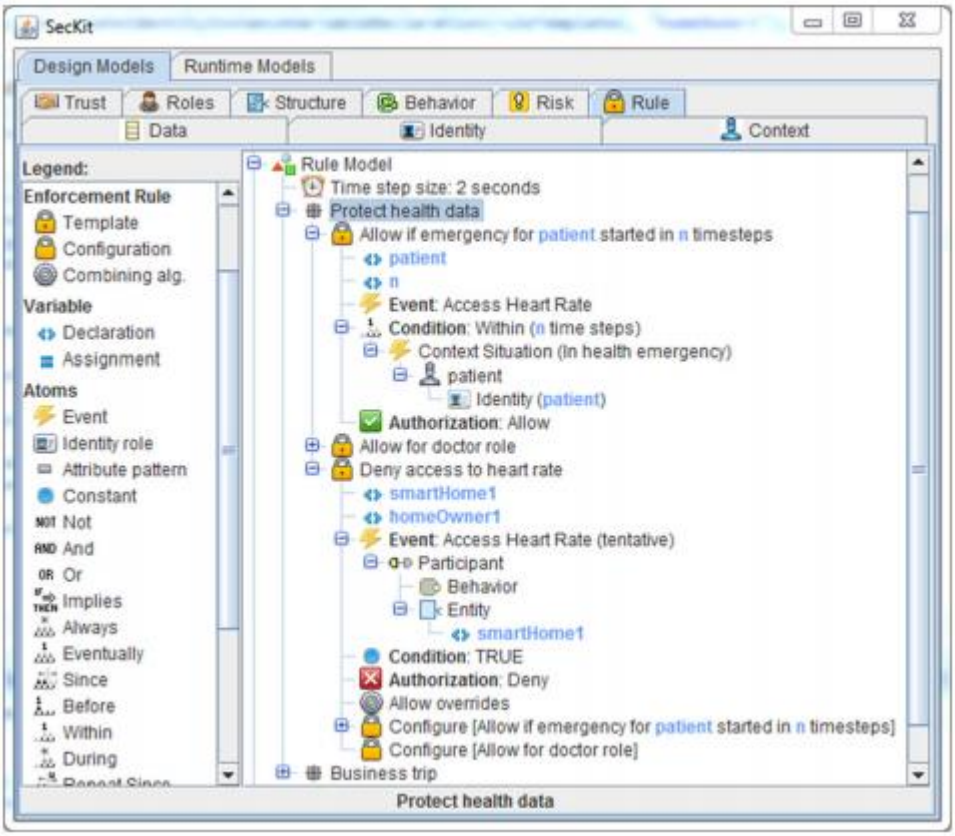


Figure 2. Sample GUI for security policy profile authoring. [2]

Ethical Design can mitigate the ethical challenges of IoT introduced in the previous section. By providing control of the collection and distribution of data or services related to the user, Ethical Design increases transparency and security in data mining of IoT. Also, it reduces business risks for investments by supporting businesses in a long term relationship with consumers who want to buy ethically-framed products and services [2].

Ethical Analysis

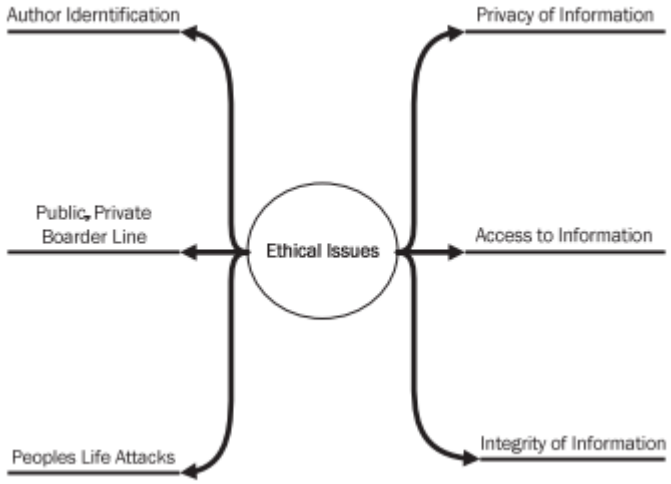


Figure 3. Possible Ethical Issues in IoT. [3]

As shown by Figure 3 above, there are multiple ethical issues of IoT. Based on personal experience, statistical evidence and ethical reasoning, our in-class discussion focused on the access and privacy of information. We also talked about the ethical concerns for implementation Ethical Design other than the ones discussed in the reading material.

What kinds of data should be considered “personal”?

In the case of privacy of IoT, it is essential to determine what kinds of data is private. And the question raises that if the data is not “personal” or cannot be related to individuals, should everyone has the right to collect and use it? The answer to the question is not absolute because the boarder between public and private data is hard to determine. By the work of Baldini [2], several claims have been made that the concept of privacy should be revisited, as the amount of collected data from the IoT will be too difficult to control — and the complexity becomes even higher when attempting to

determine which data are personal and which are not. There exist technical solutions for the problem, namely the Privacy Enhancing Technologies (PET) and the application of Privacy Enhancing Measures (PEM). With the technical measure, the developers can separate different sets of data collected. However, the market of such technique is still limited because of the opportunity to monetize data collection, and the cost of implementation of the privacy protection technique[5]. In other words, the technique to protect data privacy and to measure privacy level is not cost effective for the companies. Also as raised by one of the student, the anonymous mode is not considered private for the similar technical reason.

Is it fair to make customization of privacy settings a value-added service?

As discussed in the reading material, Ethical Design of IoT provides users with control of the data collection and distribution of IoT services. We discussed that whether the privacy setting should be a basic right for users, or should users pay companies to stop collecting and using their data. As introduced by one of the student, data collection and data usage have become the main income for many internet companies, including Facebook, Twitter and LinkedIn. For instance, by the CNBC news [6], Facebook made an average of $6.18 off each user in 2018. For companies, income from data collection helps maintain quality of services, and thus whether customization of privacy settings as a value-added service is fair has always been a controversial topic. In class discussion our classmates brought up an interesting assumption that the customization of

privacy should differ for free services (e.g., services provided by Facebook) and services based on physical goods (e.g, IoT products). By this assumption, the payment for IoT implementation compensates the income of data collection for companies.

Conclusion

The fast development of IoT technique and its widespread has brought privacy risks due to the large amount of data collected and processed. And Ethical Design of IoT services allows users to select specific sets of policies and provides control over personal data. By supporting ethical choices of users, Ethical Design mitigates the conflict between stakeholders, and further promotes the development of IoT technique. There are other ethical concerns of the Ethical Design model, for instance whether the application of Privacy Enhancing Measures (PEM) should be implemented, and whether the privacy setting should be customized. Such concerns should be considered at the point of view of both stakeholders (users and companies) in order to solver the ethical challenges of IoT products.

- Iot in environmental protection

The applications of IoT in environmental monitoring are broad − environmental protection, extreme weather monitoring, water safety, endangered species protection, commercial farming, and more. In these applications, sensors detect and measure every type of environmental change.

Air and Water Pollution

Current monitoring technology for air and water safety primarily uses manual labor along with advanced instruments, and lab processing. IoT improves on this technology by reducing the need for human labor, allowing frequent sampling, increasing the range of sampling and monitoring, allowing sophisticated testing on-site, and binding response efforts to detection systems. This allows us to prevent substantial contamination and related disasters.

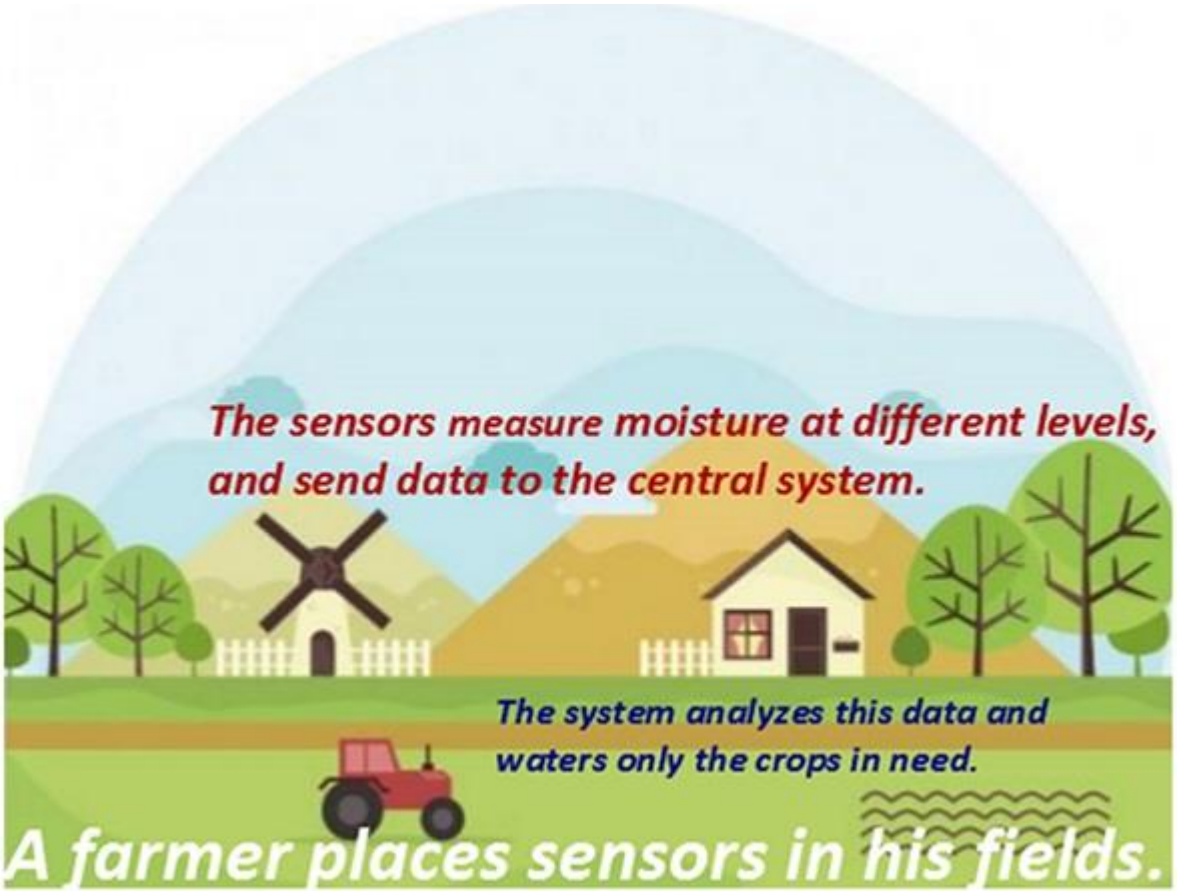
Extreme Weather

Though powerful, advanced systems currently in use allow deep monitoring, they suffer from using broad instruments, such as radar and satellites, rather than more granular solutions. Their instruments for smaller details lack the same accurate targeting of stronger technology.

New IoT advances promise more fine-grained data, better accuracy, and flexibility. Effective forecasting requires high detail and flexibility in range, instrument type, and deployment. This allows early detection and early responses to prevent loss of life and property.

Commercial Farming

Today's sophisticated commercial farms have exploited advanced technology and biotechnology for quite some time, however, IoT introduces more access to deeper automation and analysis.



Much of commercial farming, like weather monitoring, suffers from a lack of precision and requires human labor in the area of monitoring. Its automation also remains limited.

IoT allows operations to remove much of the human intervention in system function, farming analysis, and monitoring. Systems detect changes to crops, soil, environment, and more. They optimize standard processes through analysis of large, rich data collections. They also prevent health hazards

- Short answers

  What Is home automation ?

  Applications of iot in smart cities?

  What is industrial iot?

Applications of iot in health and lifestyle?

- Long answers

  Explain about iot designs and ethics?

  Write about iot in environment protection?

INTERNAL EXAMINATION 1

Answer any five of the following questions (5*2=10)

Section A

1. What is definition of iot?
2. What are the chaaracteristics of iot?
3. Explain about things in iot?
4. Explain about REST protocol
5. What is WPAN technology?
6. Exlain about ZIGBEE,HART?
7. What is ip base protocols
8. What is AMPQ protocols

Section B

Answer any two of below 2*10=20

Unit 1

9.explain the chaaracteristics of iot in detail?

(Or)

10.write about things in iot ?

unit 2

11.. explain about edge connectivity and protocols?

(Or)

12. explain about iot development boards?

INTERNAL EXAMINATION 2

Section A

Answer any five of the following 5*2=10

1.what is ipv6?

2.what is mqtt?

3.what are data handling technologies?

4.what is data acquisition?

5.what is cloud analytics?

6.what are local analytics?

7.applications of iot in home automation?

8.what are applications of iot in smart cities?

Section B

Answer any two of the following 2*10=20

Unit 1

9.explain about Edge /fog computing?

Or

10.write about iot in environmental protection?

Unit 2

11.explain about Hadoop?

Or

12.what are iot designs and ethics?

MASTER OF COMPUTER APPLICATIONS DEGREE EXAMINATION

MCA 402-INTERNET OF THINGS

(Common paper to university and alla affiliated colleges)

Time :3 hours max .marks:70

Part A

Answer any FIVE of the following questions. Each question carries 4 marks (5*4=20)

a. What is definition of iot?

b. What are the chaaracteristics of iot?

c. What is WPAN technology?

d. Explain about ZIGBEE,HART?

e. what is cloud analytics?

f. what are local analytics?

g. Applications of iot in home automation?

i. Applications of iot in home automation?

j. what are applications of iot in smart cities?

Part B

Answer FIVE questions ,choosing one question from each unit. Each question carries 10 marks

(5*10=50)

Unit 1

2.explain the chaaracteristics of iot in detail?

(or)

3.write about things in iot ?

unit 2

4. explain about edge connectivity and protocols?

(Or)

5. explain about iot development boards?

Unit 3

6.What are wpn Technologies?

(Or)

7.What are ip based protocols?

Unit 4

8.explain about Edge /fog computing?

(Or)

9.write about iot in environmental protection?

Unit 5

10.explain about Hadoop?

(Or)

11.what are iot designs and ethics?