ONJOB TRAINING

Undergone at JUSCO

JUSCO
quality services for life
A TATA Enterprise

Project on INITIATIVES FOR DIGITILISATION

Under the Guidance of

Mr.Gaurav Anand

Submitted By

Department of Computer Science

The Graduate School College For Women

Manisha Kaushal

ACKNOWLEDGEMENT

It would be my at most pleasure to express my sincere thanks to our guide Mr. Gaurav Anand in providing a helping hand in this project. His unflagging patience ,creativity and immense knowledge that he shared with us ,have proved to be highly beneficial .It has made my project both possible and successful.

CONTENTS

1. INTRODUCTION

The **Initiatives For Digitilisation** is the extension of internet connectivity into physical devices and everyday objects. Embedded with electronics,Internet Connectivity , and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled.

A growing portion of digitilisation are created for consumer use, including connected vehicles, home automation, wearable technology (as part of Internet of Wearable Things (IoWT)), connected health, and appliances with remote monitoring capabilities.

One of the key drivers of the digitilisation is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on the digitilisation collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used. Though still in their infancy, regulations and governance regarding these issues of privacy, security, and data ownership continue to develop.Digitilisation regulation depends on the country. Some examples of legislation that is relevant to privacy and data collection are: the US Privacy Act of 1974, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995.

Current regulatory environment:

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:

- Data Security – At the time of designing digitilisation companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defence in depth" approach and encrypt data at each stage.
- Data consent – users should have a choice as to what data they share with digitilisation companies and the users must be informed if their data gets exposed.
- Data minimization – Digitilisation companies should collect only the data they need and retain the collected information only for a limited time.

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act the Fair Credit Reporting Act, and theChildren's Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multi-stakeholder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights.

A resolution passed by the Senate in March 2015, is already being considered by the Congress.This resolution recognized the need for formulating a National Policy on Digitilisation and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the Digitilisation ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to connect IoT devices.

Several standards for the IoT industry are actually being established relating to automobiles because most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cybersecurity guidelines and a database of best practices to make automotive computer systems more secure.

A recent report from the World Bank examines the challenges and opportunities in government adoption of IoT. These include –

- Still early days for the digitilisation in government
- Underdeveloped policy and regulatory frameworks
- Unclear business models, despite strong value proposition
- Clear institutional and capacity gap in government AND the private sector
- Inconsistent data valuation and management
- Infrastructure a major barrier
- Government as an enabler
- Most successful pilots share common characteristics (public-private partnership, local, leadership).

2. INTERNET OF EVERYTHING

The internet of everything (IoE) is a broad term that refers to devices and consumer products connected to the internet and outfitted with expanded digital features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices and items connected to the global internet.

The term is somewhat synonymous with the internet of things (IoT).

IoE is based on the idea that in the future, internet connections will not be restricted to laptop or desktop computers and a handful of tablets, as in previous decades. Instead, machines will generally become smarter by having more access to data and expanded networking opportunities.

Actual IoE applications range from digital sensor tools/interfaces used for remote appliances to smarter and more well-connected mobile devices, industrial machine learning systems and other types of distributed hardware that have recently become more intelligent and automated.

IoE features fall under two main categories:

- Input: Allows analog or external data to be put into a piece of hardware
- Output: Allows a piece of hardware to be put back into the internet

The IoE term is driving much discussion about IT's future. For example, organizations like Cisco use the term in its branding to refer to the potential of modern and future technology.

The Internet of Everything (IoE) is a concept that extends the Internet of Things (IoT) emphasis on machine-to-machine (M2M) communications to describe a more complex system that also encompasses people and processes.

The concept of the Internet of Everything originated at Cisco, who defines IoE as "the intelligent connection of people, process, data and things." Because in the Internet of Things, all communications are between machines, IoT and M2M are sometimes considered synonymous. The more expansive IoE concept includes, besides M2M communications, machine-to-people (M2P) and technology-assisted people-to-people (P2P) interactions.

The Internet of Things, in its broadest conceptualization, includes any type of physical or virtual object or entity that can be made addressable and given the ability to transmit data without human-to-machine input – those are the things in the IoT. Things are often items that would not have been networked in the past; automation of thing communications is also central to the IoT concept. The IoE, on the other hand, also includes user-generated communications and interactions associated with the global entirety of networked devices.

3. IoT (INTERNET OF THINGS)

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

WHY IOT?

An article by Ashton published in the RFID Journal in 1999 said, "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. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory." This is precisely what IoT platforms does for us. It enables devices/objects to observe, identify and understand a situation or the surroundings without being dependent on human help.

WHAT IS THE SCOPE OF IOT?

Internet of Things can connect devices embedded in various systems to the internet. When devices/objects can represent themselves digitally, they can be controlled from anywhere. The connectivity then helps us capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security.

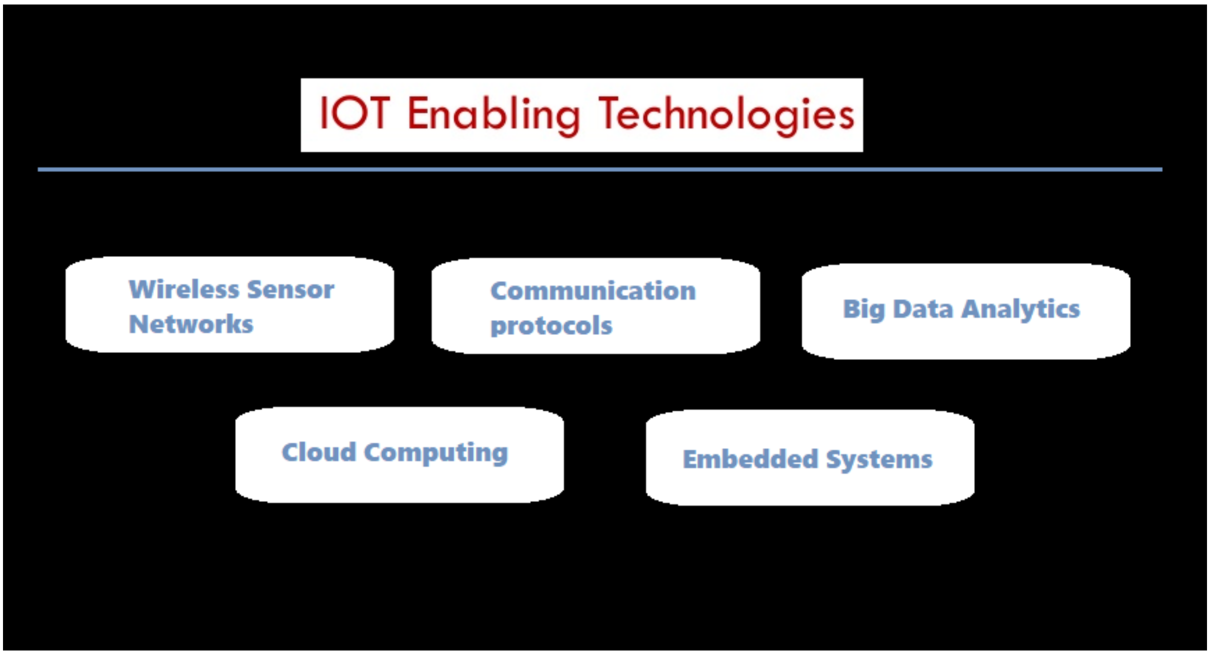
IoT is a transformational force that can help companies improve performance through IoT analytics and **IoT Security** to deliver better results. Businesses in the utilities, oil & gas, insurance, manufacturing, transportation, infrastructure and retail sectors can reap the benefits of IoT by making more informed decisions, aided by the torrent of interactional and transactional data at their disposal.

HOW CAN IOT HELP?

IoT platforms can help organizations reduce cost through improved process efficiency, asset utilization and productivity. With improved tracking of devices/objects using sensors and connectivity, they can benefit from real-time insights and analytics, which would help them make smarter decisions. The growth and convergence of data, processes and things on the internet would make such connections more relevant and important, creating more opportunities for people, businesses and industries.

4. IoT ENABLING TECHNOLOGIES

IoT is enabled by several technologies including wireless sensor networks, cloud computing, Big data analytics, Embedded Systems, Security Protocols and architectures, communication protocols, web services, Mobile Internet, and Semantic Search engines.



Wireless Sensor Networks

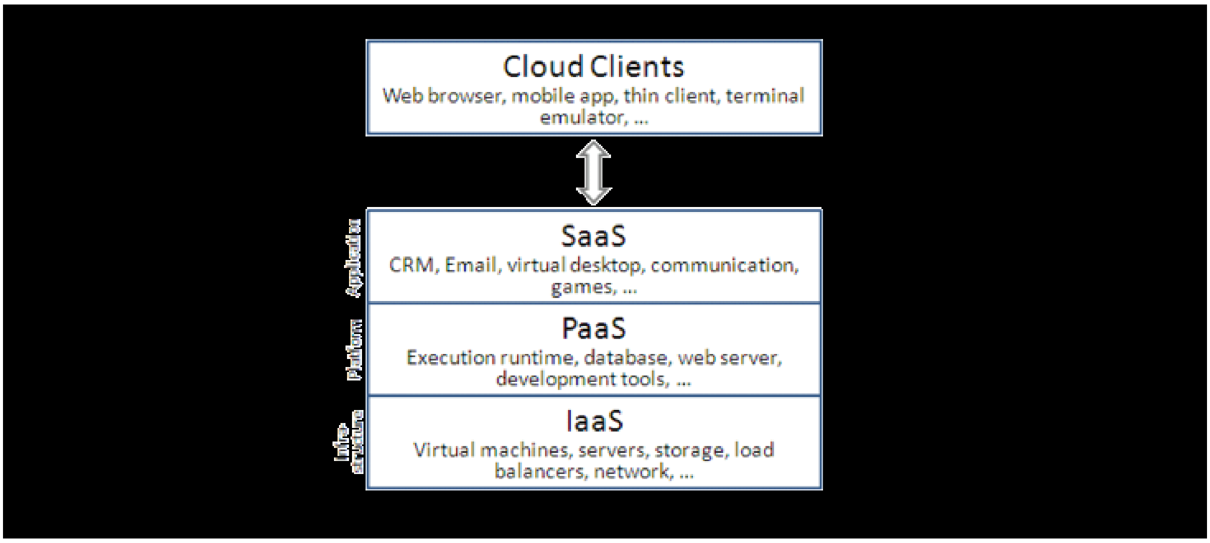
A wireless sensor network comprises of distributed device with sensor which are used to monitor the environmental and physical conditions. A WSN consists of a number of end-nodes and routers and a coordinator. End Nodes have several sensors attached to them in node can also act as routers. Routers are responsible for routing the data packets from end-nodes to the coordinator. The coordinator collects the data from all the nodes. Coordinator also act as a gateway that connects the WSN to the internet. Some examples of WSNs used in IoT systems are described as follows:

- Weather monitoring system use WSNs in which the nodes collect temperature humidity and other data which is aggregated and analyzed.
- Indoor air quality monitoring systems use WSNs to collect data on the indoor air quality and concentration of various gases
- Soil moisture monitoring system use WSNs to monitor soil moisture at various locations.
- Surveillance system use WSNs for collecting Surveillance data (such as motion detection data)
- Smart grid use WSNs for monitoring the grid at various points.

- Structural health monitoring system use WSNs to monitor the health of structures (buildings, bridges) by collecting vibration data from sensor nodes de deployed at various points in the structure.

Cloud Computing

Cloud computing is a trans-formative computing paradigm that involves delivering applications and services over the Internet Cloud computing involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the users, in a “pay as you go” model. C loud computing resources can be provisioned on demand by the users, without requiring interacyions with the cloud service Provider. The process of provisioning resources is automated. Cloud computing resources can be accessed over The network using standard access mechanisms that provide platform independent access through the use of heterogeneous client platforms such as the workstations, laptops, tablets and smartphones.



Cloud computing services are offered to users in different forms:

Infrastructure as a Service (IaaS): hardware is provided by an external provider and managed for you
Platform as a Service (PaaS): in addition to hardware, your operating system layer is managed for you
Software as a Service (SaaS): further to the above, an application layer is provided and managed for you – you won’t see or have to worry about the first two layers.

Big Data Analytics

Big Data analytics is the process of collecting, organizing and analyzing large sets of data (*called* Big Data) to discover patterns and other useful information. Big Data analytics can help organizations to better understand the information contained within the data and will also help identify the data that is most important to the business and future business decisions. Analysts working with Big Data typically want the *knowledge* that comes from analyzing the data. Some examples of big data generated by IoT systems are described as follows:

- Sensor data generated by IoT system such as weather monitoring stations.
- Machine sensor data collected from sensors embedded in industrial and energy systems for monitoring their health and detecting Failures.
- Health and fitness data generated by IoT devices such as wearable fitness bands
- Data generated by ioT systems for location and tracking of vehicles
- Data generated by retail inventory monitoring systems

Characteristics

Big data can be described by the following characteristics:

- **Volume –** The quantity of generated and stored data. The size of the data determines the value and potential insight, and whether it can be considered big data or not.
- **Variety –** The type and nature of the data. This helps people who analyze it to effectively use the resulting insight. Big data draws from text, images, audio, video; plus it completes missing pieces through data fusion.
- **Velocity –** In this context, the speed at which the data is generated and processed to meet the demands and challenges that lie in the path of growth and development. Big data is often available in real-time. Compared to small data, big data are produced more continually. Two kinds of velocity related to Big Data are the frequency of generation and the frequency of handling, recording, and publishing.
- **Veracity –** It is the extended definition for big data, which refers to the data quality and the data value. The data quality of captured data can vary greatly, affecting the accurate analysis.

Communication protocols

Communication protocols form the backbone of IoT systems and enable network connectivity and coupling to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together are known as a protocol suite; when implemented in software they are a protocol stack.

Internet communication protocols are published by the Internet Engineering Task Force (IETF). The IEEE handles wired and wireless networking, and the International Organization for Standardization (ISO) handles other types. The ITU-T handles telecommunication protocols and formats for the public switched telephone network (PSTN). As the PSTN and Internet converge, the standards are also being driven towards convergence.

5. IoT FRAMEWORKS

KAA IoT

Kaa IoT is one the most efficient and rich open source *Internet of Things* cloud platform where anyone has a free way to materialize their smart product concepts. On this platform, you can manage unlimited number of connected devices with cross device interoperability. You can achieve real time device monitoring with the possibility of remote device provisioning and configuration.

MACHINNA.io

macchina.io IoT platforms provides a web enabled, modular and extensible JavaScript and C++ runtime environment for developing IoT gateway applications. It also supports a wide variety of sensors and connection technologies including Tinkerforge, bricklets, Xbee and many others including accelerometers.

ZETTA

Zetta is a server oriented platform that has been built around ***NodeJS***, REST and a flow based **reactive programming development** philosophy linked with the Siren hypermedia APIs. They are connected with cloud services after being abstracted as REST APIs. These cloud services include visualization tools and support for machine analytics tool like splunk. It creates a gero-distributed network by connecting end points such as Linux and Arduino hacker boards with platforms such as Heroku.

GE PREDIX

GE's platform as a service software for industrial IoT is based on the concept of cloud foundry. It adds asset management, device security and real time, predictive analytics that also supports heterogeneous data acquisition, access and storage.

6. REAL WORLD APPLICATION OF INTERNET OF THINGS (IoT)

How Big is IoT?

This new wave of connectivity is going beyond laptops and smartphones, it's going towards connected cars, smart homes, connected wearables, smart cities and connected healthcare. Basically a connected life. According to Gartner report, by 2020 connected devices across all technologies will reach to 20.6 billion.

HP did a small survey in which they estimated the rise of connected devices over the years and the results are surprising. Are we moving towards a fully automated world?

These devices will bridge the gap between physical and digital world to improve the quality and productivity of life, society and industries. With IoT catching up Smart homes is the most awaited feature, with brands already getting into the competition with smart applicances. Wearables are another feature trending second on the internet. With launch of Apple Watch and more devices to flow in, these connected devices are going to keep us hooked with the inter-connected world.

A survey conducted by KRC Reserach in UK, US, Japan and Germany the early adopters of IOT has revealed which devices are the customers more likely to use in the coming years. Smart Appliances like thermostat, smart refrigerator to name a few are most liked by the customers and are seem to change the way we operate.

Real World Applications of IoT

1. Smart Home

With IoT creating the buzz, 'Smart Home' is the most searched IoT associated feature on Google. But, what is a Smart Home?

Wouldn't you love if you could switch on air conditioning before reaching home or switch off lights even after you have left home? Or unlock the doors to friends for temporary access even when you are not at home. Don't be surprised with IoT taking shape companies are building products to make your life simpler and convenient.

Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones.

The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money. With Smart home companies like Nest, Ecobee, Ring and August, to name a few, will become household brands and are planning to deliver a never seen before experience.

2. Wearables

Wearables have experienced a explosive demand in markets all over the world. Companies like Google, Samsung have invested heavily in building such devices. But, how do they work?

Wearable devices are installed with sensors and softwares which collect data and information about the users. This data is later pre-processed to extract essential insights about user.

These devices broadly cover fitness, health and entertainment requirements. The pre-requisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized.

3. Connected Cars

The automotive digital technology has focused on optimizing vehicles internal functions. But now, this attention is growing towards enhancing the in-car experience.

A connected car is a vehicle which is able to optimize it's own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity.

Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.

4. Industrial Internet

Industrial Internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines.

According to Jeff Immelt, CEO, GE Electric, IIoT is a "beautiful, desirable and investable" asset. The driving philosophy behind IIoT is that, smart machines are more accurate and consistent than humans in communicating through data. And, this data can help companies pick inefficiencies and problems sooner.

IIoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency. According to GE the improvement industry productivity will generate $10 trillion to $15 trillion in GDP worldwide over next 15 years.

5. Smart Cities

Smart city is another powerful application of IoT generating curiosity among world's population. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities.

IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied.

By installing sensors and using web applications, citizens can find free available parking slots across the city. Also, the sensors can detect meter tampering issues, general malfunctions and any installation issues in the electricity system.

6. IoT in agriculture

With the continous increase in world's population, demand for food supply is extremely raised. Governments are helping farmers to use advanced techniques and research to increase food production. Smart farming is one of the fastest growing field in IoT.

Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT.

7.Smart Retail

The potential of IoT in the retail sector is enormous. IoT provides an opportunity to retailers to connect with the customers to enhance the in-store experience.

Smartphones will be the way for retailers to remain connected with their consumers even out of store. Interacting through Smartphones and using Beacon technology can help retailers serve their consumers better. They can also track consumers path through a store and improve store layout and place premium products in high traffic areas.

8.Energy Engagement

Power grids of the future will not only be smart enough but also highly reliable. Smart grid concept is becoming very popular all over world.

The basic idea behind the smart grids is to collect data in an automated fashion and analyze the behavior or electricity consumers and suppliers for improving efficiency as well as economics of electricity use.

Smart Grids will also be able to detect sources of power outages more quickly and at individual household levels like near by solar panel, making possible distributed energy system.

9. IOT in Healthcare

Connected healthcare yet remains the sleeping giant of the Internet of Things applications. The concept of connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general.

Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices.

The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness. The video below explains how IoT can revolutionize treatment and medical help.

10.IoT in Poultry and Farming

Livestock monitoring is about animal husbandry and cost saving. Using IoT applications to gather data about the health and well being of the cattle, ranchers knowing early about the sick animal can pull out and help prevent large number of sick cattle.

7. SENSORS & DATA CAPTURE

SENSORS:

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A **Sensor** converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. Let's explain the example of temperature. The mercury in the glass thermometer expands and contracts the liquid to convert the measured temperature which can be read by a viewer on the calibrated glass tube.

Criteria to choose a Sensor

There are certain features which have to be considered when we choose a sensor. They are as given below:

1. Accuracy
2. Environmental condition - usually has limits for temperature/ humidity
3. Range - Measurement limit of sensor
4. Calibration - Essential for most of the measuring devices as the readings changes with time
5. Resolution - Smallest increment detected by the sensor
6. Cost
7. Repeatability - The reading that varies is repeatedly measured under the same environment

Classification of Sensors

The sensors are classified into the following criteria:

1. Primary Input quantity (Measurand)
2. Transduction principles (Using physical and chemical effects)
3. Material and Technology
4. Property
5. Application

Transduction principle is the fundamental criteria which are followed for an efficient approach. Usually, material and technology criteria are chosen by the development engineering group.

Classification based on property is as given below:

- **Temperature** - Thermistors, thermocouples, RTD's, IC and many more.
- **Pressure** - Fibre optic, vacuum, elastic liquid based manometers, LVDT, electronic.
- Flow - Electromagnetic, differential pressure, positional displacement, thermal mass, etc.
- **Level Sensors** - Differential pressure, ultrasonic radio frequency, radar, thermal displacement, etc.
- **Proximity and displacement** - LVDT, photoelectric, capacitive, magnetic, ultrasonic.
- **Biosensors** - Resonant mirror, electrochemical, surface Plasmon resonance, Light addressable potentio-metric.
- **Image** - Charge coupled devices, CMOS
- **Gas and chemical** - Semiconductor, Infrared, Conductance, Electrochemical.
- **Acceleration** - Gyroscopes, Accelerometers.
- **Others** - Moisture, humidity sensor, Speed sensor, mass, Tilt sensor, force, viscosity.

Surface Plasmon resonance and Light addressable potentio-metric from the Bio-sensors group are the new optical technology based sensors. CMOS Image sensors have low resolution as compared to charge coupled devices. CMOS has the advantages of small size, cheap, less power consumption and hence are better substitutes for Charge coupled devices. Accelerometers are independently grouped because of their vital role in future applications like aircraft, automobiles, etc and in fields of videogames, toys, etc. Magnetometers are those sensors which measure magnetic flux intensity B (in units of Tesla or As/m2).

Classification based on Application is as given below:

- Industrial process control, measurement and automation
- Non-industrial use – Aircraft, Medical products, Automobiles, Consumer electronics, other type of sensors.

Sensors can be classified based on power or energy supply requirement of the sensors:

- **Active Sensor** - Sensors that require power supply are called as Active Sensors. Example: LiDAR (Light detection and ranging), photoconductive cell.

· **Passive Sensor** - Sensors that do not require power supply are called as Passive Sensors. Example: Radiometers, film photography.

In the current and future applications, sensors can be classified into groups as follows:

· ***Accelerometers*** - These are based on the Micro Electro Mechanical sensor technology. They are used for patient monitoring which includes pace makers and vehicle dynamic systems.

· ***Biosensors*** - These are based on the electrochemical technology. They are used for food testing, medical care device, water testing, and biological warfare agent detection.

· ***Image Sensors*** - These are based on the CMOS technology. They are used in consumer electronics, biometrics, traffic and security surveillance and PC imaging.

· ***Motion Detectors*** - These are based on the Infra Red, Ultrasonic, and Microwave / radar technology. They are used in videogames and simulations, light activation and security detection.

Type 1: Temperature

Types of Sensors

Some commonly used sensors alongwith their principle and applications are explained as follows:

1. Temperature Sensors

This device collects information about temperature from a source and converts into a form that is understandable by other device or person. The best illustration of a temperature sensor is mercury in glass thermometer. The mercury in the glass expands and contracts depending on the alterations in temperature. The outside temperature is the source element for the temperature measurement. The position of the mercury is observed by the viewer to measure the temperature. There are two basic types of temperature sensors:

· ***Contact Sensors*** – This type of sensor requires direct physical contact with the object or media that is being sensed. They supervise the temperature of solids, liquids and gases over a wide range of temperatures.

· ***Non contact Sensors*** – This type of sensor does not require any physical contact with the object or media that is being sensed. They supervise non-reflective solids and liquids but are not useful for gases due to natural transparency. These sensors use Plank's Law to measure temperature. This law deals with the heat radiated from the source of heat to measure the temperature.

Working of different types of Temperature Sensors along with examples

(i) Thermocouple – They are made of two wires (each of different homogeneous alloy or metal) which form a measuring junction by joining at one end. This measuring junction is open to the elements being measured. The other end of the wire is terminated to a measuring device where a reference junction is formed. The current flows through the circuit since the temperature of the two junctions are different. The resulted milli-voltage is measured to determine the temperature at the junction. The diagram of thermocouple is shown below.

Fig: *Thermocouple Temperature Sensor*

(ii) Resistance Temperature Detectors (RTD) – These are types of thermal resistors that are fabricated to alter the electrical resistance with the alteration in temperature. They are very expensive than any other temperature detection devices. The diagram of Resistance Temperature Detectors is shown below.

(iii) Thermistors – They are another kind of thermal resistor where a large change in resistance is proportional to small change in temperature.

Type 2: IR Sensors

2. IR Sensor

Fig: *typical IR Sensors*

This device emits and/or detects infrared radiation to sense a particular phase in the environment. Generally, thermal radiation is emitted by all the objects in the infrared spectrum. The infrared sensor detects this type of radiation which is not visible to human eye.

Advantages

- Easy for interfacing
- Readily available in market

Disadvantages

- Disturbed by noises in the surrounding such as radiations, ambient light etc.

Working

The basic idea is to make use of IR LEDs to send the infrared waves to the object. Another IR diode of the same type is to be used to detect the reflected wave from the object. The diagram is shown below.

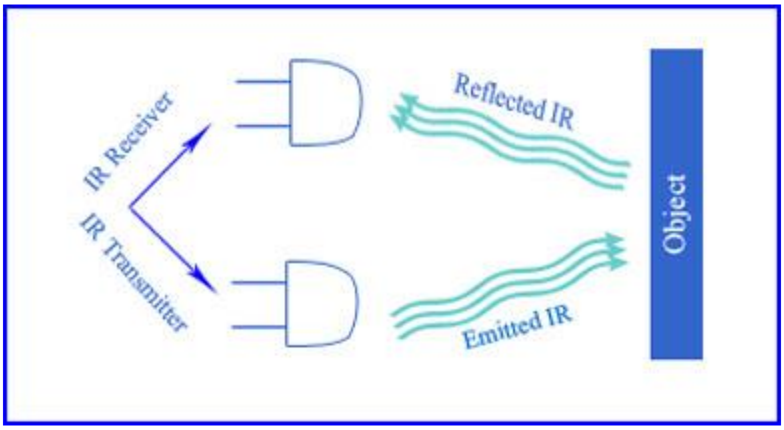


Fig: *Diagram Explaining Working Of IR Led Sensor*

When IR receiver is subjected to infrared light, a voltage difference is produced across the leads. Less voltage which is produced can be hardly detected and hence operational amplifiers (Op-amps) are used to detect the low voltages accurately.

Measuring the distance of the object from the receiver sensor: The electrical property of IR sensor components can be used to measure the distance of an object. The fact when IR receiver is subjected to light, a potential difference is produced across the leads.

Applications

- Thermography – According to the black body radiation law, it is possible to view the environment with or without visible illumination using thermography

· Heating – Infrared can be used to cook and heat food items. They can take away ice from the wings of an aircraft. They are popular in industrial field such as, print dying, forming plastics, and plastic welding.

· Spectroscopy – This technique is used to identify the molecules by analysing the constituent bonds. This technique uses light radiation to study organic compounds.

· Meteorology – Cloud heights, calculate land and surface temperature is possible when weather satellites are equipped with scanning radiometers.

· Photobiomodulation – This is used for chemotherapy in cancer patients. This is used to treat anti herpes virus.

· Climatology – Monitoring the energy exchange between the atmosphere and earth.

· Communications – Infra red laser provide light for optical fibre communication. These radiations are also used for short range communications among mobiles and computer peripherals.

Type 3: UV Sensors

3. UV Sensor

These sensors measure the intensity or power of the incident ultraviolet radiation. This form of electromagnetic radiation has wavelengths longer than x-rays but is still shorter than visible radiation. An active material known as polycrystalline diamond is being used for reliable ultraviolet sensing. UV sensors can discover the exposure of environment to ultraviolet radiation.

Criteria to select a UV Sensor

· Wavelength ranges in nanometres (nm) that can be detected by the UV sensors.

· Operating temperature

· Accuracy

· Weight

· Power range

Working

The UV sensor accepts one type of energy signal and transmits different type of energy signals.

To observe and record these output signals they are directed to an electrical meter. To create graphs and reports, the output signals are transmitted to an analog-to-digital converter (ADC), and then to a computer with software.

Examples include:

· UV phototubes are radiation-sensitive sensors supervise UV air treatments, UV water treatments, and solar irradiance.

· Light sensors measure the intensity of incident light.

· UV spectrum sensors are charged coupled devices (CCD) utilized in scientific photography.

· Ultraviolet light detectors.

· Germicidal UV detectors.

· Photo stability sensors.

Applications

· Measures the portion of the UV spectrum which sunburns human skin

· Pharmacy

· Automobiles

· Robotics

· Printing industry for solvent handling and dyeing processes

· Chemical industry for the production, storage, and transportation of chemicals

Type 4: Touch Sensor

4. Touch Sensor

A touch sensor acts as a variable resistor as per the location where it is touched. The figure is as shown below.

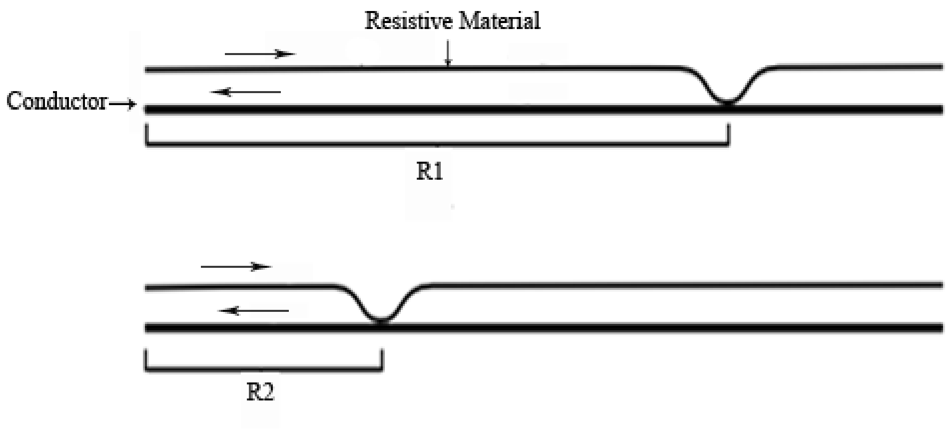


Fig: *Touch Sensor Working As Variable Resistor*

A touch sensor is made of:

· Fully conductive substance such as copper

· Insulated spacing material such as foam or plastic

· Partially conductive material

Principle and Working

The partially conductive material opposes the flow of current. The main principle of the linear position sensor is that the current flow is more opposed when the length of this material that must be travelled by the current is more. As a result, the resistance of the material is varied by changing the position at which it makes contact with the fully conductive material.

Generally, softwares are interfaced to the touch sensors. In such a case, a memory is being offered by the software. They can memorize the 'last touched position' when the sensor is deactivated. They can memorize the 'first touched position' once the sensor gets activated and understand all the values related to it. This act is similar to how one moves the mouse and locates it at the other end of mouse pad in order to move the cursor to the far side of the screen.

Applications

The touch sensors being cost effective and durable are used in many applications such as

· Commercial – Medical, vending, Fitness and gaming

· Appliances – Oven, Washing machine/dryers, dishwashers, refrigerators

· Transportation – Cockpit fabrication and streamlining control among the vehicle manufacturers

· Fluid level sensors

· Industrial Automation – Position and liquid level sensing, human touch control in automation applications

· Consumer Electronics – Provides a new feel and level of control in various consumer products

Type 5: Proximity Sensor

5. Proximity Sensor

A proximity sensor detects the presence of objects that are nearly placed without any point of contact. Since there is no contact between the sensors and sensed object and lack of mechanical parts, these sensors have long functional life and high reliability. The different types of proximity sensors are Inductive Proximity sensors, Capacitive Proximity sensors, Ultrasonic proximity sensors, photoelectric sensors, Hall-effect sensors, etc.

Working

A proximity sensor emits an electromagnetic or electrostatic field or a beam of electromagnetic radiation (such as infrared), and waits for the return signal or changes in the field. The object which is being sensed is known as the proximity sensor's target.

Inductive Proximity sensors – They have an oscillator as input to change the loss resistance by the proximity of an electrically conductive medium. These sensors are preferred for metal targets.

Capacitive Proximity sensors – They convert the electrostatic capacitance variation flanked by the detecting electrode and the ground electrode. This occurs by approaching the nearby object with a variation in an oscillation frequency. To detect the nearby object, the oscillation frequency is transformed into a direct current voltage which is compared with a predetermined threshold value. These sensors are preferred for plastic targets.

Applications

· Used in automation engineering to define operating states in process engineering plants, production systems and automating plants

· Used in windows, and the alarm is activated when the window opens

· Used in machine vibration monitoring to calculate the difference in distance between a shaft and its support bearing

Principle

Different definitions are approved to distinguish sensors and transducers. Sensors can be defined as an element that senses in one form of energy to produce a variant in same or another form of energy. Transducer converts the measurand into the desired output using the transduction principle.

Based on the signals that are obtained and created, the principle can be categorized into following groups namely, Electrical, Mechanical, Thermal, Chemical, Radiant, and Magnetic.

Let’s take the example of an ultrasonic sensor.

An ultrasonic sensor is used to detect the presence of an object. It achieves this by emitting ultrasonic waves from the device head and then receiving the reflected ultrasonic signal from the concerned object. This helps in detecting the position, presence and movement of objects.

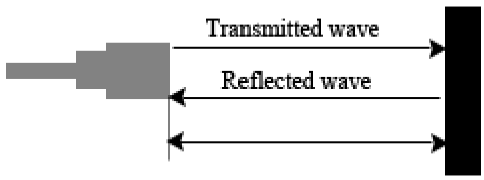


Fig: *Principle of Ultrasonic Sensor*

Since ultrasonic sensors rely on sound rather than light for detection, it is widely used to measure water-levels, medical scanning procedures and in the automobile industry. Ultrasonic waves can detect transparent objects such as transparent films, glass bottles, plastic bottles, and plate glass, using its Reflective Sensors.

Working

The movement of ultrasonic waves differ due to shape and type of media. For example, ultrasonic waves move straight in a uniform medium, and are reflected and transmitted back at the boundary between differing media. A human body in air causes considerable reflection and can be easily detected.

The travelling of ultrasonic waves can be best explained by understanding the following:

1. Multi-reflection

Multi-reflection takes place when waves are reflected more than once between the sensor and the detection object.

2. Limit Zone

The minimum sensing distance and maximum sensing distance can be adjusted. This is called the limit zone.

3. Undetection zone

The undetected zone is the interval between the surface of the sensor head and the minimum detection distance resulting from detection distance adjustment. The figure is shown below.

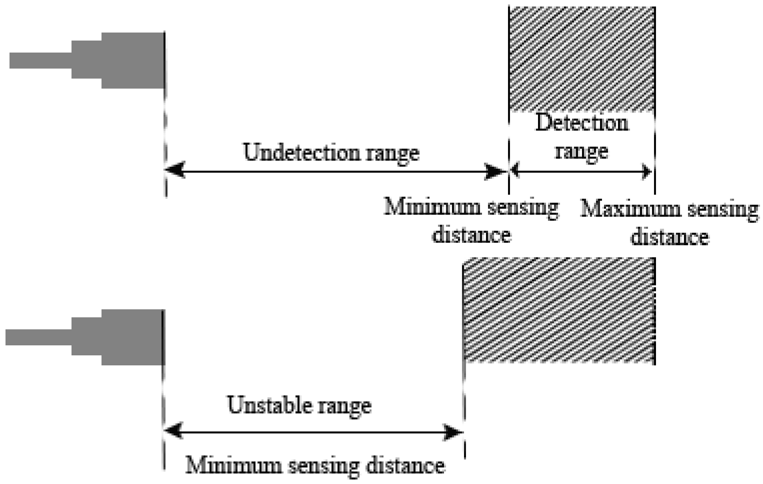


Fig: *Sensing Range In Ultrasonic Sensor*

The Undetection zone is the area close to the sensor where detection is not possible due to the sensor head configuration and reverberations. Detection may occur in the uncertainty zone due to multi-reflection between the sensor and the object.

Applications

Sensors are used in many kinds of applications such as:

- Shock Detection
- Machine monitoring applications
- Vehicle dynamics
- Low power applications
- Structural Dynamics
- Medical Aerospace
- Nuclear Instrumentation
- As pressure sensor in Mobiles 'touch key pad'
- Lamps which brighten or dim on touching its base
- Touch sensitive buttons in elevators

Advanced Sensor Technology

Sensor technology is used in wide range in the field of Manufacturing. The advanced technologies are as follows:

1. **Bar-code Identification** - The products sold in the markets has a Universal Product Code (UPC) which is a 12 digit code. Five of the numbers signify the manufacturer and other five signify the product. The first six digits are represented by code as light and dark bars. The first digit signifies the type of number system and the second digit which is parity signifies the accuracy of the reading. The remaining six digits are represented by code as dark and light bars reversing the order of the first six digits. Bar code is shown in the figure given below.

Fig: *A Typical Image Of Bar Code Scanned By Bar Code Reader*

The bar code reader can manage different bar code standards even without having the knowledge of the standard code. The disadvantage with bar coding is that the bar scanner is unable to read if the bar code is concealed with grease or dirt.

2. **Transponders** - In the automobile section, Radio frequency device is used in many cases. The transponders are hidden inside the plastic head of the key which is not visible to anyone. The key is inserted in the ignition lock cylinder. As you turn the key, the computer transmits a radio signal to the transponder. The computer will not let the engine to ignite until the transponder responds to the signal. These transponders are energized by the radio signals. The figure of a transponder is as shown below:

Fig: *A Image Of Embedded Transponder Used In Key*

3. **Electromagnetic Identification of Manufactured Components** - This is similar to the bar code technology where the data can be coded on magnetic stripe. With magnetic striping, the data can be read even if the code is concealed with grease or dirt.
4. **Surface Acoustic Waves** - This process is similar to the RF identification. Here, the part identification gets triggered by the radar type signals and is transmitted over long distances as compared to the RF systems.
5. **Optical Character Recognition** - This is a type of automatic identification technique which uses alphanumeric characters as the source of information. In United States, Optical character recognition is used in mail processing centres. They are also used in vision systems and voice recognition systems.

8. TRANSDUCERS

A transducer is an electronic device that converts energy from one form to another. Common examples include microphones, loudspeakers, thermometers, position and pressure sensors, and antenna. Although not generally thought of as transducers, photocells, LEDs (light-emitting diodes), and even common light bulbs are transducers.

Efficiency is an important consideration in any transducer. Transducer efficiency is defined as the ratio of the power output in the desired form to the total power input. Mathematically, if P represents the total power input and Q represents the power output in the desired form, then the efficiency E, as a ratio between 0 and 1, is given by:

$E = Q/P$

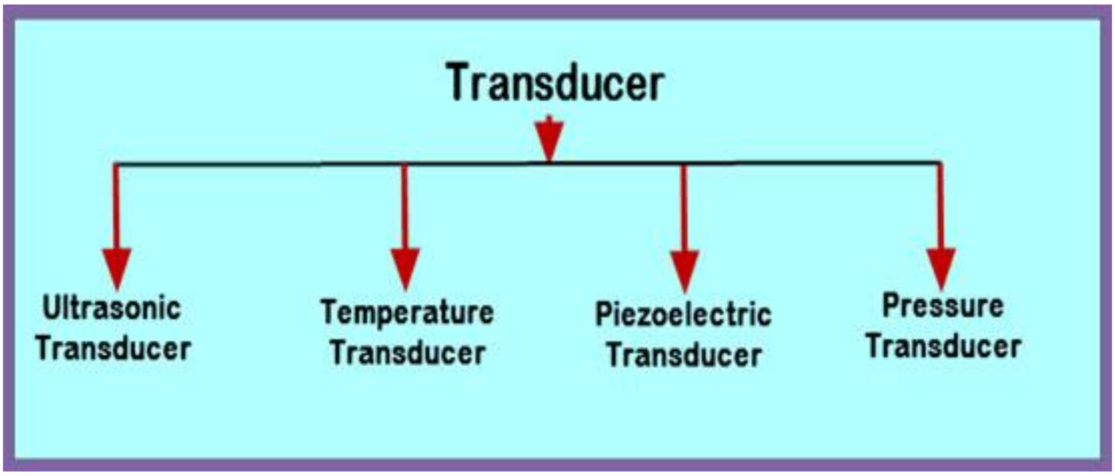
If $E_{\%}$ represents the efficiency as a percentage, then:

$E_{\%} = 100Q/P$

No transducer is 100 percent efficient; some power is always lost in the conversion process. Usually this loss is manifested in the form of heat. Some antennas approach 100-percent efficiency. A well-designed antenna supplied with 100 watts of radio frequency (RF) power radiates 80 or 90 watts in the form of an electromagnetic field. A few watts are dissipated as heat in the antenna conductors, the feed line conductors and dielectric, and in objects near the antenna. Among the worst transducers, in terms of efficiency, are incandescent lamps. A 100-watt bulb radiates only a few watts in the form of visible light. Most of the power is dissipated as heat; a small amount is radiated in the UV (ultraviolet) spectrum.It is an electrical device which is used to convert one form of energy into another form. In general, these devices deal with different types of energies such as mechanical, electrical energy, light energy, chemical energy, thermal energy, acoustic energy, electromagnetic energy, and so on.

For instance, consider a mic we use in daily life in telephones, mobile phones, that converts the sound into electrical signals and then amplifies it into the preferred range. Then, alters the electrical signals into audio signals at the o/p of the loudspeaker. Nowadays, fluorescent bulbs are used for lighting, changes the electrical energy into light energy.

The best examples of the transducer are mic, fluorescent bulb and speaker can be considered as a transducer. Likewise, there are different kinds of transducers used in electrical and electronic projects.



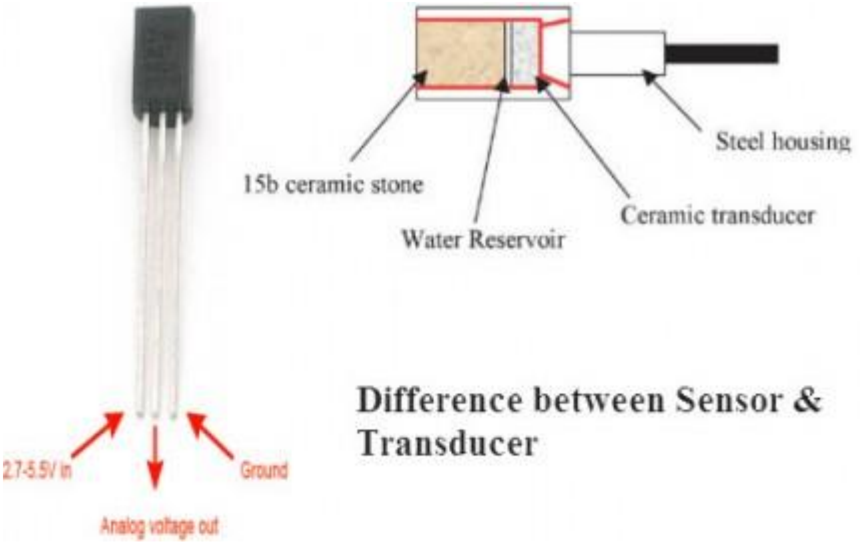
Transducer Types and Its Applications

There are a variety of transducer types like pressure transducer, piezoelectric transducer, ultrasonic transducer, temperature transducer, and so on. Let us discuss the use of different types of transducers in practical applications. Some transducer types like active transducer and passive transducers are based on whether a power source is required or not.

Active transducer doesn't require any power source for their operations. These transducers work on the principle of energy conversion. They generate an electrical signal that is proportional to the i/p. The best example of this transducer is thermocouple. Whereas passive transducer requires an external power source for their operation. They generate an o/p in the form of capacitance, resistance. Than that has to be converted to an equivalent voltage or current signal. The best example of passive transducer is a photocell.

What is the Difference Between Sensor and Transducer?

The physical devices, sensor and transducers are might used by some people interchangeably. These devices are used in numerous electrical and electronic gadgets and appliances. But, people fail to make a difference between sensor and transducer. Because, transducers are sometimes found in sensors.The main difference between sensor and transducer is, the sensor is a physical device, that senses a physical quantity and then converts it into signals which can be read by an instrument or the user. The transducer is also a physical device, that converts one form of energy into an another form. The best example of a transducer is an antenna. Because, it converts electricity to electromagnetic waves. A sensor also converts one form of energy to another, means it senses a physical quantity and converts it into an electrical signal.



9. ACCELEROMETER

An accelerometer is a device that measures changes in gravitational acceleration in a device it may be installed in. Accelerometers are used to measure acceleration, tilt and vibration in numerous devices.

At rest, an accelerometer measures 1g: the earth's gravitational pull, which registers 9.81 meters per second or 32.185 feet per second. Accelerometers that use the piezoelectric effect measure a small voltage change. Others measure capacitance between two components.

To sense motion in multiple directions, an accelerometer must be designed with multi-axis sensors or multiple linear axis sensors. Three linear accelerometers are adequate to measure movement in three dimensions.

Applications for accelerometers include:

- Monitoring devices in biology, engineering cars, industry, volcanology and more.
- Guidance devices in for telemetry in rocketry.
- Image orientation in smartphones.
- Input in smartphones, tablets and game controllers.

10. IoT WIRELESS CONNECTIVITY

The Internet of Things (IoT) starts with connectivity, but since IoT is a widely diverse and multifaceted realm, you certainly cannot find a one-size-fits-all communication solution.

Each solution has its strengths and weaknesses in various network criteria and is therefore best-suited for different IoT use cases.

1. LPWANs

Low Power Wide Area Networks (LPWANs) are the new phenomenon in IoT. By providing long-range communication on small, inexpensive batteries that last for years, this family of technologies is purpose-built to support large-scale IoT networks sprawling over vast industrial and commercial campuses. LPWANs can literally connect all types of IoT sensors – facilitating numerous applications from **remote monitoring**, **smart metering** and **worker safety** to **building controls**and **facility management**. Nevertheless, LPWANs can only send small blocks of data at a low rate, and therefore are better suited for use cases that don’t require high bandwidth and are not time-sensitive.

Also, not all LPWANs are created equal. Today, there exist technologies operating in both the licensed (NB-IoT, LTE-M) and unlicensed (e.g. MIOTY, LoRa, Sigfox etc.) spectrum with varying degrees of performance in key network factors. For example, while power consumption is a major issue for cellular-based, licensed LPWANs; Quality-of-Service and scalability are main considerations when adopting unlicensed technologies. Standardization is another important factor to think of if you want to ensure reliability, security, and interoperability in the long run.

2. Cellular (3G/4G/5G)

Well-established in the consumer mobile market, cellular networks offer reliable broadband communication supporting various voice calls and video streaming applications. On the downside, they impose very high operational costs and power requirements.

While cellular networks are not viable for the majority of IoT applications powered by battery-operated sensor networks, they fit well in specific use cases such as **connected cars** or **fleet management in transportation and logistics**. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services can all rely on the ubiquitous and high bandwidth cellular connectivity.

Cellular next-gen 5G with high-speed mobility support and ultra-low latency is positioned to be the future of autonomous vehicles and augmented reality. 5G is also expected to enable real-time video surveillance for **public safety**, real-time mobile delivery of medical data sets for **connected health**, and several **time-sensitive industrial automation**applications in the future.

3. Zigbee and Other Mesh Protocols

Zigbee is a short-range, low-power, wireless standard (IEEE 802.15.4), commonly deployed in mesh topology to extend coverage by relaying sensor data over multiple sensor nodes. Compared to LPWAN, Zigbee provides higher data rates, but at the same time, much less power-efficiency due to mesh configuration. Because of their physical short-range (< 100m), Zigbee and similar mesh protocols (e.g. Z-Wave, Thread etc.) are best-suited for medium-range IoT applications with an even distribution of nodes in close proximity. Typically, Zigbee is a perfect complement to Wi-Fi for various **home automation** use cases like smart lighting, HVAC controls, security and energy management, etc. – leveraging home sensor networks.

Until the emergence of LPWAN, mesh networks have also been implemented in industrial contexts, supporting several remote monitoring solutions. Nevertheless, they are far from ideal for many industrial facilities that are geographically dispersed, and their theoretical scalability is often inhibited by increasingly complex network setup and management.

4. Bluetooth and BLE

Defined in the category of Wireless Personal Area Networks, Bluetooth is a short-range communication well-positioned in the consumer marketplace. The new Bluetooth Low-Energy, also known as Bluetooth Smart is further optimized for **Consumer IoT** applications thanks to low power consumption.

BLE-enabled devices are mostly used in conjunction with electronic devices – often smartphones – that serve as a hub for transferring data to the cloud. Nowadays, BLE is widely integrated in **fitness and medical wearables** (e.g. smartwatches, glucose meters, pulse oximeters etc.) as well as **Smart Home devices** (e.g. door locks) – whereby data is conveniently communicated to and visualized on smartphones. In retail contexts, BLE can be coupled with **beacon** technology for enhanced customer services like in-store navigation, personalized promotions, and content delivery.

5. Wi-Fi / Wi-Fi HaLow

There is virtually no need to explain Wi-Fi (IEEE 802.11a/b/g/n), given its pervasiveness in both enterprise and home environments. However, in the IoT world, Wi-Fi plays a less significant role. Except for few applications like **digital signages** and **indoor security cameras**, Wi-Fi is not often a feasible solution for connecting IoT end devices because of its major limitations in coverage, scalability and power consumption. Instead, the technology can perform as a **back-end network** for offloading aggregated data from a central IoT hub to the cloud, especially in the Smart Homes. Critical security issues often hinder its adoption in industrial and commercial use cases.

A new, less known derivative of Wi-Fi – Wi-Fi HaLow (IEEE 802.11ah) – introduces noticeable improvements in range and energy efficiency that cater to a wider array of IoT use cases. Nonetheless, the protocol has received little traction and industry support so far, partly because of its low security. HaLow also operates in the 900 MHz frequency band only available in the USA, making it far from a global solution.

6. RFID

Radio Frequency Identification (RFID) uses radio waves to transmit small amounts of data from an RFID tag to a reader within a very short distance. Till now, the technology has facilitated a major revolution in **retail** and **logistics**.

By attaching an RFID tag to all sorts of products and equipment, businesses can track their inventory and assets in real-time – allowing for better stock and production planning as well as optimized **supply chain management**. Alongside increasing IoT adoption, RFID continues to be entrenched in the retail sector, enabling new IoT applications like smart shelves, self-checkout, and smart mirrors.

Key IoT Verticals	LPWAN (Star)	Cellular (Star)	Zigbee (Mostly Mesh)	BLE (Star & Mesh)	Wi-Fi (Star & Mesh)	RFID (Point-to-point)
Industrial IoT	●	○	○			
Smart Meter	●					
Smart City	●					
Smart Building	●		○	○		
Smart Home			●	●	●	
Wearables	○			●		
Connected Car					○	
Connected Health		●		●		
Smart Retail		○		●	○	●
Logistics & Asset Tracking	○	●				●
Smart Agriculture	●					

● Highly applicable ○ Moderately applicable

Each IoT wireless technology is relevant for different IoT verticals.

To quickly sum up, each IoT vertical and application has its own unique set of network requirements. Choosing the best wireless technology for your IoT use case means accurately weighing criteria in terms of range, bandwidth, QoS, security, power consumption, and network management.

11. RFID SYSTEMS

An RFID system consists of three components: a scanning antenna and transceiver (often combined into one reader, also known as an interrogator) and a transponder, the RFID tag. An RFID tag consists of a microchip, memory and antenna.

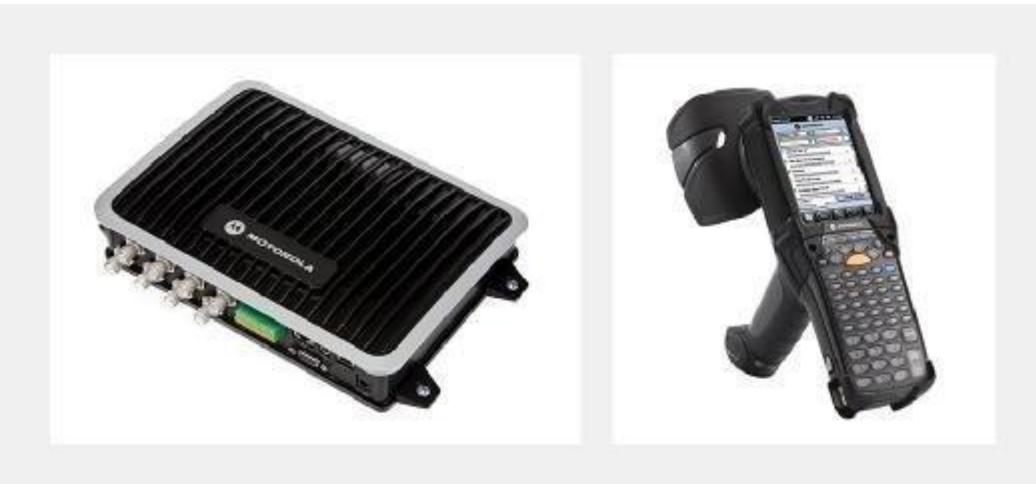
The RFID reader is a network-connected device that can be permanently attached or portable. It uses radio frequency waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

<u>Types of RFID tags</u>

There are two main types of RFID tags: active RFID and passive RFID. An active RFID tag has its own power source, often a battery. A passive RFID tag, on the other hand, does not require batteries; rather it 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.

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. Generally speaking, active RFID tags have a longer read range than passive RFID tags due to the stronger power source.



RFID frequencies: 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 range from 30 KHz to 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 systems range from 3 MHz to 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 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 run at 2.45 GHz and can be read from more than 30-plus feet away.

The frequency used will depend on the RFID application, with actual obtained distances sometimes varying considerably from what might be expected. For example, when the U.S. State Department announced it was to issue electronic passports enabled with an RFID chip, it said the chips would only be able to be read from approximately four inches away. However, the State Department was soon confronted with evidence that RFID readers could skim the information from the RFID tags from much farther than 4 inches, some claiming upward of 33 feet away, proving the difference between advertised and actual range can vary immensely.

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

RFID frequencies and ranges

FREQUENCY	BAND	RANGE
LF RFID	30-500 KHz, typically 125 KHz	Less than three feet
HF RFID	3-30 MHz, typically 13.56 MHz	Less than six feet
UHF RFID	300-960 MHz, typically 433 MHz	25+ feet
Microwave	2.45 GHz	30+ feet

RFID applications and use cases

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

The most common RFID application is for tracking and management. This includes pet and livestock tracking, inventory management and asset tracking, cargo and supply chain logistics, and vehicle tracking. RFID can also be used in retail for advertising customer service and loss control; in the supply chain for improved visibility and distribution; and in security situations for access control.

Multiple industries use RFID applications, including healthcare, manufacturing, retail, business and home use.

12. CONNECTIVITY OPTIONS FOR IoT

Connectivity is a critical piece of the IoT projects puzzle. Stakeholders need to find the most suitable connectivity option for their products and projects. With about 30 IoT connectivity options on the market today, their constant evolution and the development of new ones, this search can be difficult. New technologies such as LPWAN and 5G are gaining more attention, while others such as Bluetooth and Wi-Fi are evolving and thereby changing the IoT connectivity landscape. Let's explore how not to get lost among the choices when choosing the best IoT connectivity option for your business. To realize the potential of IoT, whole industries are working hard to develop the devices, and connectivity solutions to enable communication among the devices, in one ecosystem. It's no easy task, for a number of reasons.

First, the amount of collected data is growing, and current solutions are increasingly challenged to handle the rising data volume.

In addition, IoT app developers and device manufacturers must provide for interoperability of all the elements of the IoT ecosystem. The ideal situation is to make all the devices work without any coordination required among vendors. So far appliance manufacturers are trying to preserve a certain level of control over connectivity standards, with Samsung, LG and other tech companies announcing their own standards. And though there is no doubt that these devices will be made interoperable, interconnectivity remains a serious barrier.

IoT developers and device manufacturers must also strike a balance between three key parameters: bandwidth, range and power consumption. Programmers are trying to create a solution that would be a perfect combination of high bandwidth for transmitting large amounts of data over huge distances while consuming little battery power. But, at this point, that perfect solution doesn't exist. This means IoT developers must make trade-offs, perhaps prioritizing bandwidth over power consumption, or vice versa.

There is no one-size-fits-all protocol capable of supporting all technological and analytical tasks. But some solutions are better suited for specific use cases.

Classic Connectivity Solutions

The capacities of classic connectivity protocols are naturally limited to the expectations of past days, when the first IoT networks cropped up around smart home projects. Now these short-range wireless solutions are being modified and adapted to the new reality created by an avalanche of data from connected devices. Here we look at the traditional connectivity options, examining their advantages and disadvantages from the point of view of IoT projects.

<u>Wi-Fi</u>

Perfect solution for: data-intensive uses and in-building or campus environments, like home automation and house energy management.

Why? In most cases, Wi-Fi is 20 to 30 times quicker than Bluetooth Low Energy (BLE), making it a more suitable choice when the transmission of large files is needed.

Weak points: Transmitting large files comes at a cost of high power consumption. Wi-Fi was not designed expressly for IoT networks (though two recently developed IEEE standards, 802.11ah and 802.11ax, were). Sensors, key elements in IoT network development, are battery-based and transmit small amounts of data over huge distances. Consequently, they need another type of connectivity solution.

Bluetooth and Bluetooth Low Energy

Perfect solution for: personal IoT devices like wearables and fitness trackers, as well as beacons.

Why? Bluetooth has long been popular in the consumer electronics segment for its ability to continuously stream large amounts of data. And BLE was designed specifically for low-powered IoT devices. BLE is best suited for devices that transmit low volumes of data in bursts, as the devices are designed to save power when they are not transmitting data.

Weak points: Its application in industrial projects has been limited because of its very short-range connectivity and high battery consumption. Still, the low price of this solution attracts developers, who have introduced hybrid architecture schemes with Bluetooth, which help to overcome the Bluetooth short-range restriction. These schemes use Bluetooth for connecting dozens of endpoint devices to one master access device. In turn, the access device uses another, more expensive technology (for example, cellular) for connecting to the back end (which is referred to as Bluetooth bridging).

Mesh Technologies

Perfect solution for: in-house applications and neighboring projects like smart lighting, security systems, HVAC systems and remote controls.

Why? Mesh technologies such as ZigBee and Z-Wave use a system of interconnected nodes to carry small data packets over short to midrange distances.

Weak points: Mesh technology can be challenging in some implementations. For instance, interoperability between Zigbee gadgets needs to be preplanned. With Z-Wave, however, communication between devices is easily accomplished.

IoT Rapid Development: New Protocols on the Market

New connectivity solutions are being developed to tackle the challenges of more complex IoT projects like smart cities, smart agricultural practices, smart metering and other entities, which demand a new level of connectivity standards.

LPWAN

Perfect solution for: massive IoT projects like smart cities or smart agriculture.

Why? Low-power wide-area network (LPWAN) is an umbrella term for any network that allows communication over large distances (at least 500 meters of signal range from the gateway device to the endpoint) using minimal power. These networks are divided into licensed (LTE-M, NB-IoT and EC-GSM) and unlicensed (SigFox and LoRa-based-standards).

These solutions have been designed particularly for IoT; therefore, they're designed to send small amounts of data at longer intervals from a lot of endpoints, but within a long period (hence the need for low-power usage) and at longer distances.

Weak points: LPWAN technology is still in the early stages of deployment (the much discussed NB-IoT was presented only in 2016), and its full potential and disadvantages won't become clear until the networks have been implemented at a greater scale. Today, only 20% of the global population is covered by an LPWAN network; that low uptake prevents it from becoming a default solution within the next five years. However, LPWAN availability is growing rapidly, and by 2022 LPWAN technologies are expected to provide coverage for 100% of the world population.

5G

Perfect solution for: the most bandwidth-intensive applications, remote surgery and massive machine-type communications.

Why? As IoT solutions will be getting more elaborate and emit more data, a demand for a larger bandwidth will only be growing, and 5G is expected to face this challenge. The first public networks are not here yet (they are expected to be made available in 2020), and we can only make predictions about how this fifth generation of mobile technologies' extension to LTE technologies — already called "a game changer" by specialists — will function and how it will influence both software and mobile developers and end users. And these predictions are ambitious: By 2021, 5G's broad enablement of IoT use cases is expected to drive a whopping 70% of Global 2000 companies to spend $1.2 billion on connectivity management solutions.

Weak points: Time will be needed to make 5G universal. Plus, we still need to wait and see whether the reality will correspond with the high expectations.

13. WIRED INTERFACES

RS-232

In telecommunications, **RS-232**, **Recommended Standard 232**[1] refers to a standard originally introduced in 1960[2] for serial communicationtransmission of data. It formally defines signals connecting between a *DTE* (*data terminal equipment*) such as a computer terminal, and a *DCE*(*data circuit-terminating equipment* or *data communication equipment*), such as a modem. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pinout of connectors. The current version of the standard is *TIA-232-F Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, issued in 1997. The RS-232 standard had been commonly used in computer serial ports.

A serial port complying with the RS-232 standard was once a standard feature of many types of computers. Personal computers used them for connections not only to modems, but also to printers, computer mice, data storage, uninterruptible power supplies, and other peripheral devices.

RS-232, when compared to later interfaces such as RS-422, RS-485 and Ethernet, has lower transmission speed, short maximum cable length, large voltage swing, large standard connectors, no multipoint capability and limited multidrop capability. In modern personal computers, USB has displaced RS-232 from most of its peripheral interface roles. Many computers no longer come equipped with RS-232 ports and must use either an external USB-to-RS-232 converter or an internal expansion card with one or more serial ports to connect to RS-232 peripherals. Nevertheless, thanks to their simplicity and past ubiquity, RS-232 interfaces are still used—particularly in industrial machines, networking equipment, and scientific instruments where a short-range, point-to-point, low-speed wired data connection is fully adequate.

VIRTUAL SERIAL PORTS

In computing, a **serial port** is a serial communication interface through which information transfers in or out one bit at a time (in contrast to a parallel port).[1] Throughout most of the history of personal computers, data was transferred through serial ports to devices such as modems, terminals, and various peripherals.

While such interfaces as Ethernet, FireWire, and USB all send data as a serial stream, the term *serial port* usually identifies hardware compliant to the RS-232 standard or similar and intended to interface with a modem or with a similar communication device.

Modern computers without serial ports may require USB-to-serial converters to allow compatibility with RS-232 serial devices. Serial ports are still used in applications such as industrial automation systems, scientific instruments, point of sale systems and some industrial and consumer products. Server computers may use a serial port as a control console for diagnostics. Network equipment (such as routers and switches) often use serial console for configuration. Serial ports are still used in these areas as they are simple, cheap and their console functions are highly standardized and widespread. A serial port requires very little supporting software from the host system.

Fig: male D-subminiature connector used for a serial port on an IBM PC compatible computer along with the serial port symbol.

RS-485 PROTOCOL

This information touches on some of the most commonly asked aspects of RS-485 communications. B&B Electronics has a free application note available on RS-422/485 that gives a more complete picture of RS-485 networks. Request B&B's RS-422/485 Application Note, available by mail or on our websites, www.bb-elec.com or www.bb-europe.com

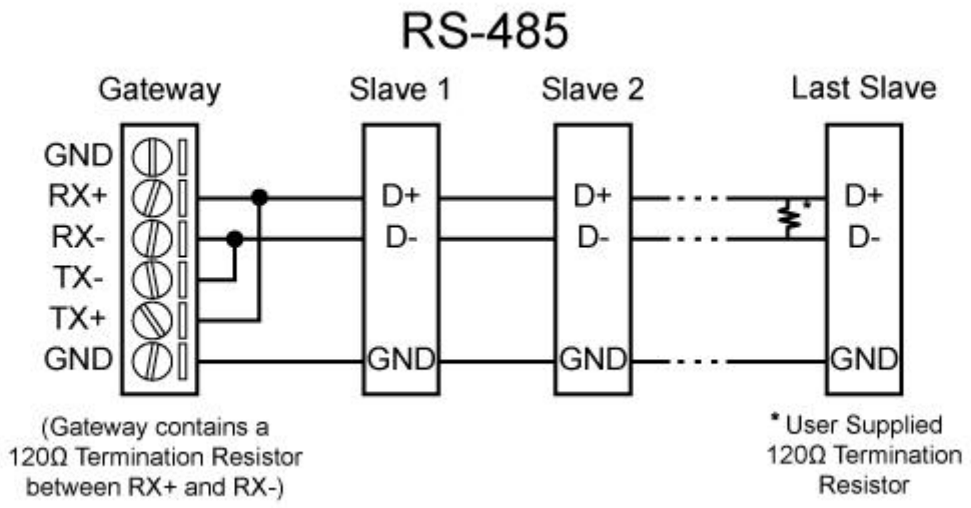
What is an RS-485 network? RS-485 allows multiple devices (up to 32) to communicate at half-duplex on a single pair of wires, plus a ground wire (more on that later), at distances up to 1200 meters (4000 feet). Both the length of the network and the number of nodes can easily be extended using a variety of repeater products on the market.

How does the hardware work? Data is transmitted differentially on two wires twisted together, referred to as a "twisted pair." The properties of differential signals provide high noise immunity and long distance capabilities. A 485 network can be configured two ways, "two-wire" or "four-wire." In a "two-wire" network the transmitter and receiver of each device are connected to a twisted pair. "Four-wire" networks have one master port with the transmitter connected to each of the "slave" receivers on one twisted pair. The "slave" transmitters are all connected to the "master" receiver on a second twisted pair. In either configuration, devices are addressable, allowing each node to be communicated to independently. Only one device can drive the line at a time, so drivers must be put into a high-impedance mode (tri-state) when they are not in use. Some RS-485 hardware handles this automatically. In other cases, the 485 device software must use a control line to handle the driver. (If your 485 device is controlled through an RS-232 serial port, this is typically done with the RTS handshake line.) A consequence of tri-stating the drivers is a delay between the end of a transmission and when the driver is tri-stated. This turn-around delay is an important part of a two-wire network because during that time no other transmissions can occur (not the case in a four-wire configuration). An ideal delay is the length of one character at the current baud rate (i.e. 1 ms at 9600 baud). The device manufacturer should be able to supply information on the delay for their products.

Two-wire or four-wire? Two-wire 485 networks have the advantage of lower wiring costs and the ability for nodes to talk amongst themselves. On the downside, two-wire mode is limited to half-duplex and requires attention to turn-around delay. Four-wire networks allow full-duplex operation, but are limited to master-slave situations (i.e. a "master" node requests information from individual "slave" nodes). "Slave" nodes cannot communicate with each other. Remember when ordering your cable, "two-wire" is really two wires + ground, and "four-wire" is really four wires + ground.

How does the software work? 485 software handles addressing, turn-around delay, and possibly the driver tri-state features of 485. Determine before any purchase whether your software handles these features. Remember, too much or too little turn-around delay can cause troubleshooting fits, and delay should be a function of baud rate. If you're writing your own software or using software written for an RS-232 application, be certain that provisions are made for driver tri-state control. Luckily, there are usually hardware alternatives for controlling driver tri-stating. Contact B&B Technical Support for further details.

Connecting a multidrop 485 network. The EIA RS-485 Specification labels the data wires "A" and "B", but many manufacturers label their wires "+" and "-". In our experience, the "-" wire should be connected to the "A" line, and the "+" wire to the "B" line. Reversing the polarity will not damage a 485 device, but it will not communicate. This said, the rest is easy: always connect A to A and B to B.



UNIVERSAL SERIAL BUS

Universal Serial Bus (**USB**) is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supplybetween computers, peripheral devices and other computers.[3] Released in 1996, the USB standard is currently maintained by the USB Implementers Forum (USB-IF). There have been three generations of USB specifications: USB 1.*x*, USB 2.0 and USB 3.*x*; the fourth called USB4 is scheduled to be published in the middle of 2019.

USB was designed to standardize the connection of peripherals to personal computers, both to communicate with and to supply electric power. It has largely replaced interfaces such as serial ports and parallel ports, and has become commonplace on a wide range of devices.

USB connectors have been increasingly replacing other types for battery chargers of portable devices.

Examples of peripherals that are connected via USB include keyboards, pointing devices, digital still and video cameras, printers, portable media players, disk drives and network adapters.

14. CONCLUSION

I am presenting this project on the topic **Initiatives For Digitilisation**. In this project I have tried to give all the important things about my project.

This project contains about **Digitilisation,Sensors And IoT Wireless Technology,**

RFID Tags and Wired Interfaces. I have given information in this project by consulting by my mentor **MR. Gaurav Anand** and from useful websites.

I have tried my best to avoid mistakes. If there is any mistake, please avoid it.

Thanks.

15. BIBLOGRAPHY

- www.wikipedia.com
- Techopedia