Course Activity Report

What is Internet of Things? What does the term 'Things' refer to?

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Here, the term 'Things' refer to the everyday objects that are now embedded with such devices. For example, Washing Machines, Fridges, TV, etc. are now equipped with such peripherals that puts them in the category of IoT.

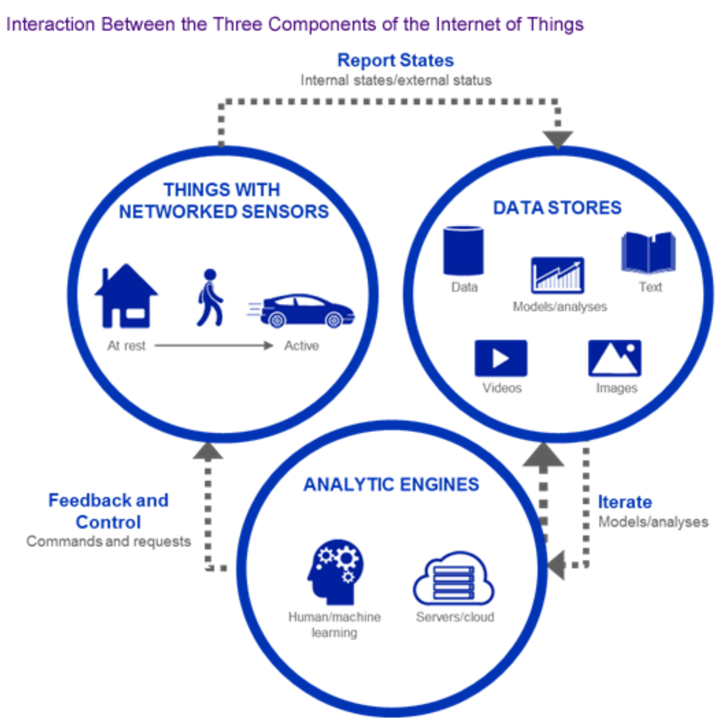
Discuss the History of IoT.

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke vending machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold or not. 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. 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". 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.

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet for things". At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.

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.

The key driving force behind the Internet of things is the MOSFET (metal-oxide-semiconductor field-effect transistor, or MOS transistor), which was originally invented by Mohamed M. Atalla and Dawon Kahng at Bell Labs in 1959. The MOSFET is the basic building block of most modern electronics, including computers, smartphones, tablets and Internet services. MOSFET scaling miniaturization at a pace predicted by Dennard scaling and Moore's law has been the driving force behind technological advances in the electronics industry since the late 20th century. MOSFET scaling has been extended into the early 21st century with advances such as reducing power consumption, silicon-on-insulator (SOI) semiconductor device fabrication, and multi-core processor technology, leading up to the Internet of things, which is being driven by MOSFETs scaling down to nanoelectronic levels with reducing energy consumption.[



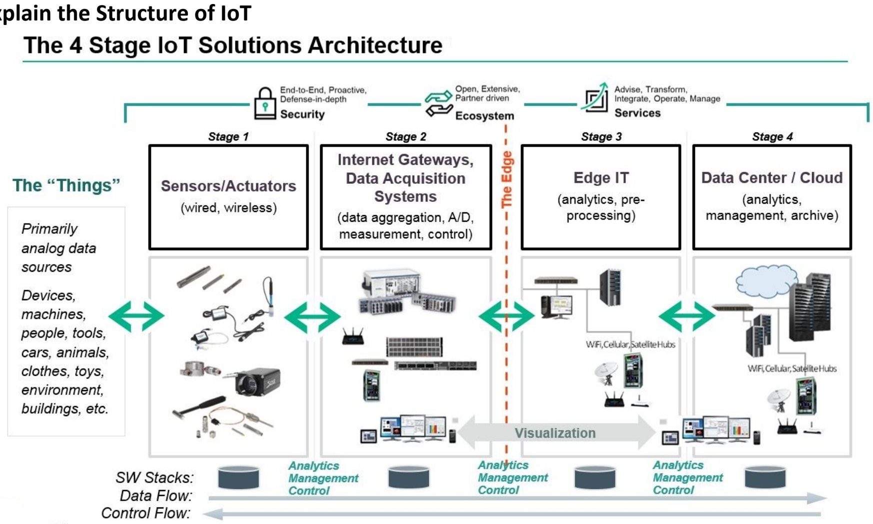
Explain how IoT works?

All IoT devices are equipped with sensors that sense the environment and get meaningful information from it. This Information is passed to the Cloud/Server via the established gateway where it can be constructed/processed furhur.

List and explain all capablities of IoT.

The core capablities of IoT are
1. Connectivity
2. Control of Device
3. Device Management
4. Querying of Data.

Explain the Structure of IoT



In simple terms, the 4 Stage IoT architecture consists of
1. Sensors and actuators
The outstanding feature about sensors is their ability to convert the information obtained in the outer world into data for analysis. In other words, it's important to start with the inclusion of sensors in the 4 stages of an IoT architecture framework to get information in an appearance that can be actually processed.
For actuators, the process goes even further — these devices are able to intervene the physical reality. For example, they can switch off the light and adjust the temperature in a room.
Because of this, sensing and actuating stage covers and adjusts everything needed in the physical world to gain the necessary insights for further analysis.

2. Internet getaways and Data Acquisition Systems
Even though this stage of IoT architecture still means working in a close proximity with sensors and actuators, Internet getaways and data acquisition systems (DAS) appear here too. Specifically, the later connect to the sensor network and aggregate output, while Internet getaways work through Wi-Fi, wired LANs and perform further processing.
The vital importance of this stage is to process the enormous amount of information collected on the previous stage and squeeze it to the optimal size for further analysis. Besides, the necessary conversion in terms of timing and structure happens here.
In short, Stage 2 makes data both digitalized and aggregated.

3. Edge IT
During this moment among the stages of IoT architecture, the prepared data is transferred to the IT world. In particular, edge IT systems perform enhanced analytics and pre-processing here. For example, it refers to machine learning and visualization technologies. At the same time, some additional processing may happen here, prior to the stage of entering the data center.
Likewise, Stage 3 is closely linked to the previous phases in the building of an architecture of IoT. Because of this, the location of edge IT systems is close to the one where sensors and actuators are situated, creating a wiring closet. At the same time, the residing in remote offices is also possible.

4. Data center and cloud.
The main processes on the last stage of IoT architecture happen in data center or cloud. Precisely, it enables in-depth processing, along with a follow-up revision for feedback. Here, the skills of both IT and OT (operational technology) professionals are needed. In other words, the phase already includes the analytical skills of the highest rank, both in digital and human worlds. Therefore, the data from other sources may be included here to ensure an in-depth analysis.
After meeting all the quality standards and requirements, the information is brought back to the physical world — but in a processed and precisely analyzed appearance already.

What do you mean by a Sensor?
In the broadest definition, a sensor is a device, module, machine, or subsystem whose purpose is to detect events or changes in its environment and send the information to other electronics, frequently a computer processor. A sensor is always used with other electronics.

What is the difference between a sensor and a transducer?
Sensor and Transducer are physical devices that are used in electrical, electronic and many other types of gadgets and appliances. These are physical devices that are used in electrical and electronic gadgets and are often encountered by mechanics. While a sensor is a device that, as its name signifies, measures a physical quantity and then converts it into signals that can be read by the user or by any other instrument. Transducer, on the other hand is a physical device (Electrical, electro-mechanical, electromagnetic, photonic or photovoltaic) that converts either one type of energy into another or a physical attribute into another for the purposes of measurement or transfer of information.

Define Transducer. Give detailed classification of transducers.
A transducer is a device that converts energy from one form to another. Usually a transducer converts a signal in one form of energy to a signal in another.

List and explain the different types of sensors and transducers.
Types of Sensors
- Active sensors require an external power source to operate, which is called an excitation signal. The signal is modulated by the sensor to produce an output signal. For example, a thermistor does not generate any electrical signal, but by passing an electric current through it, its resistance can be measured by detecting variations in the current or voltage across the thermistor.
- Passive sensors, in contrast, generate an electric current in response to an external stimulus which serves as the output signal without the need of an additional energy source. Such examples are a photodiode, and a piezoelectric sensor, thermocouple.

Types of Transducers
- Electrical
- Mechanical

What do you mean by embedded intelligence?
Embedded intelligence is also sometimes called “embedded analytics.” The idea is that a system can monitor itself with specific analytics that fine-tune its own operations in some way.

Discuss the roles of embedded systems in IoT.
Embedded system is basically the study of how to setup a device that is hardware or software or both that is embedded in a larger system and is mostly a real time system. An embedded system usually consists of a microcontroller programmed to do a specific job.
Internet of things is how these devices communicate with each other directly and indirectly to serve a specific purpose. Directly is when two devices or more talk peer to peer. And decide actions based on what the other device says. Indirect is when all of these devices are connected to a single node and the node receives and transmits signals to the devices and intercommunicate is thus established.

Discuss the current status and future prospect 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.

According to the report published on by deloitte and Nasscom, The Internet of Things (IoT) market is expected to reach $ 9 billion by 2020. By the end of 2020 more than 1.9 billion devices are expected to be connected in India which leads to grow this market 31 times from the current market share of 5.6 this year.

Indian IoT market has huge potential and expected to grow across industries in manufacturing, automotive, transportation and logistics. IoT is set to become a major differentiation in driving the next generation of services and products.

Write a short note on IoT as "networks of networks"

The Internet of things (IoT) is the inter-networking of physical devices, vehicles , smart-devices, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. In this way the IoT establishes a large amount of networks. This is why it is referred to as "Networks of networks"

How is knowledge management carried out in IoT?

A knowledge management system (KMS) is a system for applying and using knowledge management principles. These include data-driven objectives around business productivity, a competitive business model, business intelligence analysis and more.

A knowledge management system is made up of different software modules served by a central user interface. Some of these features can allow for data mining on customer input and histories, along with the provision or sharing of electronic documents. Knowledge management systems can help with staff training and orientation, support better sales, or help business leaders to make critical decisions

What do you feel is the future of IoT?

It's no secret that the IoT market is now very actively evolving and growing, dozens of new startups appear every day. According to the research of many large companies and publishing houses, such as Forbes for example:

B2B spending on IoT technologies, apps and solutions will reach €250B ($267B) by 2020

Spending on IoT applications is predicted to generate €60B ($64.1B) by 2020

IoT Analytics spending is predicted to generate €20B ($21.4B) by 2020

These crazy numbers show how demanded this market among investors and that in the coming years it will only grow. So if you're still thinking about the idea of a startup, it's time to look at IoT market.

So even this simple examples can show us, that IoT is our near future.

Suggest how can it smoothen/benefit the domestic & industrial activities.

Domestic/Consumer IoT devices and services are oriented toward individual users or families. This includes products like Amazon's Echo (Fig. 2) or Google's Nest Thermostat (see "An Elegant Thermostat Designed For The Internet"). Hardware tends to be designed for low cost and limited lifetime and maintenance. A device is likely to have a shelf life measured in months or years, with new versions quickly replacing older products on store shelves. The device lifetime may be many years, but replacement rather than maintenance or upgrade is the norm.

Industrial IoT might be viewed as rugged, long-term commercial IoT, but that overlooks the differences in IIoT's design and infrastructure. Like many commercial solutions, IIoT solutions often target existing automated industrial systems. The difference is that these systems may be older, so the level of sensors is often based on what was available. They provide sufficient information to control the industrial process, but additional information would be useful if it's possible to incorporate more sensors. Such sensors might track the status of components such as plumbing. Sometimes, it can provide supplemental information about system wear and tear to anticipate maintenance requirements.

List all the areas of application of IoT.

The extensive set of applications for IoT devices is often divided into consumer, commercial, industrial, and infrastructure spaces.

- **<u>Consumer applications</u>**

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

  - Smart home

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off.
A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's HomeKit, manufacturers can have their home products and accessories controlled by an application in iOS devices such as the iPhone and the Apple Watch. This could be a dedicated app or iOS native applications such as Siri. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub. In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz.

  - Elder care

One key application of a smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.
The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.

- **Commercial application**
  - Medical and healthcare

The Internet of Medical Things (IoMT), (also called the Internet of health things), is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. The IoMT has been referenced as "Smart Healthcare", as the technology for creating a digitised healthcare system, connecting available medical resources and healthcare services.
IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialised implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used "to analyse, capture, transmit and store health statistics from multiple resources, including sensors and other biomedical acquisition systems".
Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.
Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and-throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wirelessly powered disposable

sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.
As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar,to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information. Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behaviour. This can lead to more accurate underwriting and new pricing models.
The application of the IOT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.

- Transportation

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance. In Logistics and Fleet Management, for example, an IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send specific alerts when management exceptions occur (delays, damages, thefts, etc.). This can only be possible with the IoT and its seamless connectivity among devices. Sensors such as GPS, Humidity, and Temperature send data to the IoT platform and then the data is analyzed and then sent to the users. This way, users can track the real-time status of vehicles and can make appropriate decisions. If combined with Machine Learning, then it also helps in reducing traffic accidents by introducing drowsiness alerts to drivers and providing self-driven cars too.

- V2X communications

In vehicular communication systems, vehicle-to-everything communication (V2X), consists of three main components: vehicle to vehicle communication (V2V), vehicle to infrastructure communication (V2I) and vehicle to pedestrian communications (V2P). V2X is the first step to autonomous driving and connected road infrastructure.

- Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. The integration of the Internet with building energy management systems in order to create energy efficient and IOT-driven "smart buildings".
The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors.
The integration of smart devices in the built environment and how they might to know how to be used in future applications.

- **Industrial applications**

Also known as IIoT, industrial IoT devices acquire and analyze data from connected equipment, (OT) operational technology, locations and people. Combined with operational technology (OT) monitoring devices, IIOT helps regulate and monitor industrial systems.

- Manufacturing

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyber-physical space, it opens the door to create whole new business and market opportunities for manufacturing.[59] Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well.[60] The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.
Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Industrial management systems can also be integrated with smart grids, enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.

Industrial IoT (IIoT) in manufacturing could generate so much business value that it will eventually lead to the Fourth Industrial Revolution, also referred to as Industry 4.0. The potential for growth from implementing IIoT may generate $12 trillion of global GDP by 2030.

Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes.
An IoT-enabled intelligent system of such cases was proposed in 2001 and later demonstrated in 2014 by the National Science Foundation Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at the University of Cincinnati on a bandsaw machine in IMTS 2014 in Chicago. Bandsaw machines are not necessarily expensive, but the bandsaw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, advising users when is the best time to replace the belt. This will significantly improve user experience and operator safety and ultimately save on costs.

- **Agriculture**

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs.
In August 2018, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide. The specific computer programs used in the process fall under the Azure Machine Learning and the Azure IoT Hub platforms.

- Infrastructure applications

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. The IoT can benefit the construction industry by cost saving, time reduction, better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

- Metropolitan scale deployments

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is gradually being built, with approximately 70 percent of the business district completed as of June 2018. Much of the city is planned to be wired and automated, with little or no human intervention.
Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants has already seen 18,000 downloads of its city smartphone app. The app is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda, and more. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.
Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. Using its RPMA (Random Phase Multiple Access) technology, San Diego-based Ingenu has built a nationwide public network for low-bandwidth data transmissions using the same unlicensed 2.4 gigahertz

spectrum as Wi-Fi. Ingenu's "Machine Network" covers more than a third of the US population across 35 major cities including San Diego and Dallas. French company, Sigfox, commenced building an Ultra Narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far.[85][86] Cisco also participates in smart cities projects. Cisco has started deploying technologies for Smart Wi-Fi, Smart Safety & Security, Smart Lighting, Smart Parking, Smart Transports, Smart Bus Stops, Smart Kiosks, Remote Expert for Government Services (REGS) and Smart Education in the five km area in the city of Vijaywada. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.

- Energy management

Significant numbers of energy-consuming devices (e.g. switches, power outlets, bulbs, televisions, etc.) already integrate Internet connectivity, which can allow them to communicate with utilities to balance power generation and energy usage and optimize energy consumption as a whole. These devices allow for remote control by users, or central management via a cloud-based interface, and enable functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). The smart grid is a utility-side IoT application; systems gather and act on energy and power-related information to improve the efficiency of the production and distribution of electricity. Using advanced metering infrastructure (AMI) Internet-connected devices, electric utilities not only collect data from end-users, but also manage distribution automation devices like transformers.

- Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.

- Living Lab

Another example of integrating the IoT is Living Lab which integrates and combines research and innovation process, establishing within a public-private-people-partnership. There are currently 320 Living Labs that use the IoT to collaborate and share knowledge between stakeholders to co-create innovative and technological products. For companies to implement and develop IoT services for smart cities, they need to have incentives. The governments play key roles in smart cities projects as changes in policies will help cities to implement the IoT which provides effectiveness, efficiency, and accuracy of the resources that are being used. For instance, the government provides tax incentives and cheap rent, improves public transports, and offers an environment where start-up companies, creative industries, and multinationals may co-create, share common infrastructure and labor markets, and take advantages of locally embedded technologies, production process, and transaction costs. The relationship between the technology developers and governments who manage city's assets, is key to provide open access of resources to users in an efficient way.

- **Military Applications**

The Internet of Military Things (IoMT) is the application of IoT technologies in the military domain for the purposes of reconnaissance, surveillance, and other combat-related objectives. It is heavily influenced by the future prospects of warfare in an urban environment and involves the use of sensors, munitions, vehicles, robots, human-wearable biometrics, and other smart technology that is relevant on the battlefield.

- Internet of Battlefield Things

The Internet of Battlefield Things (IoBT) is a project initiated and executed by the U.S. Army Research Laboratory (ARL) that focuses on the basic science related to IoT that enhance the capabilities of Army soldiers. In 2017, ARL launched the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA), establishing a working collaboration between industry, university, and Army researchers to advance the theoretical foundations of IoT technologies and their applications to Army operations.

- Ocean of Things

The Ocean of Things project is a DARPA-led program designed to establish an Internet of Things across large ocean areas for the purposes of collecting, monitoring, and analyzing environmental and vessel activity data. The project entails the deployment of about 50,000 floats that house a passive sensor suite that autonomously detect and track military and commercial vessels as part of a cloud-based network.

With context to IoT, explain the following:

- **Interoperablity in IoT**

In the future, the Internet of Things may be a non-deterministic and open network in which auto-organized or intelligent entities (web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the object's ability to detect changes in the environment (faults affecting sensors) and introduce suitable mitigation measures constitutes a major research trend,[112] clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation, but more sophisticated forms of intelligence are requested to permit sensor units and intelligent cyber-physical systems to be deployed in real environments.

- **Integrations of sensors and actuators.**

IoT system architecture, in its simplistic view, consists of three tiers: Tier 1: Devices, Tier 2: the Edge Gateway, and Tier 3: the Cloud. Devices include networked things, such as the sensors and actuators found in IIoT equipment, particularly those that use protocols such as Modbus, Zigbee, or proprietary protocols, to connect to an Edge Gateway. The Edge Gateway consists of sensor data aggregation systems called Edge Gateways that provide functionality, such as pre-processing of the data, securing connectivity to cloud, using systems such as WebSockets, the event hub, and, even in some cases, edge analytics or fog computing. The final tier includes the cloud application built for IIoT using the microservices architecture, which are usually polyglot and inherently secure in nature using HTTPS/OAuth. It includes various database systems that store sensor data, such as time series databases or asset stores using backend data storage systems (e.g. Cassandra, Postgres). The cloud tier in most cloud-based IoT system features event queuing and messaging system that handles communication that transpires in all tiers. Some experts classified the three-tiers in the IIoT system as edge, platform, and enterprise and these are connected by proximity network, access network, and service network, respectively.

Explain the use of data analytics & cloud computing in IoT.

The definition of the Internet of Things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and 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 intelligence can be offered at three levels: IoT devices, Edge/Fog nodes, and Cloud computing. The need for intelligent control and decision at each level depends on the time sensitiveness of the IoT application. For example, an autonomous vehicle's camera needs to make real-time obstacle detection to avoid an accident. This fast decision making would not be possible through transferring data from the vehicle to cloud instances and return the predictions back to the vehicle. Instead, all the operation should be performed locally in the vehicle. Integrating advanced machine learning algorithms including deep learning into IoT devices is an active research area to make smart objects closer to reality. Moreover, it is possible to get the most value out of IoT deployments through analyzing IoT data, extracting hidden information, and predicting control decisions. A wide variety of machine learning techniques have been used in IoT domain ranging from traditional methods such as regression, support vector machine, and random forest to advanced ones such as convolutional neural networks, LSTM, and variational autoencoder.

What do you mean by sensor cloud?

Sensor cloud is the infrastructure constituting WSN and cloud capable of monitoring the sensor data, sensor position and data origin.

The Sensor-Cloud Infrastructure virtualizes a physical sensor as a virtual sensor on the cloud computing. Dynamic grouped virtual sensors on cloud computing can be automatic provisioned when the users need them. The approach to enable the sensor management capability on cloud computing. Since the resource and capability of physical sensor devices is limited, the cloud computing on the IT infrastructure can be behalf of the sensor management such as availability and performance of physical sensors.

Recent developments in sensor networks and cloud computing saw the emergence of a new platform called sensor-clouds. While the proposition of such a platform is to virtualise the management of physical sensor devices, we are seeing novel applications been created based on a new class of social sensors. Social sensors are effectively a human-device combination that sends torrent of data as a result of social interactions and social events. The data generated appear in different formats such as photographs, videos and short text messages. Unlike other sensor devices, social sensors operate on the control of individuals via their mobile devices such as a phone or a laptop. And unlike other sensors that generate data at a constant rate or format, social sensors generate data that are spurious and varied, often in response to events as individual as a dinner outing, or a news announcement of interests to the public. This collective presence of social data creates opportunities for novel applications never experienced before.