Define IoT. Discuss various application areas of IoT.

- Internet of Things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting things based on existing and evolving interoperable information and communication technologies.

Application areas of IoT:

- Smart Home:

Wouldn't you love it if you could switch on the AC before reaching home or switch off the lights after leaving home? The smart home is one of the most popular applications of IoT.

The cost of owning a house is the biggest expense in a homeowner’s life. Smart homes are promised to save the time, money and energy.

- Smart cities:

The smart city is another powerful application of IoT. It includes smart surveillance, environment monitoring, automated transformation, urban security, smart traffic management, water distribution, smart healthcare etc.

- Wearables:
Wearables are devices that have sensors and software installed which can collect data about the user which can be later used to get the insights about the user. They must be energy efficient and small sized.

- **Connected cars:**

  A connected car is able to optimize its own operation, maintenance as well as passenger’s comfort using sensors and internet connectivity.

- **Smart retail:**

  Retailers can enhance the in-store experience of the customers using IoT. The shopkeeper can also know which items are frequently bought together using IoT devices.

- **Smart healthcare:**

  People can wear the IoT devices which will collect data about user's health. This will help users to analyze themselves and follow tailor-made techniques to combat illness. The doctor also doesn't have to visit the patients in order to treat them.

**Explain time for convergence for IoT.**

- We are in an age of smartphones.
- However, they cannot run user-driven applications which are connected to sensors.
- Some applications are there but they still do not work properly.
- So, the steps towards IoT will be:
1) The coherence of object capabilities and behaviour:
   - There will be a large number of objects available with sensing and actuation capabilities for information processing.

2) The coherence of application interactivity:
   - The applications' interaction will increase, the complexity will increase and the boundaries between the applications will be unclear to a high degree.

3) The coherence of corresponding technology approaches:
   - Development of robotics, smart cities, the future internet will evolve and ultimately merge with IoT.

4) The coherence of real and virtual world:
   - Today, the real and virtual worlds are seen as two antagonistic conceptions but they will converge with the help of IoT in future.
Discuss issues of IoT.

- Major issues related to IoT are:

1) How will the devices be named and organized?
   - How will we name the devices? How will we be able to develop new naming schemes? One solution for this is to use the DNS. It will ensure that we don’t have to create any new protocols.

2) How will the devices communicate with each other?
   - We will need some standards to ensure interoperability of devices so that each and every type of device can communicate with each other. We will need cloud-based servers to achieve this feature.

3) How is the performance measurement and optimized?
   - The amount of data keeps on growing with the number of devices. This data will put a lot of pressure on the network and the performance will be degraded. How will manufacturers ensure optimal performance?

4) How are security and privacy ensured?
   - Security and privacy of data are two of the biggest issues surrounding IoT. If the security system fails, every IoT device can be under threat and all the information will lose its privacy. There are some big data tools which can help but this will still remain the biggest concern for the users as well as the manufacturers.

5) How will the devices be maintained?

Maintenance becomes an issue when we are dealing with billions of IoT devices connected to the internet. We will need a strong and secure OS that can handle these many devices and performs optimally.
Define M2M. Explain reasons for shifting from M2M to IoT.

- M2M: Machine to Machine (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.

Here are the key factors responsible for a shift from M2M towards IoT:

1) Moving away from an isolated solution to an open environment

2) Use of IP and web as a technology toolbox

3) Current internet as a foundation for enterprise and government operations

4) Multimodal sensing and actuation

5) Knowledge creating technologies

6) General move towards horizontal layering of both technology and business

Explain smart parking application of IoT with the figure.

- A good smart parking system does not only be aware of the occupancy status but also guides the user to it too.
- There should be no human intervention in this parking system.
- The system will have occupancy sensors which will check if the slot is occupied by car or not.
- There will be gateway devices which transmit the occupancy status to the server.
- It will collect data from sensors and send it to the server.
- The server will calculate which slots are empty based on the data.
- Then, it will communicate with the user’s mobile application, show the parking map and the empty slots.
- This way, the user will not have to find empty spots and it will save time, money and energy.
The design for the smart parking system will look like this:

Explain the smart home application of IoT with the figure.

- The smart home is one of the most popular applications of IoT.
- Wouldn’t you love to be able to switch off the lights after leaving home or turning on the AC before reaching home?
- Smart home will save energy, time and money of users.
- Every appliance, sensor, and service in the home will be connected to the internet.
- Everything in the house will be accessed by an application on the user’s smartphone.
- Following is the figure:
Explain eHealth IoT applications.

- IoT will make a huge impact on the healthcare sector.
- These are some of the application of IoT in eHealth.

1) There will be remote monitoring systems and emergency notification system. These systems will help the patient measure blood pressure level and heart rate by wearing IoT devices. There will be more advanced devices to monitor specialized implants in future.

2) There will be real-time location monitoring system which helps the doctor check patient's location and reach immediately in case of emergency. Wheelchairs, nebulizers, pumps etc. can be tagged and reached easily with the help of IoT.

3) The patient's data will be uploaded to the cloud so that every medical person can find it easily without patient's help. IoT promises to bring down the cost of medical services and improve the quality. It will help the doctors reach patients faster and it will be affordable to the patients too.

4) IoT will also help in the research area in the healthcare sector. The researchers will be able to find a lot of new things and concepts which they can make reachable to patients using IoT.
devices. For example, there are wearable devices for dementia patients who have a habit of forgetting things, apps for patients to guide them about their medicine dose etc.

5) There will be IoT devices which measure patient’s condition and provide accurate diet plans and exercise schedules for each individual.

- So, these were some of the few huge applications of IoT in health care.
- There are a lot of issues that the manufactures will have to face in order to achieve this.
- Some of the issues are:
  - Meeting the demand for number of resources
  - Motivate people to share their medical information online
  - Keep the services at reasonable cost
  - Real timeliness
  - Developing smart hospitals

**Explain security concerns for the smart home.**

- Here are the biggest security concerns for smart home:

1) Hacking the connected thermostats:

- A thermostat is a device which is connected to the internet and maintains the temperature of the house.
- Hacking of such a device may not sound like a big deal but it is.
- By hacking the thermostat, hackers can know how many people are there in the house, their schedules, their sleep timings as every mentioned thing affects the temperature.

2) Hacking the smart TV:

- This may again not sound like a big deal but it actually is.
- Some smart TVs come with a camera that can be hacked easily by the hackers.
- This way they can spy on you and your family even when the TV is not turned on.
3) Hacking the security systems:

- Many smart home users manage their security systems like door locks, cameras and other things with the help of a mobile app.
- Now imagine someone hacks this system.
- This way they can enter your home when you are not around and also spy on you using the cameras.

4) Eavesdropping:

- Hackers can hack the communication systems like e-mail, phone call etc. that the user uses and can steal a lot of valuable information about the user.

5) Hacking the lighting system:

- Lighting systems are very important in a smart home.
- If the hackers hack them, they can change the amount of power the house is consuming leading to huge financial losses to the user as they will have to pay a huge amount of money as electricity bill.
- So, these are the primary security concerns for a smart home.

**Explain reasons to converge the technologies and shift to IoT.**

- Improved customer engagement and communication
- Support for wide range of data collection
- Automation in almost object
- Improves the quality of life of people
- Saves time
- Saves money
- Optimizes technology

**Explain research directions for IoT.**
The goal of the IoT Strategic Research Agenda is to direct the research efforts to focus areas of identified significant value creation.

The latest computing and communication technologies are going to transform our corporate and personal environment radically.

These new technologies like cloud networking, nano-electronics, network virtualization etc. require an internet connection all the time.

Mobile data traffic will increase rapidly.

Mobile operators are facing a problem to provide the required bandwidth to the clients and customers due to that.

The extra frequency spectrum is not available in some countries.

So, there can be an integration of existing Wi-Fi network into the mobile eco-system and also this will have a big impact on IoT eco-system.

The architecture of mobile devices will change as the baseband chip takes control of the routine process.

So, it is necessary to develop a chip that integrates all the process. It is called a multicom chip.

Today many European projects address IoT technologies, knowledge and also it has been mentioned that these topics can be heterogeneous and specialized also there is a strong need for integration of the individual results.

In this context, the integration of knowledge has been conceptualized as the process through which some specialized cognizance situated in multiple projects across Europe is applied and assimilated.

The agenda of strategic research and innovation has been developed with the proper support of a European-led community of interrelated projects and their stakeholders with a dedication to the innovation, creation, development, and use of the IoT technology.

**Explain security concerns for the industry in IoT.**

- These are some of the major security concerns for industries:

  1) Rush in production:
- The consumer demand is increasing day by day and industries are not focusing on security of the products that they produce in order to meet the demands quickly.
- This can lead to hazardous results.
- It can cause problems like malware vulnerabilities, man in the middle, DDoS etc. attacks.

2) No standardization:

- There are no firm standards that the companies have to follow while developing their products.
- This can lead to security issues on some devices.
- Thus, standardization is necessary when we are talking about every device being connected to the internet.

3) Privacy:

- Privacy is another huge concern for industries.
- Information that the user communicates with the device will be going on the internet.
- So, the industries have to ensure the safety of that data. Otherwise, the users will lose their trust and the idea of IoT can fail.

4) Protecting from other corporations:

- Some users may not want to share their data with everyone.
- So, protecting the data from other corporations is equally important as protecting it from hackers.

5) Upgrades:

- Mostly the computers upgrade the software by itself as the users are too lazy to do that.
- But when we talk about IoT, the safety of your data is in the user's hands. So, this will require the user to update every software and device every time and that can raise some security issues.

6) More devices, more problems:
Last but not the least is the number of increasing devices connected to the internet. These all above-mentioned problems will increase as the number of IoT devices increase. It will be a huge challenge for industries to handle such big data and maintain its security. So, these were the security concerns for industries using IoT.

Module – 2

M2M to IoT – A Basic Perspective

Explain M2M value chains.

M2M Value chains:

- Input: Inputs are the base raw ingredients that are turned into a product.
- Production: Production refers to a process that the raw inputs are put through to become a part of the value chain.
- Processing: Processing refers to the process whereby a product is prepared for sale.
- Packaging: Packaging refers to the process whereby a product can be branded as would be recognizable to consumers.
- Distribution: This process refers to the channels to market for products.

Explain IoT value chains.
IoT value chains:

- Input: There is significantly a number of inputs in an IoT value chain than an M2M value chain. These can be open data, devices/sensors, OSS/BSS, corporate databases.

- Production: In this process, the raw inputs will undergo initial development into information components and products. Irrespective of the input type, this process will need to include tagging and linking of data items in order to provide traceability and performance across the value chain.

- Processing: In this stage, the data from various inputs from production stage are combined together to create information.

- Packaging: After the data from various inputs have been combined, the packaging component in the value chain creates information components. These components can be charts or any other traditional method to communicate the information to consumers.

- Distribution: This is the final stage in the value chain in which the information products are created.
Explain I-GVC with the figure.

- I-GVC stands for Information driven Global Value Chain.
- There are five fundamental roles involved:

1) Input

- Sensors, RFID, and other devices
- End users

2) Data factories

3) Service providers

4) Intermediaries

5) Resellers

1) Input:
• The sensors and devices are working as input by the means of capturing and transmitting the data in order to develop information products.
• The end users also provide inputs to the system.
• Every human that enters any search query, allows location information, uses NFC is also a part of value chain now.
• Both of these sources provide a few inputs which are then analyzed, aggregated, repackaged and exchanged.

2) Data factories:

• Data factories produce data in a digital form so that other parts of I-GVC can use it.

3) Service providers:

• Service providers collect data from various sources and create massive databases. They use it to improve their own information product or sell some information product in various forms.

3) Intermediaries:

• There is a need of intermediaries in the emerging structure of I-GVC.
• Intermediaries are also required to handle scalability issues and the security and privacy of data that is developed into information products.

4) Reseller:

• Resellers combine several inputs, analyze them and sell them to end-users or corporate entities.

Explain main design principles and needed capabilities of IoT.

• In order to develop the reference models or architecture for M2M or IoT, these primary sources can be identified.
1) SENSEI

2) ETSI TC M2M

3) IoT-A

1) SENSEI:

- The approach in SENSEI was to develop a model that integrates the real world into the future internet.
- There is a service infrastructure that provides services that are common to many IoT applications and the communication network should use the Internet Protocol (IP).
- The architecture relies on the sensors and actuators, a set of contextual and real-world entity-centric devices and the users.
- It also relies on an open-ended constellation of providers and users.
- The architecture also has its own key capabilities.

2) ETSI TC M2M:

- The telecommunication industry has focused on defining a common service core for M2M.
- The approach taken is to analyze M2M use cases, derive requirements and then provide the architecture.
- Similar to SENSEI, there was a clear approach towards horizontal architecture.
- Gateways, devices, communication network, service core and applications all are separated by the reference points.

3) IoT-A:

- The approach here is different from previous ones.
- Here, the reference architecture is created first and captured in the IoT ARM.
• Via ARM, it aims to achieve a high level of interoperability between different IoT solutions at the different level of communication, service, and information.
• It proposes a methodology on how to arrive at concrete architecture using use cases and requirements.

Module-3

IoT Architecture

Explain IoT architecture outline with a diagram.

- The assets of interest are the real world objects and entities that are subject to being monitored and controlled, as well as having digital representation and identities.
- The resource layer provides different capabilities such as sensing, actuation, and embedded identities. Sensors and actuators in the devices that may be smartphones, smart meters, other sensors and actuators deliver these functions.
- The purpose of communication layer is to provide the means for connectivity between the resources on one end and the different computing instances that host and execute the service support and application logic on the other hand. It can use LAN or WAN.
- Service support layer is generally executed in data centers or server farms inside the organizations or in a cloud environment. Few examples include software upgrades, remote diagnostics and recovery services.
- The data information layer provides a more abstract set of functions as its main purpose is to capture knowledge and provide advanced control logic support.
- The application layer provides specific IoT applications. There is an open-ended array of applications and typical examples include smart metering in the smart grid.
- In the business layer, the integration of the IoT application and business processes occur. It focuses on supporting the core business or operations of any enterprise that is interested in IoT applications.
- Apart from the functional layers, there are three functional groups across different layers:

  1) Management:

   - As the name implies, the management group deals with the management of system solution related to maintenance, administration, operation, and provisioning. This includes management of devices, communication networks and general IT infrastructure in the organization.

  2) Security:

   - Security is the protection of the system, its information, and services from the external threats and any other harm. Authorization, authentication, identity management, and trust are main capabilities.

  3) Data and services:

   - Data and service processing can, from a topological perspective, be done in a very distributed fashion and at different levels of complexity.

**Discuss the functional view of IoT.**
Functional view describes system’s runtime functional components, their responsibilities, default functions, interfaces and primary interactions.

- **Device and application FG**: Device functional component contains the sensing, actuation log, processing and storage components. Application functional group contains the standalone application.
- **Communication FG**: It contains the components for end-to-end communication, network communication, and hop-by-hop communication.
- **IoT service FG**: It consists of IoT service FC and IoT service resolution FC. Various service implementations are covered in service FC and service resolution FC contain necessary functions to realize a directory of IoT services that allow dynamic management of IoT service descriptions.
- **Virtual entity FG**: The virtual entity FG contains functions that support the interactions between users and physical things through virtual entity services.
- **Process management FG**: Provides the functional concepts necessary to conceptually integrate the IoT world into traditional processes.
- **Service organization FG**: Acts as a communication hub between several other functional groups by composing and orchestrating services of different level of abstraction.
• Security FG: It is responsible for security and privacy matters in IoT-A compliant IoT systems.

• Management FG: It is responsible for the composition and tracking of actions that involve in the other FGs.

**Explain ETSI M2M High-Level Architecture.**

- A high-level architecture of an M2M system consists of a device and gateway domain and a network domain.
- The device and gateway domain consist the following elements:

  1) M2M device runs M2M device operations using M2M device service capabilities layer (DSCL).

  2) M2M gateway runs M2M gateway applications using M2M gateway service capabilities layer (GSCL).

  3) M2M area network provides connectivity based on personal or local area network technologies between M2M devices and M2M gateways.
The network domain contains the following elements:

1) M2M Access network:
   - It allows M2M devices and M2M gateways to communicate with the core network.
   - It uses any one of the solutions such as Satellite, Digital Subscriber Line (DSL), WiFi, WiMax etc. that can be optimized for M2M communication when needed.

2) M2M Core network:
   - This network enables interconnection with other networks, provides IP connectivity or other connectivity options, service and control functions and roaming.

3) M2M Network Capabilities Layer:
   - It provides M2M functions which are shared by different M2M applications.

4) M2M Applications:
   - They run the service logic and use M2M service capabilities via open interfaces.

5) M2M Network Management Function:
   - They consist of all the functions required to manage access and core networks.

6) M2M Management Function:

M2M management functions consist of all the functions used to facilitate the bootstrapping of permanent M2M service layer security credentials required to manage M2M service capabilities in the network domain.

**Explain IoT reference architecture’s deployment and operational view.**

- Deployment and the operational view are very important in addressing how the actual system can be realized by selecting technologies and making them communicate and operate in a comprehensive way.
- This view depends upon actual use case and requirements.
- Let’s take an example of the parking lot system.

As we can see in the figure, there are two sensor nodes #1 and #2, each of which is connected to eight car presence sensors.

- They are also connected to the payment stations through wireless or wired communication.
- The payment station acts both as a user interface for the device to pay and get a payment receipt as well as a communication gateway that connects the two sensor nodes and payment interface physical devices with the internet through WAN.
- The occupation sign also acts as a communication gateway for the actuator node, and we assume that because of the deployment, a direct connection to the payment station is not feasible.
- The physical gateway devices connect through WAN to the internet and towards a data center where the parking lot management system software is hosted as one of the virtual machines on a platform as service configurations.
- The two main applications connected to this management system are human user mobile phone applications and parking operation center applications.
**Explain IoT domain model notations and semantics.**

- Unified Modelling Language (UML) is used to show relationships between the main concepts of the IoT domain model.
- Each class in UML is a set of objects that have similar structure, behavior, and properties.
- Each class contains the name and a set of attributes.
- The interaction with the physical world is the key for IoT and it needs to be captured in the domain model.
- The domain model represents the main concepts of IoT and the relationships between them.

![Diagram](image)

- As shown in the diagram, a physical entity can contain another physical entity. For example, a building contains several floors and each floor has several rooms.
- The physical entity is represented in the digital world as the virtual entity.
- A virtual entity can be a database entry, an image or avatar or any other digital unit.
- The relations between the services and entities are represented using associations.
- These associations can be static or dynamic.
Three types of devices are very important in IoT domain model:

1) Sensors: to covert physical properties to electrical signals.

2) Actuators: to convert electrical signals to physical properties.

3) Tags: to uniquely identify any physical entity.

**Explain reference architecture for IoT using figure.**
The reference architecture is a starting point for generating concrete architectures and actual systems.

It is based on the concepts of architectural views and architectural perspectives.

A view is a representation of one or more structural aspects of a reference architecture that illustrates how the reference architecture can be adapted to address one or more concerns held by its stakeholders.

A perspective addresses the non-functional requirement issues of the architecture.

Views are useful for reducing the complexity of reference architectures.

Reference architecture serves as a guide for one or more concrete system architects.

It does not contain details about the environment where the actual system is deployed.

The reference architecture is a set of architectural views as follows:

1) Functional view: Describes what system does and its main functions

2) Information view: Describes what data and information system handles

3) Deployment and operational view: Describes the real world components of the system

Explain architecture reference model in IoT.
- An Architecture Reference Model (ARM) is divided into two main parts: reference model and reference architecture.
- The reference model is a division of functionality into elements together with the data flow among those elements.
- The reference architecture is a reference model mapped onto software element that implements the functionality defined in the reference model.

The reference model consists of the domain, information, functional, communication, and security model.
- The domain model is responsible for outlining core concepts in IoT such as devices, services, and virtual entities.
- The information model defines the generic structural properties of information in an IoT system.
- The functional model identifies groups of functionalities based on the relations defined in the domain model.
- The communication model addresses the complexity of communications in IoT environment.
- The security model provides security and ensures the safety of the IoT application.
The ARM also defines reference architecture which is the reference for developing the actual system.

The figure shows that IoT architecture model is related to IoT reference model.

It shows two facets of IoT ARM:

1) How to actually create an IoT ARM.

2) How to use it with respect to building actual systems.

**Explain information view in IoT reference architecture.**

- Information view provides the overview of how the static and dynamic information is represented.
- It also describes the components that handle the information, the flow of information through the system and the life cycle of information in the system.
- One of the main purposes of connected and smart objects in the IoT is the exchange of information between each other and also with external systems.
- Information flow in IoT can use two paths:

  1) From devices such as sensors, actuators, tags until it reaches the consumer application.

  2) From the application part of the larger system until it reaches the consumer part of the system.

- An IoT system is typically deployed to monitor and control physical entities, monitoring and controlling physical entities in turn performed by mainly the devices, communication, IoT services and virtual entity functional group in the functional view.
- The virtual entity in any IoT system models the physical entity.
- Information in the system is handled by services.
- Services are registered to the IoT system using service description which is provided by service itself.
- There is four common message exchanging patterns considered for information exchange between IoT functional components.

  1) Push pattern: It is the one-way communication between two devices.
2) Request response pattern: It is the synchronous way of communication in which client waits for the server response. A client will send the request to the server. The server will get the request and send a response.

3) Subscribe/notify pattern: It is the asynchronous way of communication in which client doesn't wait for the server response. It just sends the subscribe-call to the server. The server gets it and notifies the client when it sends the response.

4) Publish/subscribe pattern: It allows the loose coupling between communication partners. The services are advertised on the broker component and whenever client shows the interest in a service, the connection between client and server is established.

Module-4

IoT Applications for Value Creations

What are the requirements that IoT application for industrial application should meet?

- Reliability: Reliable IoT devices and systems should allow a continuous operation of industrial processes and perform on-site activities.
- Robustness: The IoT application and devices should be robust and should adopt the task and hard working conditions.
- Reasonable cost: Reasonable here does not mean low cost. It is rather concerned about the right balance between the cost and benefit.
- Security and safety: Safety is mainly related to the device construction and area of use but also to usability such that no safety threats occur due to the use of IoT applications and devices.
- Simple use: Two of the most important things for IoT applications’ acceptance are their simplicity to use and self-explaining nature.
- Standardization: IoT devices must be using a set of standards to support interoperability of IoT devices, easy exchange, and multivendor possibilities.
- Low maintenance: The cost for the maintenance of IoT devices should be optimal so that everyone can afford them.
Support optimal and adaptive set of features.

What can the shopping basket tell: IoT for the retailing industry?

- IoT has changed the retailing industry significantly.
- There are four broad IoT application areas within the retailing industry.

1) Sensors fitted in the refrigerator and other electronic devices can save a huge amount of energy for the retailers. This way the retailers can reduce their carbon footprint which will lead to better customer loyalty.

2) Installing CCTV cameras for video analysis can trigger real-time automated alerts which can help the retailer to provide stuff to the customers in urgent need. It will lead to better customer experience, effective labor utilization and will ultimately increase sales.

3) IoT sensors can enable the dynamic re-routing of delivery vans based on the weather forecast and live traffic updates. Retailers can get better visibility into the inventory using the RFID tags. This all results in cost saving and improved customer satisfaction.

4) Using in-store sensors and video analysis, the retailer can understand customer hot spots, flow pattern and purchase timings. This way the retailer can keep the things together which is often bought by customers together. This is called market basket analysis. It will increase the revenues for sure.

- So, using IoT retailers can gain a deeper understanding of customer’s path to purchase, shopping habits that can be used in a variety of ways to optimize various customer touch points and build strong brand perception.
- Latest technologies like RFID, NFC, Big Data, sensors, cloud computing etc. have provided opportunities to redefine retail stores like never before.

Explain four aspects of the business to master IoT.

Here are the four aspects of the business to master IoT:
1) Technology:

- IoT will offer a huge global platform to connect smartphones, sensors, actuators and possibly every physical device connected to the internet.

- Companies are adapting to open standards for developing newer systems.

- Because of that, the business has moved to system and software platforms on the internet.

2) Business innovation:

- The combination of people and smart objects in an enterprise will lead to innovation in business models.

- The internet business models are already taking over traditional methods in some organizations.

3) Market:

- IoT has crosscut many industries and that is why they meet in the market for the first time.

- They co-operate in developing business products and increase overall sales.

- IoT has brought together many separate industries in order to make more benefits.

4) Competencies:

- Software and system competencies linked to the deep domain knowledge and enlightened with creativity are the core for innovation in business and technology.

- So, these are the four main aspects of the business to master IoT.

**Explain in brief future factory concepts.**

- The convergence of physical and virtual worlds has given a rise to smart factories.

- The future factories will use artificial intelligence, IoT, M2M, machine learning and many other advanced concepts.
- It will totally change how products are invented, manufactured and shipped.
- Using IoT in factories will increase the safety of the workers of the factory.
- It will reduce the emissions of harmful gases. Thus, it will help heal the environment.
- Manufacturing has made huge progress in recent years.
- The automation levels have increased in development of every product.
- This has led to factories meeting the demands of customers in quick successions.
- IoT will help manufacturers to manage their supply chains better.
- It will also help them to optimize their inventories so that the production cost can be reduced.
- IoT can help monitor the status of the machinery in real-time.
- In short, the manufactures can take care of what is happening at every point in the production process.
- Production of smart products will increase.
- Smart products generally have three components: 1) Physical components, 2) Smart components and 3) Connectivity components.
- However, as the factories will merge physical and virtual worlds, the system will also have to take care of the security and confidentiality.
- The following diagram shows the future factory concept:
Explain need of IoT in oil and gas industry.

- Unconventional resources challenge the oil industry.
- Exploration and development of oil and gas reservoirs require new sensors, analytics, and processes.
- Systems require better connectivity, monitoring and control and process automation.
- Process industry in general and oil and gas, in particular, put special requirements on field devices.
- It is a challenge to develop a field device that not only is easy to install and maintain, have a long enough life length but also withstand this tough environment.
- At a time when well drilling and completion complexities are increasing and field experts are becoming scarcer, automation offers many benefits.
- Besides capturing domain knowledge, automation increases safety and decreases personnel time on-site and therefore lowers the cost.
- A large field of wells can produce a massive amount of valuable information. The results include better asset utilization, reduced effluents, and fast production.
- Some of the small AC motors on an oil rig are highly critical with respect to regularity, some are critical with respect to safety if for instance placed in an explosion-prone zone.
• Large machines are always monitored but there is "run to failure" policy applied to small AC motors.
• WiMon 100 is a battery operated the device with an expected lifetime of five years.
• Due to the cost efficiency, small size and ease of installation and commissioning of the WiMon100 sensor, online vibration monitoring can now be realized for all types of rotating machines.
• WiMon100 unit contains a vibration sensor, a temperature sensor, a long-life battery and communicating wireless HART.
• The WiMon data manager handles data acquisition and storage as well as provides UI for commissioning, configuration, machine supervision and network operation.

Enlist the challenges faced by industry related IoT applications.

Here are some of the biggest challenges faced by the industry related IoT applications:

• Security
• Trust and Privacy
• Complexity
• Evolving architectures
• Concrete use cases and compelling value proportions
• Ongoing development of wireless standards

Enlist IoT applications for value creation.

Here are the IoT applications for value creation:

• Visibility identification
• Location tracking
• Reduced energy consumption
• Reduced production loses
• New type of processes made possible by IoT applications
• New type of maintenance and lifetime approaches
• Enabled by smart objects, connected aspects
- Improved operation and flow in industry
- Security
- Providing and collecting right information

**Explain value creation from big data and serialization.**

- Serialization is the process of transforming data entities into bytes for persistence or transportation from one machine to another over a network.
- Serialization engine provides the ability to serialize and de-serialize data. In big data, it is required to exchange messages between machines and for persisting them.
- Serialized identifiers to build IoT are as important as IP is to the web.
- Big data cannot be handled or processed using traditional databases and conventional tools. It required exceptional technologies.
- Technologies applied to big data have distributed file system, distributed database, parallel processing database, data mining grids, internet and scalable storage systems.
- These technologies are linked with natural as well as business environment.
- Big data is characterized by 4 Vs: volume, velocity, variety, and veracity.
- One example of big data is the data generated from RFID and sensors in medical devices and pharmaceutical manufacturing organizations. The volume of this data will be huge.
- The pharmaceutical industry has always struggled to keep track of the products distributed to different shops.
- This problem gets bigger when the products cross international borders.
- So, the industries need serialization to solve this problem.
- It will generate huge data sets and will require significant investment.
- However, this much data will surely provide insights into business and provide valuable information.
- Thus, creating a global, scalable serialization architecture to manage a complete end-to-end business process is critical.
- Supply chain management has some issues like load balancing, route planning, warehouse management, distribution network design etc. too.
- Product identifiers can come handy in solving this issue.
- There can be issues like legal information and finance.
- Legal information issues include the question of jurisdiction over data and ownership of data.
- Finance issues are also there for manufacturing, distribution, monitoring, delivery etc. using IoT devices require massive investment.

Module-5

Internet of Things Privacy, Security and Governance

Discuss GAMBAS middleware.

- GAMBAS means Generic Adaptive Middleware for Behaviour-driven Autonomous Service.
- The GAMBAS middleware will enable the development of novel applications and internet-based services that utilize context information in order to adapt to the behavior of the user autonomously.
- The middleware will provide the means to gather context in generic yet resource efficient manner and it will support the privacy-preserving sharing of the acquired data.
- Thereby, it will apply interoperable data representations which support scalable processing of data gathered from a large number of connected objects.
- The middleware will also support intent-aware interaction by providing a constant stream of relevant recommendations for services.
- GAMBAS middleware is secure as the data acquisition; data storage and processing are tightly controlled by the user.
- There is a data processing component to store and manage data. It has three sub-components: 1)store data, 2)query data and 3)discover data.
- Thus, the GAMBAS middleware simplifies the development of smart city applications by focusing on three common tasks: 1)data acquisition, 2)secure data distribution and 3)interoperable data integration.
Explain SMARTIE approach for IoT.

- SMARTIE is used to design and build data-centric information sharing platform.
- This information is accessed by an information service layer.
- SMARTIE is the first EU project that relies on the IoT-ARM.
- Here are the IoT layers with their responsibilities in SMARTIE project.

<table>
<thead>
<tr>
<th>IoT layer</th>
<th>Devices and functions</th>
<th>Security requirements</th>
</tr>
</thead>
</table>
| Application layer | 1) Intelligent transportation  
  2) Smart energy  
  3) Public safety  
  4) Utilities  
  5) Service providers | 1) Authentication, authorization, assurance.  
  2) Privacy protection and policy management.  
  3) Secure Computation.  
  4) Discovery of information sources. |
<p>| Information services layer | 1) In-network data | 1) Cryptographic data storage. |</p>
<table>
<thead>
<tr>
<th><strong>Network layer</strong></th>
<th><strong>Secure data management and handling.</strong></th>
<th><strong>Communication and connectivity security.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Networking infrastructure</td>
<td>2) Network level protocols</td>
<td>2) Secure sensor interaction.</td>
</tr>
<tr>
<td>3) Cross-domain data security handling.</td>
<td></td>
<td>3) Cross-domain data security handling.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Smart object</strong></th>
<th><strong>Data format and structures.</strong></th>
<th><strong>Access control to nodes.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Sensors for data collections</td>
<td>2) Actuators</td>
<td>3) Lightweight encryption</td>
</tr>
<tr>
<td>4) Trust attestation.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The objectives of SMARTIE are:

- Understanding requirements for data and application security and creating a policy-enabled framework supporting data sharing across applications.
- Developing new technologies that establish trust and security in perception layer and network layer.
- Develop new technologies for trusted information creation and secure storage for the information service layer.
- Develop new technologies for information retrieval and processing guided by access control policies in the application layer.
- Demonstrate the project results in real use cases.

**Explain Butler project.**
The main aim of BUTLER project is the creation of an experimental technical platform to support the development of the IoT.

BUTLER focused on five innovative eco-systems:

1) Smart cities
2) Smart healthcare
3) Smart home and offices
4) Smart shopping
5) Smart transport

These are commonly used in most people’s daily lives. So, BUTLER project will help mankind a lot.

The BUTLER project uses secure communication devices that are adapted to the limited capacity of devices that are part of the network.

The main achievement of BUTLER project is the release of the open-platform portal on which IoT applications can be created.

This platform can also be used to define their relationships, reference to existing use cases, infrastructures and deployment.

BUTLER also provides an authorization server which combined with managed resources share the credentials for generation of session keys.

Authorization server authenticates the user and grants user the access to the application.

The BUTLER project also provides a threat analysis model which can be used to evaluate possible threats to the application in different scenarios.

**Explain data aggregation for IoT in smart cities security.**

The starting point of data aggregation is the collection of information from different sensors.
- IoT is heterogeneous both semantically and syntactically.
- Despite this, IoT applications like the smart home smart city will require that all data be easily compared, correlated and merged and that the interpretation of the resulting aggregate into a higher level context that matches people's need and requirements.
- Data aggregation research has been focused on the database schema integration approaches and one major benefit of that is its ability to provide high level and expressive abstractions.
- We all know that all the smart city data is going to be stored in the cloud.
- This exposes the data to many threats and that is why the security of this data is very important.
- An attacker can hack the system and use the smart city data in wrong way, damage the sensors and actuators physically etc.
- SMARTIE is the first step in the direction of smart cities security.
- It assures the main aspects of security such as confidentiality, integrity, and availability.
- Confidentiality means the absence of unauthorized disclosure of information.
- Integrity is the prevention of unauthorized modification.
- Availability means the system should be available all the time when users need it.
- It will ensure that the private data is preserved while sharing.

**Explain contributions from the FP7 project.**

- FP7 means 7th framework program for research and technological development. It lasted for 7 years from 2007 until 2013.

i)FP7 iCore access framework:

- The iCore cognitive framework is based on the principle that any real-world object and any digital object that is available, accessible or controllable can have a representation in IoT.
- The iCore initiative addresses two key issues in the context of IoT, namely how to abstract the technological heterogeneity that derives from the vast amount of heterogeneous objects and how to consider the views of different stakeholders.
2) IoT @ work capability-based access control system:

- A capability is a communicable, unforgeable rights makeup, which corresponds to a value that uniquely specifies certain access rights to objects owned by subjects.
- In CAP-BAC, the user needs to show the service provider the authorization certificate prior to performing resource request operations.

3) GAMBAS middleware:

- GAMBAS means Generic Adaptive Middleware for Behaviour driven Autonomous Service.
- Middleware will provide the means to gather context in a generic yet resource efficient manner and it will support the privacy-preserving sharing of the acquired data.
- GAMBAS middleware simplifies the development of smart city application focusing on common tasks, namely efficient data acquisition, secure and privacy-preserving data as well as data integration.

4) BUTLER project:

- The goal of BUTLER project is the creation of an experimental technical platform to support the development of IoT.
- BUTLER focused on five “innovation eco-systems” that are part of most people’s lives:

1) Smart homes and offices
2) Smart shopping
3) Smart transport
4) Smart healthcare
5) Smart cities
Explain security, privacy, and trust in IoT-data platforms for smart cities.

- SMARTIE is a secure smart city management system.
- It works on security, privacy, and trust for data exchange between IoT devices and consumers of their information.
- A secure, trusted but easy to use IoT system for a smart city will benefit the various stack-holders of a smart city.
- The city administration will have it easier to get information from their citizens while protecting their privacy.
- Furthermore, the services offered will be more reliable if quality and trust of the information are ensured.
- Privacy and trust are key pre-requisites for citizens to participate in smart city activities.
- A smart city can improve their lives significantly.
- Enterprises also benefit from the securely provided information as they can optimize the demands and offer more tailored solutions.
- All parties involved in the system such as sensors, actuators, users, owners and service providers need strong mechanisms for reliability and trust.
- Risk mitigation is really important because if the trust of the citizens is not maintained, the smart city IoT system will fail badly.
- The objectives of SMARTIE are:
  - Understanding requirements for data and application security and creating a policy-enabled framework supporting data sharing across applications.
  - Developing new technologies that establish trust and security in perception layer and network layer.
  - Develop new technologies for trusted information creation and secure storage for the information service layer.
  - Develop new technologies for information retrieval and processing guided by access control policies in the application layer.
  - Demonstrate the project results in real use cases.