Q-1 What is Internet of things ? OR

Define Internet of things.

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 and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Wikipedia :--

The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances.

Center for Data and Innovation:-

Internet of Things refers to the concept that the Internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them."

Cisco:-

IoT is a network of physical objects access through the internet, as defined by technology analysts and visinaries.

IoT 2008 :-

The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects.

IoT in 2020 :-

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts".

Q-2 What is the Vision of internet of things? OR

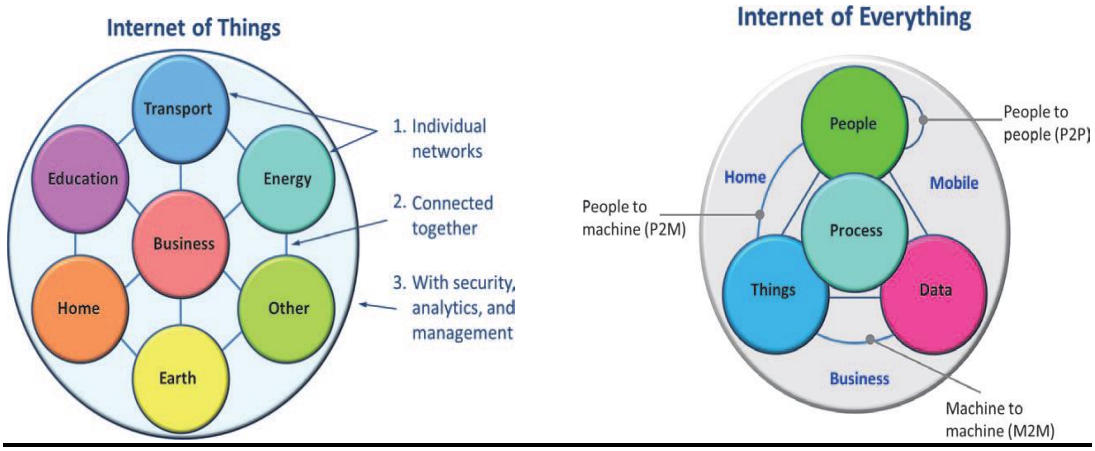
Explain Vision of IOT.

The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service.

Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the act that they can communicate information about themselves.

New types of applications can involve the electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment are integrated into a single ecosystem with a shared user interface.

In the future computation, storage and communication services will be highly pervasive and distributed: people, smart objects, machines, platforms and the surrounding space (e.g., with wireless/wired sensors, M2M devices, RFID tags, etc.) will create a highly decentralized common pool of resources (up to the very edge of the "network") interconnected by a dynamic network of networks.



Q3. The Internet of Things Today

One year after the past edition of the Clusterbook 2012 it can be clearly stated that the Internet of Things (IoT) has reachedmany different players and gained further recognition. Out of the potential Internet of Things application areas,Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem (Figure 1.1) have acquired high attention.

Fig. 1.1 IoT Ecosystem.

In line with this development, the majority of the governments in Europe, in Asia, and in the Americas consider now the Internet of Things as an area of innovation and growth. Although larger players in some application areas still do not recognise the potential, many of them pay high attention or even accelerate the pace by coining new terms for the IoT and adding additional components to it.Moreover, end-users in the private and business domain have nowadays acquired a significant competence in dealingwith smart devices and networked applications.

As the Internet of Things continues to develop, further potential is estimated by a combination with related technology approaches and concepts such as Cloud computing, Future Internet, Big Data, robotics and Semantic Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.

Factors are

No clear approach for the utilisation of unique identifiers and numbering spaces for various kinds of persistent and volatile objects at a global scale.

• No accelerated use and further development of IoT reference architectures like for example theArchitectureReferenceModel (ARM) of the project IoT-A.

• Less rapid advance in semantic interoperability for exchanging sensor information in heterogeneous environments.

• Difficulties in developing a clear approach for enabling innovation, trust and ownership of data in the IoT while at the same time respecting security and privacy in a complex environment.

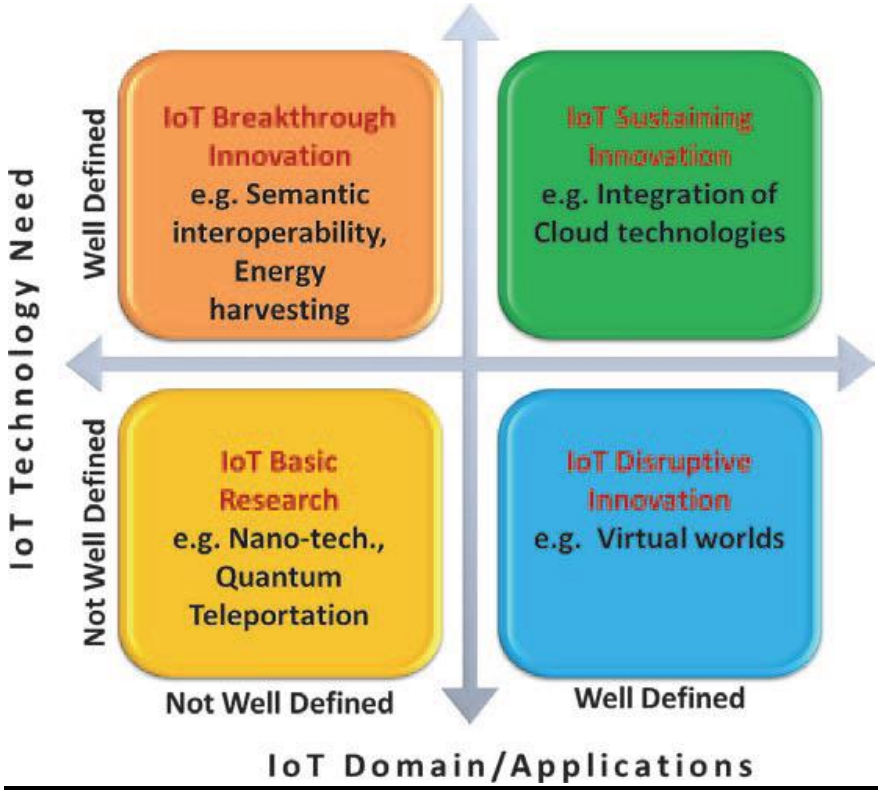
• Difficulties in developing business which embraces the full potential of the Internet of Things.

• Missing large-scale testing and learning environments, which both facilitate the experimentation with complex sensor networks and stimulate innovation through reflection and experience.1.2 Time for Convergence 3

• Only partly deployed rich interfaces in light of a growing amount of data and the need for context-integrated presentation.

Q-4 Explain Time of Convergence with reference to IOT.

Integrated environments that have been at the origin of the successful take up of smartphone platforms and capable of running a multiplicity of user-driven applications and connecting various sensors and objects are missing today.



Innovation Matrix of IERC — Internet of Things European Research Cluster

• ***Coherence of object capabilities and behaviour*:** the objects in the Internet of Things will show a huge variety in sensing and actuation capabilities, in information processing functionality and their time of existence. In either case it will be necessary to generally apprehend object as entities with a growing "intelligence" and patterns of autonomous behaviour.

• ***Coherence of application interactivity*:** the applications will increase in complexity and modularisation, and boundaries between applications and services will be blurred to a high degree. Fixed programmed suites will evolve into dynamic and learning application packages. Besides technical, semantic interoperability will become the key for context aware information exchange and processing.

• ***Coherence of corresponding technology approaches*:** larger concepts like Smart Cities, Cloud computing, Future Internet, robotics and others will evolve in their own way, but because of complementarity also partly merge with the Internet of Things. Here a creative view on potential synergies can help to develop new ecosystems.

• ***Coherence of real and virtual worlds*:** today real and virtual worlds are perceived as two antagonistic conceptions. At the same time virtual worlds grow exponentially with the amount of stored data and ever increasing network and information processing capabilities. Understanding both paradigms as complementary and part of human evolution could lead to new synergies and exploration of living worlds.

Q-5 The Internet of Things Applications OR

List and Explain Difference areas of Internet of things.

The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nanoelectronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering),institutional, and economical issues.

1. Smart home

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

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

Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels. More than 60,000 people currently search for the term "Smart Home" each month. This is not a surprise. The IoT Analytics company database for Smart Home includes 256 companies and startups. More companies are active in smart home than any other application in the field of IoT. The total amount of funding for Smart Home startups currently exceeds $2.5bn. This list includes prominent startup names such as Nest or AlertMe as well as a number of multinational corporations like Philips, Haier, or Belkin.

2. Wearables

Wearables remains a hot topic too. As consumers await the release of Apple's new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet. Of all the IoT startups, wearables maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars!

3. Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

By 2023, there will be 30 mega cities globally, with 55 percent in developing economies of India, China, Russia and Latin America.

- Smart features,
    - Smart Economy,
    - Smart Buildings,
    - Smart Mobility,
    - Smart Energy
    - Smart Information Communication and Technology,
    - Smart Planning,
    - Smart Citizen and Smart Governance.

4. Smart grids

Smart grids is a special one. A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity. 41,000 monthly Google searches highlights the concept's popularity

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

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

5. Industrial internet

The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearables do. The industrial internet however has a lot going for it. The industrial internet gets

the biggest push of people on Twitter (~1,700 tweets per month) compared to other non-consumer-oriented IoT concepts.

6. Connected car

The connected car is coming up slowly. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet. But it seems we are getting there. Most large auto makers as well as some brave startups are working on connected car solutions. And if the BMWs and Fords of this world don't present the next generation internet connected car soon, other well-known giants will: Google, Microsoft, and Apple have all announced connected car platforms.

7. Connected Health (Digital health/Telehealth/Telemedicine)

Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential (see our analysis of market segments), not just for companies also for the well-being of people in general. Yet, Connected Health has not reached the masses yet. Prominent use cases and large-scale startup successes are still to be seen. Might 2015 bring the breakthrough?

8. Smart Transportation and Mobility

Internet of Vehicles (IoV) connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation.

Creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

9. Smart Building

Intelligent Building Management Systems can be considered part of a much larger information system.

This system is used by facilities managers in buildings to manage energy use and energy procurement and to maintain buildings systems. It is based on the infrastructure of the existing Intranets and the Internet, and therefore utilizes the same standards as other IT devices.

10. Infrastructure

Critical Infrastructures migrating toward Smart Infrastructures by deploying IoT. They invest on remote management and big data to improve the quality of service.

Smart Infrastructures comprise several operators from different domains of activity, such as energy, public transport, public safety.

11. Smart Health

The concept of connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general.

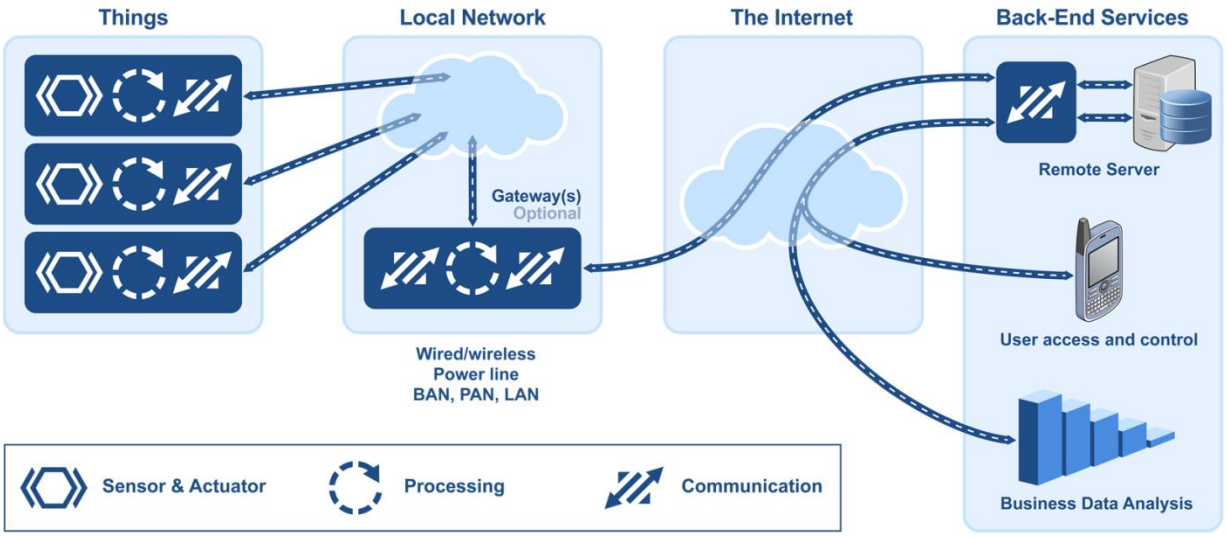
IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices.

The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness.

Q-6 Explain Networks and Communication and Data Management

Networks Technology

Network users will be humans, machines, things and groups of them.



- **Complexity of the Networks of the Future:**

  the complexity of future networks and the expected growth of complexity due to the growth of Internet of Things.

- **Growth of Wireless Networks:**

  Wireless networks especially will grow largely by adding vast amounts of small Internet of Things devices with minimum hardware, software.

- **Mobile Networks:**

  The mobile phone of the future could provide mobile function.

- **Expanding Current Networks to Future Networks:**

  expand current end user network nodes into networks of their own or even a hierarchy of networks.

- **Overlay Networks:**

  In some locations even multiple networks overlaying one another physically and logically.

- **Network Self-organization:**

  Self-organization principles will be applied to configuration by sensing.

- **IPv6, IoT and Scalability:**

  The current transition of the global Internet to IPv6 will provide a virtually unlimited number of public IP addresses able to provide bidirectional and symmetric (true M2M) access to Billions of smart things.

- **Green Networking Technology:** GreenTouch

- These network technologies have to be appropriate to realise the Internet of Things and the Future Internet in their most expanded state to be anticipated by the imagination of the experts.

Communication Technology

- **Unfolding the Potential of Communication Technologies:**

  communication technology to be undertaken in the coming decade will have to develop and unfold all potential communication profiles of Internet of Things devices.

- Communications technologies for the Future Internet and the Internet of Things will have to avoid such bottlenecks by construction not only for a given status of development, but for the whole path to fully developed and still growing nets.

- **Correctness of Construction:**

  Correctness of construction of the whole system is a systematic process that starts from the small systems running on the devices up to network and distributed applications.

- **An Unified Theoretical Framework for Communication:**

- Communication between processes running within an operating system on a single or multicore processor
- communication between processes running in a distributed computer system,
- the communication between devices and structures in the Internet of Things and the Future Internet using wired and wireless channels shall be merged into a unified minimum theoretical framework covering and including formalized communication within protocols.

Data Management

- Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.
- challenges and opportunities of data management
  - Data Collection and Analysis
  - Big Data
  - Semantic Sensor Networking
  - Virtual Sensors
  - Complex Event Processing

Q-7 Explain Data Collection and Analysis (DCA)

The DCA module is part of the core layer of any IoT platform.

functions of a DCA module

- **User/customer data storing:**

  Provides storage of the customer's information collected by sensors

- **User data & operation modelling:**

Allows the customer to create new sensor data models to accommodate collected information and the modelling of the supported operations.

- **On demand data access:**

Provides APIs to access the collected data.

- **Device event publish/subscribe/forwarding/notification:**

  Provides APIs to access the collected data in real time conditions

- **Customer rules/filtering:**

  Allows the customer to establish its own filters and rules to correlate events.

- **Customer task automation:**

  Provides the customer with the ability to manage his automatic processes.

- **Customer workflows:**

  Allows the customer to create his own work flow to process the incoming events from a device

- **Multitenant structure:**

  Provides the structure to support multiple organizations and reseller schemes.

Features Data Collection and Analysis platform:

- **Multi-protocol:** DCA platforms should be capable of handling or understanding different input (and output) protocols and formats.
- **De-centralization:** Sensors and measurements/ observations captured by them should be stored in systems that can be de-centralised from a single platform.
- **Data mining features:** DCA systems should also integrate capacities for the processing of the stored info, making it easier to extract useful data from the huge amount of contents that may be recorded
- **Security:** DCA platforms should increase the level of data protection and security, from the transmission of messages from devices (sensors, actuators, etc.) to the data stored in the platform.

Q-8 What is M2M?

- **Wikipedia**: Machine to machine refers to technology that allowed both wireless and wired systems to communicate with other devices of the same type.
- **Digi**: Machine to Machine (M2M) technology allows organization to gather data from the edge of the enterprise and apply it in way that positively impact the business.
- **Orange**: exchange the information between machine that is established between central control system (server) and any type of equipment, through one or several communication networks.

Q-9 Define Following terms:-
(1) Global Value Chain
(2) Ecosystems Vs. Value Chain
(3) Industrial Structure

(1) Global Value Chains:

A value chain describes the full range of activities that firms and workers Perform to bring a product from its conception to end use and beyond, including design, production, marketing, distribution, and support to the final consumer.

(2) Ecosystems vs. value chains:

Business Ecosystems, defined by James Moore (Moore 1996), refer to "an economic community supported by a foundation of interacting organizations and individuals . The economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organisms also include suppliers, lead producers, competitors, and other stakeholders.

(3) Industrial structure:

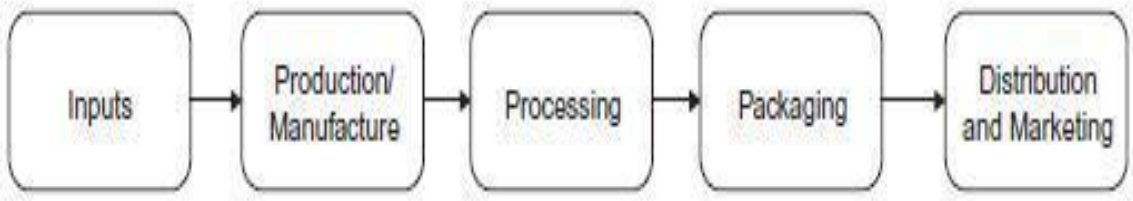
Industrial structure refers to the procedures and associations within a given industrial sector. It is the structure that is purposed towards the achievement of the goals of a particular industry. This is one of the key differences between the M2M and IoT markets _ how the industrial structures will be formed around these solutions, despite very similar technology implementations. This is covered in more detail in the following sections.

Q-10 Explain M2M value chains

Reasons for using M2M vary from project to project and company to company, but can include things such as cost reductions through streamlined business processes, product quality improvements, and increased health and safety protection for employees. These solutions are

generally all internal to a company's business processes and do not included extensive interactions with other parties.

let's take a look at the inputs and outputs of an M2M value chain.



Inputs: Inputs are the base raw ingredients that are turned into a product. Examples could be cocoa beans for the manufacture of chocolate or data from an M2M device that will be turned into a piece of information.

Production/Manufacture: Production/Manufacture refers to the process that the raw inputs are put through to become part of a value chain. For example, cocoa beans may be dried and separated before being transported to overseas markets. Data from an M2M solution, meanwhile, needs to be verified and tagged for provenance.

Processing: Processing refers to the process whereby a product is prepared for sale. For example, cocoa beans may now be made into cocoa powder, ready for use in chocolate bars. For an M2M solution, this refers to the aggregation of multiple data sources to create an information component _ something that is ready to be combined with other data sets to make it useful for corporate decision-making.

Packaging: Packaging refers to the process whereby a product can be

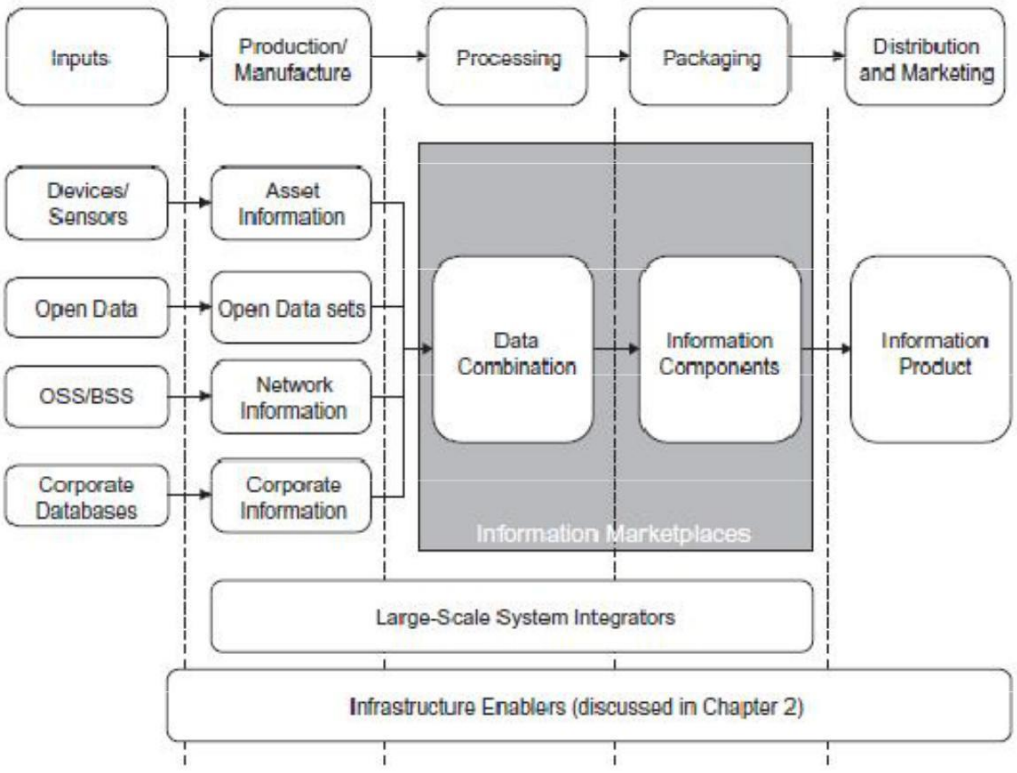
branded as would be recognizable to end-user consumers. For example, a chocolate bar would now be ready to eat and have a red wrapper with the words "KitKatt" on it. For M2M solutions, the data will have to be combined with other information from internal corporate databases, for example, to see whether the data received requires any action. This data would be recognizable to the end-users that need to use the information, either in the form of visualizations or an Excel spreadsheet.

Distribution/Marketing: This process refers to the channels to market for products. For example, a chocolate bar may be sold at a supermarket, a kiosk, or even online. An M2M solution, however, will have produced an Information Product that can be used to create new knowledge within a corporate environment _ examples include more detailed scheduling of maintenance based on real-world information or improved product design due to feedback from the M2M solution.

As mentioned previously, M2M value chains are internal to one company and cover one solution. IOT Value Chains, meanwhile, are about the use and reuse of data across value chains and across solutions.

Q-11 IOT value chains

IoT value chains based on data are to some extent enabled by Open APIs and the other open web-based technologies Open APIs allow for the knowledge contained within different technical systems to become unembedded, creating the possibility for many different economic entities to combine and share their data as long as they have a well-defined interface and description of how the data is formatted.



Let's take a closer look at a possible IoT value chain, including anInformation Marketplace, illustrated in Figure.

(1) **Inputs:** The first thing that is apparent for an IoT value chain is that there are significantly more inputs than for an M2M solution.

Devices/Sensors: these are very similar to the M2M solution devices and sensors, and may in fact be built on the same technology. As we will see later, however, the manner in which the data from these devices and sensors is used provides a different and much broader marketplace than M2M does.

Open Data: Open data is an increasingly important input to Information Value Chains. A broad definition of open data defines it as: "A piece of data is open if anyone is free to use, reuse, and redistribute it _ subject only, at most, to the requirement to attribute and/or share-alike"

OSS/BSS: The Operational Support Systems and Business Support Systems of mobile operator networks are also important inputs to information value chains, and are being used increasingly in tightly closed information marketplaces that allow operators to deliver services to enterprises _ for example, where phone usage data is already owned by the company in question.

Corporate Databases: Companies of a certain size generally have multiple corporate databases covering various functions, including supply chain management, payroll, accounting, etc. . . . Over the last decades, many of these databases within corporations have been increasingly interconnected using Internet Protocol (IP) technologies. As the use of devices and sensors increases, these databases will be connected to this data to create new information sources and new knowledge.

(2) **Production/Manufacture:** In the production and manufacturing processes for data in an IoT solution, the raw inputs described above will undergo initial development into information components and products. Irrespective of input type described above, this process will need to include tagging and linking of relevant data items in order to provide provenance and traceability across the information value chain.

Asset Information: Asset information may include data such as temperature over time of container during transit or air quality during a particular month. Essentially, this relates to whatever the sensor/device has been developed to monitor.

Open Data Sets: Open data sets may include maps, rail timetables, or demographics about a certain area in a country or city.

Network Information: Network information relates to information such as GPS data, services accessed via the mobile network, etc. . . .

Corporate Information: Corporate information may be, for example, the current state of demand for a particular product in the supply chain at a particular moment in time.

(3) **Processing:** During the processing stage, data from various sources is mixed together. At this point, the data from the various inputs from the production and manufacture stage are combined together to create information.

(4) **Packaging:** After the data from various inputs has been combined together, the packaging section of the information value chain creates information components. These components could be produced as charts or other traditional methods of communicating information to end-users.

(5) **Distribution/Marketing:** The final stage of the Information Value Chain is the creation of an Information Product. A broad variety of such products may exist, but they fall into two main categories:

- **Information products for improving internal decision-making:** These information products are the result of either detailed information analysis that allows better decisions to be made during various internal corporate processes, or they enable the creation of previously unavailable knowledge about a company's products, strategy, or internal processes.

- **Information products for resale to other economic actors:** These information products have high value for other economic actors and can be sold to them. For example, through an IoT solution, a company may have market information about a certain area of town that another entity might pay for (e.g. a real-estate company).

Q-12 Explain An emerging industrial structure for IoT

Where the technologies of the industrial revolution integrated physical components together much more rapidly, M2M and IoT are about rapidly integrating data and workflows that form the basis of the global economy at increasing speed and precision.

In contrast to fixed broadband technologies, which are limited to implementation in households mainly in the developed world, mobile places consumer electronic goods into the hands of over 4 billion end-users across the globe, and connects billions of new devices into the mobile broadband platform. Concepts such as cloud computing, meanwhile, have the ability to provide low cost access to computational capacity for these billions of end-users via these mobile

devices. Combined, these two technologies create a platform that will rapidly redefine the global economy. A new form of value chain is actually emerging as a result _ one driven by the creation of information, rather than physical products.

For IoT, however, new sets of system integrator capacity are required for two main reasons:

Technical: The factors driving the technical revolution of these industries means that the complexity of the devices in question require massive amounts of R&D; as do semiconductors with large amounts of functionality built into the silicon. Services will require multiple devices, sensors, and actuators from suppliers to be integrated and exposed to developers. Only those companies with sufficient scale to understand the huge number of technologies well enough to integrate them fully on behalf of a customer can handle this technical complexity. While niche integrators will continue to exist, full solutions will be integrated and managed by large companies, or partnerships between vendors.

Financial: Only those companies that are able to capture the added value created in the emerging industrial structure will recoup enough money to re-invest in the R&D required to participate in the systems integration market. It is highly likely that the participants that do not capture part of the integration market will be relegated to "lower" ends of the value chain, producing components as input for other system integrators.

There is in fact a new type of value chain emerging _ one where the data gathered from sensors and radio frequency identification (RFID) is combined with information from smartphones that directly identifies a specific individual, their activities, their purchases, and preferred method of communication.

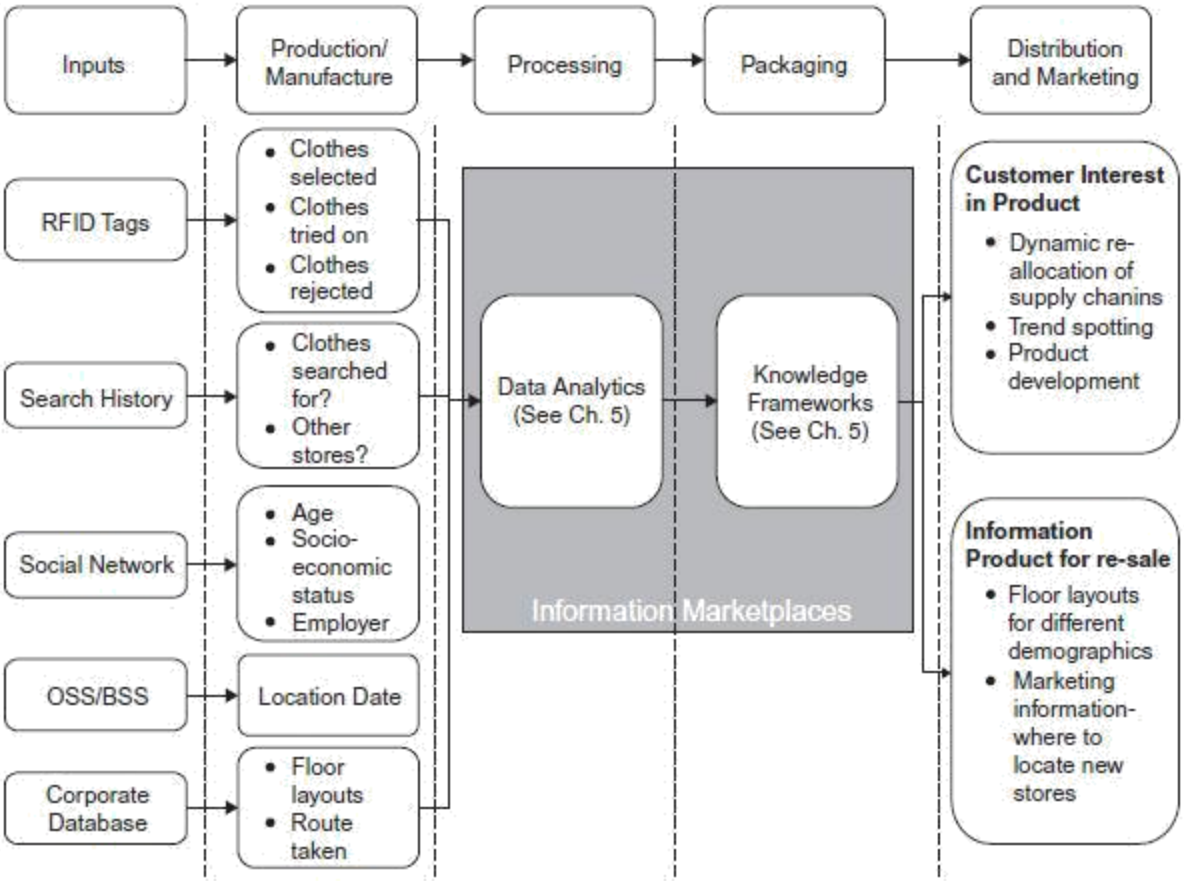
if I was in a clothing store searching for a new outfit for work, through a combination of information about myself and the RFID tags on the different clothes, I could be guided to the correct clothing selection for my age group, my education level, and also my current employer.

Information about what path I take through the store during my search for the clothes could be fed back into an information system that would allow the store to reorganize their floor layouts more effectively, track the clothes that I was interested in, and those which I actually select 3.5 An emerging industrial structure for IoT 49 to try on and purchase.

This streamlining could also be extended into the processes of production, changing orders based on consumer interest in products, and not just their purchasing patterns.

This would result in less wasted stock and a much closer understanding of seasonal trends and an increased level of control for those companies working as system integrators.

The integration of these data streams allows for concatenation of supply chains not just internally to one company, therefore, but across industrial boundaries.


Inputs
Production/ Manufacture
Processing
Packaging
Distribution and Marketing
RFID Tags
Search History
Social Network
OSS/BSS
Corporate Database
Clothes selected
Clothes tried on
Clothes rejected
Clothes searched for?
Other stores?
Age
Socio-economic status
Employer
Location Date
Floor layouts
Route taken
Data Analytics (See Ch. 5)
Knowledge Frameworks (See Ch. 5)
Information Marketplaces
Customer Interest in Product
Dynamic re-allocation of supply chanins
Trend spotting
Product development
Information Product for re-sale
Floor layouts for different demographics
Marketing information-where to locate new stores

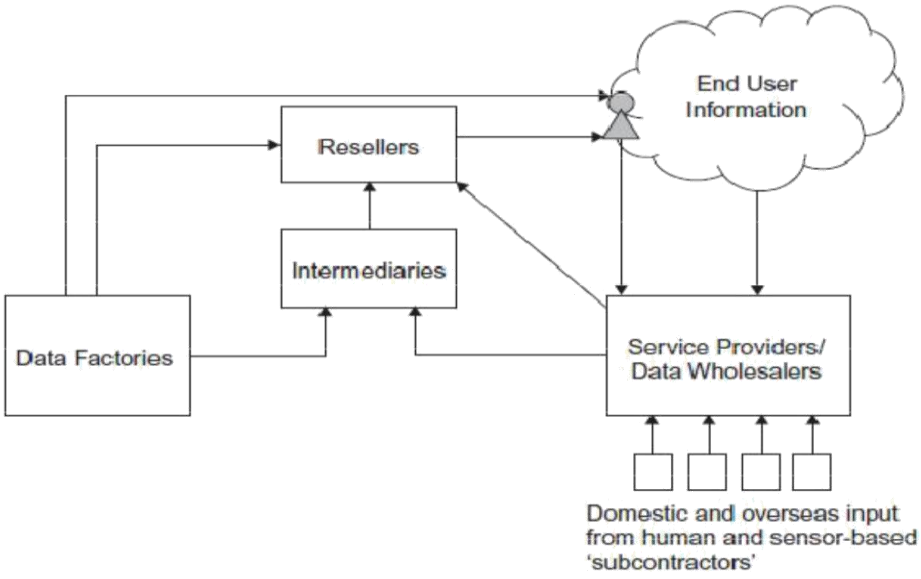
Q-13 The information-driven global value chain(I-GVC)

There are five fundamental roles within the I-GVC (Information-Driven Global Value Chain) that companies and other actors are forming around,

- Inputs:
Sensors, RFID, and other devices.

    - End-Users.

- Data Factories.
- Service Providers/Data Wholesalers.
- Intermediaries.
- Resellers.



(1) Inputs to the information-driven global commodity chain

There are two main inputs into the I-GVC:

1. Sensors and other devices (e.g. RFID and NFC).
2. End-users.

Both of these information sources input tiny amounts of data into the I-GVC chain, which are then aggregated, analyzed, repackaged, and exchanged between the different economic actors that form the value chain.

Sensors and radio frequency identification

- Sensors and RFID are already found in a multitude of different applications worldwide 2), helping to smooth supply and demand in various supply chains worldwide and gathering climate and other localized data that is then transmitted back to a centralized information processing system.

- These devices are working as inputs to the I-GVC through the capture and transmission of data necessary for the development of information products.
- Smartphones have also been developed that allow mobile devices to interact with sensors and RFID. This allows for a two-way interaction between a mobile terminal and the sensor technology.

- The data, however, is used as one part of the input to the commodity chain, which uses it to create the information products that are eventually exchanged.

- In this sense, the sensor networks, and NFC and RFID technologies may be viewed as subcontractors to the I-GVC, workers that constantly gather data for further processing and sale.

End-users

- The second main inputs to the I-GVC are the end-users.
- End-users that choose to use and participate within the digital world are now deeply embedded into the very process of production.
- Every human that enters a search query into a search engine, every human that agrees to allow the mobile broadband platform to inform a service of their location, every human that uses NFC to allow a bank to establish and confirm their identity are also functioning as subcontractors to the global information systems that form the basis of the I-GVC.
- Each individual's data can be treated as unique within this value chain; in fact, it is the ability to capture the uniqueness of every person that is a key aspect of the I-GVC in comparison to the other commodity chains that are at work within the global economy.

Data factories

- Data factories are those entities that produce data in digital forms for use in other parts of the I-GVC.

- Previously, such data factories would create paper-based products and sell them to end-users via retailers.
- With the move to the digital era, however, these companies now also provide this data via digital means.

Service providers/data wholesalers

- Service Providers and Data wholesalers are those entities that collect data from various sources worldwide, and through the creation of massive databases, use it to either improve their own information products or sell information products in various forms.
- Many examples exist; several well-known ones are Twitter, Facebook, Google, etc.. Google "sells" its data assets through the development of extremely accurate, targeted, search-based advertising mechanisms that it is able to sell to companies wishing to reach a particular market.
- Twitter, meanwhile,through collating streams of "Tweets" from people worldwide, is able to collate customer entiment about different products and world events, from service at a restaurant to election processes across the globe; through what Twitter refers to as a "data hose," companies and developers can access 50% of end-user Tweets for $360,000 USD per annum.

Intermediaries

In the emerging industrial structure of the I-GVC, there is a need for intermediaries that handle several aspects of the production of information products.

As mentioned above, there are many privacy and regional issues associated with the collection of personal information.

In Europe, the manner in which Facebook collects and uses the data of the individuals that participate in its service may actually be in contravention of European privacy law.

These corporations will provide protection for the consumer that their data is being used in an appropriate manner, i.e. the manner in which the consumer has approved its usage.

For example, I may happily share my personalized information about my tastes with a clothing company or music store in order to receive better service, while I may not be happy for my credit rating or tax data to be shared freely with different companies. I would therefore allow an

intermediary to act on my behalf, tagging the relevant information in some form to ensure that it was not used in a manner that I had not previously agreed to.

Resellers

Resellers are those entities that combine inputs from several different intermediaries, combine it together, analyze, and sell it to either end-users or to corporate entities.

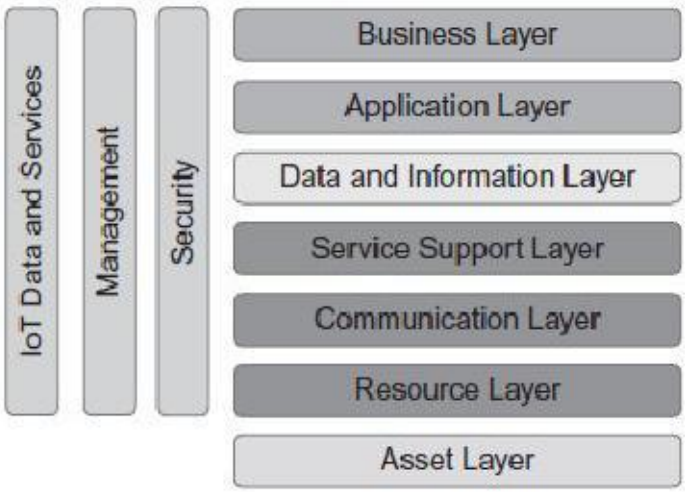
One example is BlueKai, which tracks the online shopping behavior of Internet users and mines the data gathered for "purchasing intent" in order to allow advertisers to target buyers more accurately.

BlueKai combines data from several sources, including Amazon, Ebay, and Alibaba. Through this data, it is able to identify regional trends, helping companies to identify not just which consumer group to target their goods to, but also which part of the country.

As an example, BlueKai is able to identify all those end-users in West Virginia currently searching for a washing machine in a certain price bracket.

Q-14 Explain An IoT architecture outline OR

Draw and explain layered Architecture of IOT.



Functional Layers and capabilities of an IOT Solutions

(1) Asser Layer

At the lowest level is the Asset Layer. This layer is, strictly speaking, not providing any functionality within a target solution, but represents the raison d'eˆtre for any IoT application.

The assets of interest are the real world objects and entities that are subject to being monitored and controlled, as well as having digital representations and identities.

The typical examples include vehicles and machinery, fixed infrastructures such as buildings and utility systems, homes, and people themselves.

Assets are instrumented with embedded technologies that bridge the digital realm with the physical world, and that provide the capabilities to monitor and control the assets as well as providing identities to the assets.

(2) Resource Layer

The Resource Layer provides the main functional capabilities of sensing, actuation, and embedded identities.

Sensors and actuators in various devices that may be smartphones or Wireless Sensor Actuator Networks (WSANs), M2M devices like smart meters, or other sensor/actuator nodes, deliver these functions.

Identification of assets can be provided by different types of tags; for instance, Radio Frequency Identification (RFID), or optical codes like bar codes or Quick Response (QR) codes.

(3) Communication Layer

The purpose of the Communication Layer is to provide the means for connectivity between the resources on one end and the different computing infrastructures that host and execute service support logic and application logic on the other end.

Different types of networks realize the connectivity, and it is customary to differentiate between the notion of a Local Area Network (LAN) and a Wide Area Network (WAN).

WANs can be realized by different wired or wireless technologies, for instance, fiber or Digital Subscriber Line (DSL) for the former, and cellular mobile networks, satellite, or microwave links for the latter.

(4) Service Support Layer

IoT applications benefit from simplification by relying on support services that perform common and routine tasks. These support services are provided by the Service Support Layer and are typically executing in data centers or server farms inside organizations or in a cloud environment.

These support services can provide uniform handling of the underlying devices and networks, thus hiding complexities in the communications and resource layers.

Examples include remote device management that can do remote software upgrades, remote diagnostics or recovery, and dynamically reconfigure application processing such as setting event filters.

Communication-related functions include selection of communication channels if different networks can be used in parallel, for example, for reliability purposes, and publish_subscribe and message queue mechanisms. Location Based Service (LBS) capabilities and various Geographic Information System (GIS) services are also important for many IoT applications.

(5) Data and Information Layer

Where the Resource, Communication, and Service Support layers have concrete realizations in terms of devices and tags, networks and network nodes, and computer servers, the Data and Information Layer provides a more abstract set of functions as its main purposes are to capture knowledge and provide advanced control logic support.

Key concepts here include data and information models and knowledge representation in general, and the focus is on the organization of information. We refer to a Knowledge Management Framework (KMF) as a collective term to include data, information, domain-specific knowledge, actionable services descriptions as, for example, represented by single

actuators or more complex composite sensing and actuation services, service descriptors, rules, process or orkflow descriptions, etc.

(6) Application Layer

The Application Layer in turn provides the specific IoT applications.

There is an open-ended array of different applications, and typical examples include smart metering in the Smart Grid, vehicle tracking, building automation.

(7) Business Layer

The final layer in our architecture outline is the Business Layer, which focuses on supporting the core business or operations of any enterprise, organization, or individual that is interested in IoT applications.

The enterprise systems can, for example, be Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), or other Business Support Systems (BSS).

The business layer also provides exposure to APIs for third parties to get access to data and information, and can also contain support for direct access to applications by human users.

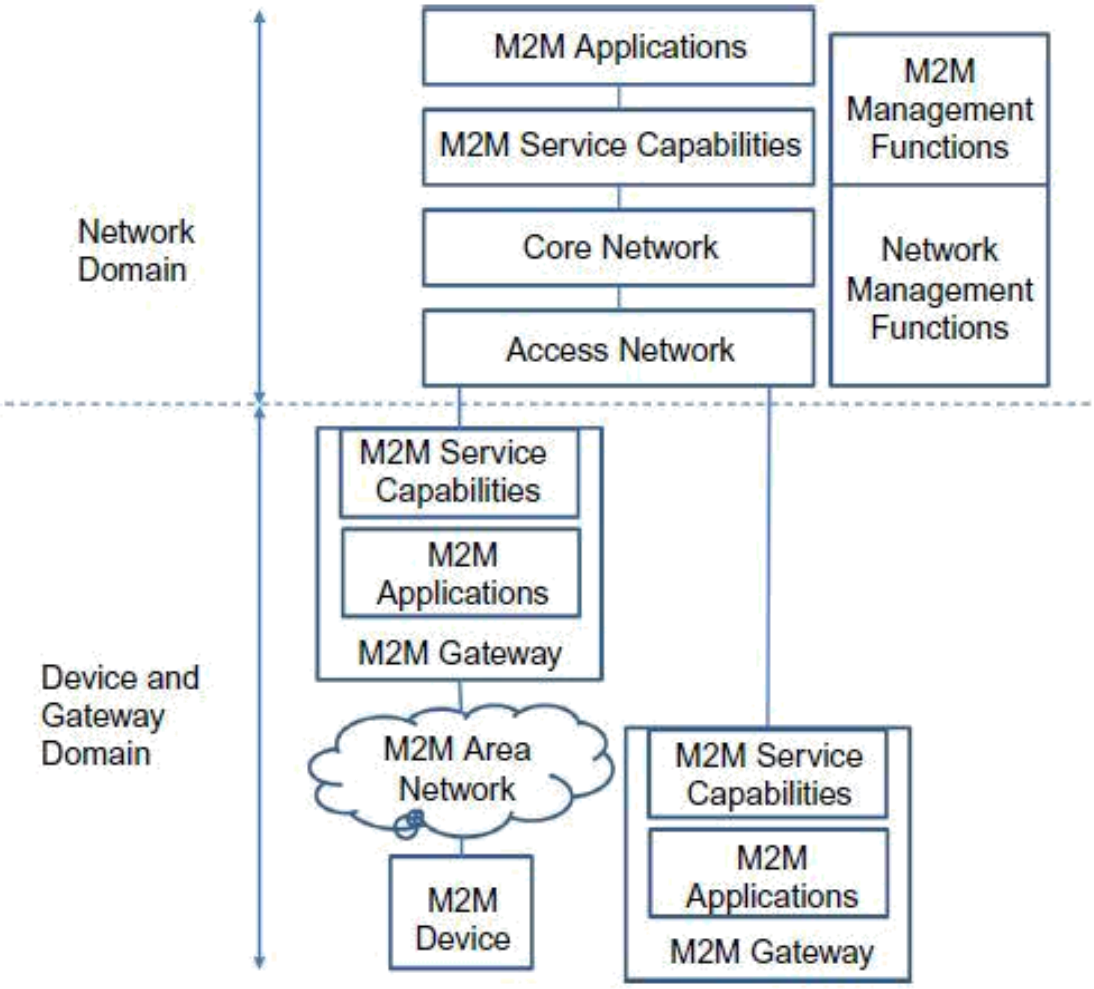
The business layer relies on IoT applications as one set of enablers out of many (e.g. field force automation), and takes care of necessary orchestration and composition to support a business process workflow.

Q- 14 ETSI M2M high-level architecture

This high-level architecture is a combination of both a functional and topological view showing some functional groups (FG) clearly associated with pieces of physical infrastructure (e.g. M2M Devices, Gateways) while other functional groups lack specific topological placement.

There are two main domains, a network domain and a device and gateway domain.

The boundary between these conceptually separated domains is the topological border between the physical devices and gateways and the physical communication infrastructure (Access network).



The Device and Gateway Domain contains the following functional/ topological entities:

M2M Device: This is the device of interest for an M2M scenario, for example, a device with a temperature sensor.
An M2M Device contains M2M Applications and M2M Service Capabilities. An M2M device connects to the Network Domain either directly or through an M2M Gateway:

Direct connection: The M2M Device is capable of performing registration, authentication, authorization, management, and provisioning to the Network Domain. Direct connection also means that the M2M device contains the appropriate physical layer to be able to communicate with the Access Network.

Through one or more M2M Gateway: This is the case when the M2M device does not have the appropriate physical layer, compatible with the Access Network technology, and therefore it needs a network domain proxy. Moreover, a number of M2M devices may form their own local M2M Area Network that typically employs a different networking technology from the Access Network.

M2M Area Network: This is typically a local area network (LAN) or a Personal Area Network (PAN) and provides connectivity between M2M Devices and M2M Gateways.

Typical networking technologies are IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee, IETF 6LoWPAN/ROLL/ CoRE), MBUS, KNX (wired or wireless) PLC, etc.

M2M Gateway: The device that provides connectivity for M2M Devices in an M2M Area Network towards the Network Domain. The M2M Gateway contains M2M Applications and M2M Service Capabilities. The M2M Gateway may also provide services to other legacy devices that are not visible to the Network Domain.

The Network Domain contains the following functional/topological entities:

Access Network: this is the network that allows the devices in the Device and Gateway Domain to communicate with the Core Network.

Core Network: Examples of Core Networks are 3GPP Core Network and ETSI TISPAN Core Network. It provides the following functions:

- IP connectivity.
- Service and Network control.
- Interconnection with other networks.

- Roaming.

M2M Service Capabilities: These are functions exposed to different M2M Applications through a set of open interfaces. These functions use underlying Core Network functions, and their objective is to abstract the network functions for the sake of simpler applications.

M2M Applications: These are the specific M2M applications (e.g. smart metering) that utilize the M2M Service Capabilities through the open interfaces.

Network Management Functions: These are all the necessary functions to manage the Access and Core Network (e.g. Provisioning, Fault Management, etc.).

M2M Management Functions: These are the necessary functions required to manage the M2M Service Capabilities on the Network Domain while the management of an M2M Device or Gateway is performed by specific M2M Service Capabilities.

There are two M2M Management functions:

- **M2M Service Bootstrap Function (MSBF):** The MSBF facilitates the bootstrapping of permanent M2M service layer security credentials in the M2M Device or Gateway and the M2M Service Capabilities in the Network Domain.
- **M2M Authentication Server (MAS)**: This is the safe execution environment where permanent security credentials such as the M2M Root Key are stored. Any security credentials established on the M2M Device or Gateway are stored in a secure environment such as a trusted platform module.

An important observation regarding the ETSI M2M functional architecture is that it focuses on the high-level specification of functionalities within the M2M Service Capabilities functional groups and the open interfaces between the most relevant entities, while avoiding specifying in detail the internals of M2M Service Capabilities.

The most relevant entities in the ETSI M2M architecture are the M2M Nodes and M2M Applications.

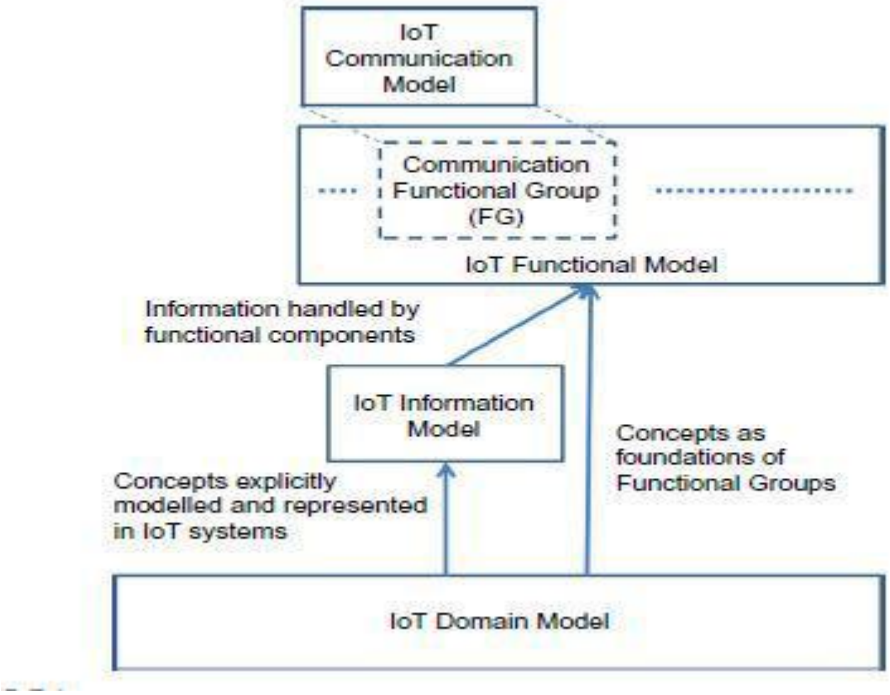
An M2M Node is a logical representation of the functions on an M2M Device, Gateway, and Network that should at least include a Service Capability Layer (SCL) functional group.

Q-15 Reference model and architecture

An ARM (Architecture Reference Model) consists of two main parts: a Reference model and a Reference Architecture.

For describing an IoT ARM, we have chosen to use the IoTA ARM

The foundation of an IoT Reference Architecture description is an IoT reference model. A reference model describes the domain using a number of sub-models



The domain model of an architecture model captures the main concepts or entities in the domain in question, in this case M2M and IoT.

When these common language references are established, the domain model adds descriptions about the relationship between the concepts.

A working system that captures and operates on the domain and information model contains concepts and entities of its own, and this need to be described in a separate model, the functional model.

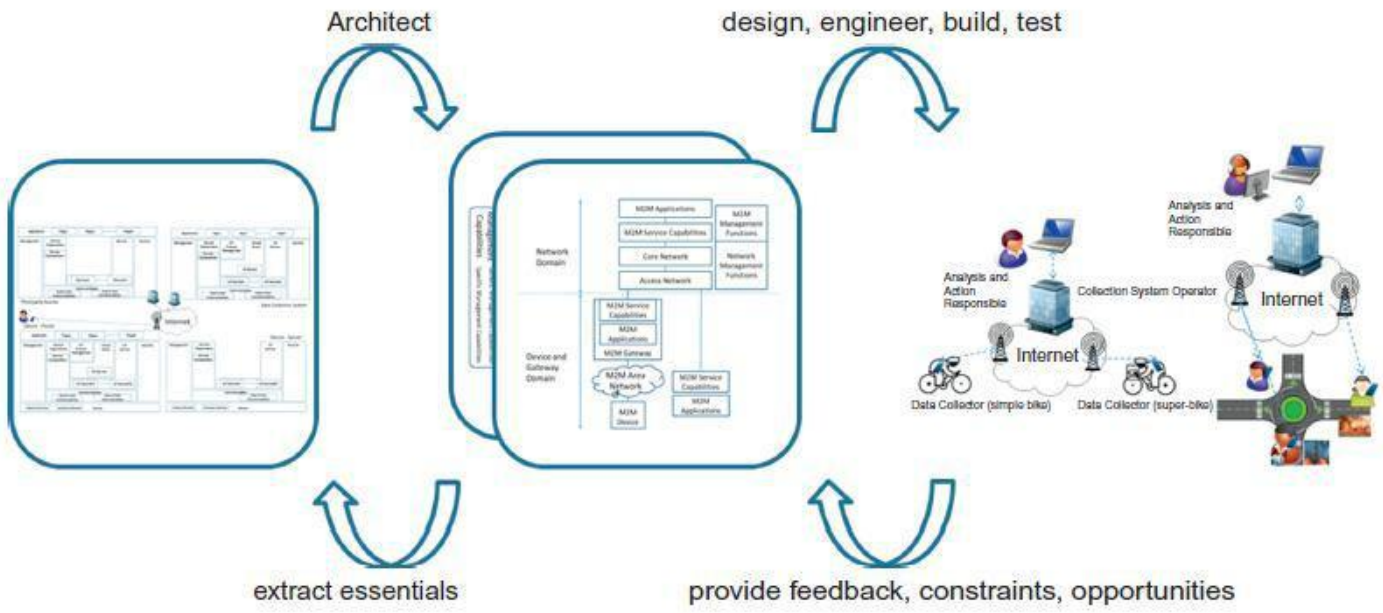
An M2M and IoT system contain communicating entities, and therefore the corresponding communication model needs to capture the communication interactions of these entities.

Apart from the reference model, the other main component of an ARM is the Reference Architecture.

A System Architecture is a communication tool for different stakeholders of the system. Developers, component and System managers, partners, suppliers, and customers have different views of a single system based on their requirements and their specific interactions with the system.

The task becomes more complex when the architecture to be described is on a higher level of abstraction compared with the architecture of real functioning systems.

The high-level abstraction is called Reference Architecture as it serves as a reference for generating concrete architectures and actual systems, shown in the below figure.



A Reference Architecture captures the essential parts of an architecture, such as design principles, guidelines, and required parts (such as entities), to monitor and interact with the physical world for the case of an IoT Reference architecture.

A concrete architecture can be further elaborated and mapped into real world components by designing, building, engineering, and testing the different components of the actual system.

As the figure implies, the whole process is iterative, which means that the actual deployed system in the field provides invaluable feedback with respect to the design and engineering choices, current constraints of the system, and potential future opportunities that are fed back to the concrete architectures.

The general essentials out of multiple concrete architectures can then be aggregated, and contribute to the evolution of the Reference Architecture.

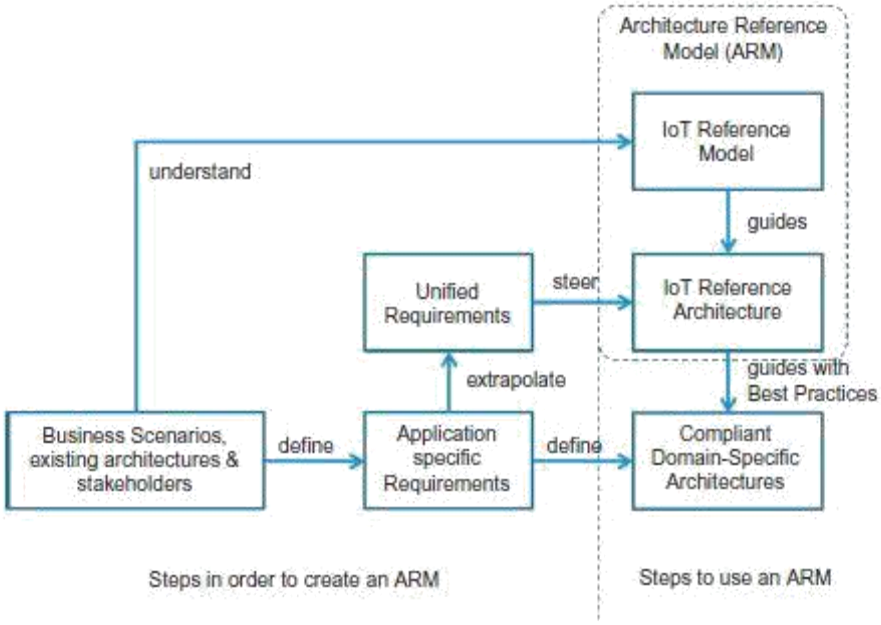


FIGURE 7.3

IoT Reference Model and Reference Architecture dependencies.

Q-16 IoT Reference Architecture

Reference Architecture is a starting point for generating concrete architectures and actual systems.

A Reference Architecture, on the other hand, serves as a guide for one or more concrete system architects. However, the concept of views for the presentation of an architecture is also useful for the IoT Reference Architecture.

Views are useful for reducing the complexity of the Reference Architecture blueprints by addressing groups of concerns one group at a time.

However, since the IoT Reference Architecture does not contain details about the environment where the actual system is deployed, some views cannot be presented in detail or at all;

for example, the view that shows the concrete Physical Entities and Devices for a specific scenario.

In order to address the concerns of mainly the concrete IoT architect, and secondly the concerns of most of the above stakeholders, we have chosen to present the Reference Architecture as a set of architectural views.

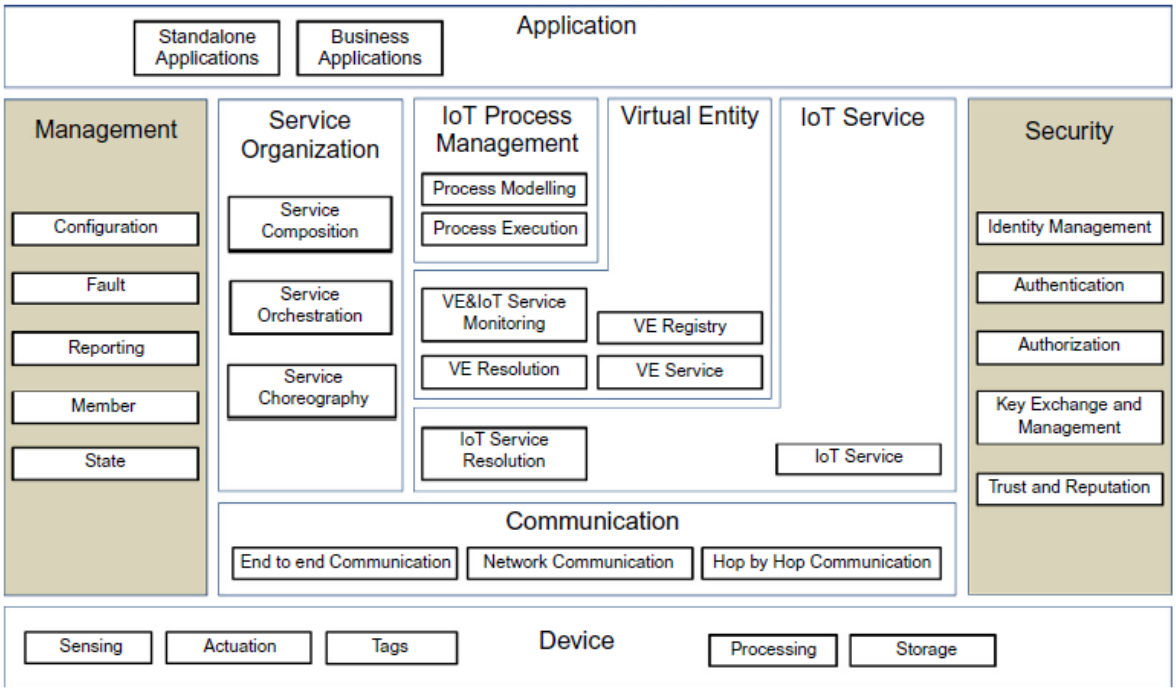
- **Functional View:** Description of what the system does, and its main functions.
- **Information View:** Description of the data and information that the system handles.

• **Deployment and Operational View:** Description of the main real world components of the system such as devices, network routers, servers, etc.

Q-17 Functional View

The functional view for the IoT Reference Architecture is presented in the following architecture.

Functional Groups (FGs) presented earlier in the IoT Functional Model, each of which includes a set of Functional Components (FCs). It is important to note that not all the FCs are used in a concrete IoT architecture, and therefore the actual system as explained earlier.



(1) Device and Application functional group

The Device and Application FGs are already covered in the IoT Functional Model. For convenience the Device FG contains the Sensing, Actuation, Tag, Processing, Storage FCs, or simply components. These components represent the resources of the device attached to the Physical Entities of interest. The Application FG contains either standalone applications (e.g. for iOS, Android, Windows phone), or Business Applications that connect the IoT system to an Enterprise system.

(2) Communication functional group

Communication functional group The Communication FG contains the End-to-End Communication, Network Communication, and Hop-by-Hop communication components:

The Hop-by-Hop Communication is applicable in the case that devices are equipped with mesh radio networking technologies such as IEEE 802.15.4 for which messages have to traverse the mesh from node-to-node (hop-by-hop) until they reach a gateway node which forwards the message (if needed) further to the Internet.

The Network FC is responsible for message routing & forwarding and the necessary translations of various identifiers and addresses.

The translations can be

(a) between network layer identifiers to MAC and/or physical network identifiers,

- between high-level human readable host/node identifiers to network layer addresses (e.g. Fully Qualified Domain Names (FQDN) to IP addresses, a function implemented by a Domain Name System (DNS) server), and
- translation between node/service identifiers and network locators in case the higher layers above the networking layer use node or service identifiers that are decoupled from the node addresses in the network

The End-to-End Communication FC is responsible for end-to-end transport of application layer messages through diverse network and MAC/PHY layers. In turn, this means that it may be responsible for end-to-end retransmissions of missing frames depending on the configuration of the FC. For example, if the End-to-End Communication FC is mapped in an actual system to a component implementing the Transmission Control Protocol (TCP) protocol, reliable

transfer of frames dictates the retransmission of missing frames.

(3)IoT Service functional group

The IoT Service FG consists of two FCs: The IoT Service FC and the IoT Service Resolution FC:

The IoT Service FC is a collection of service implementations, which interface the related and associated Resources.

For a Sensor type of a Resource, the IoT Service FC includes Services that receive requests from a User and returns the Sensor Resource value in synchronous or asynchronous (e.g. subscription/notification) fashion.

A Tag IoT Service can behave both as a Sensor (for reading the identifier of the Tag), or as an Actuator (for writing a new identifier or information on the Tag, if possible).

The IoT Service Resolution FC contains the necessary functions to realize a directory of IoT Services that allows dynamic management of IoT Service descriptions and discovery/lookup/resolution of IoT Services by other Active Digital Artifacts.

(4) Virtual Entity functional group

The Virtual Entity FG contains functions that support the interactions between Users and Physical Things through Virtual Entity services.

An example of such an interaction is the query to an IoT system of the form, "What is the temperature in the conference room Titan?" The Virtual Entity is the conference room "Titan," and the conference room attribute of interest is "temperature."

Assuming that the room is actually instrumented with a temperature sensor, if the User had the knowledge of which temperature sensor is installed in the room (e.g. TempSensor #23), then the User could re-formulate and re-target this query to, "What is the value of TempSensor #23?"

The Virtual Entity Service FC enables the interaction between Users and Virtual Entities by means of reading and writing the Virtual Entity attributes (simple or complex), which can be read or written, of course.

In general attributes that are associated with IoT Services, which in turn represent Sensor Resources, can only be read.

There can be, of course, special Virtual Entities associated with the same Sensor Resource through another IoT Service that allow write operations.

The Virtual Entity Registry FC maintains the Virtual Entities of interest for the specific IoT system and their associations. The component offers services such as creating/reading/updating/deleting Virtual Entity descriptions and associations.

The Virtual Entity Resolution FC maintains the associations between Virtual Entities and IoT Services, and offers services such as creating/reading/updating/deleting associations as well as lookup and discovery of associations.

The Virtual Entity and IoT Service Monitoring FC includes:

(a) functionality to assert static Virtual Entity_IoT Service associations,
(b) functionality to discover new associations based on existing associations or Virtual Entity attributes such as location or proximity, and
(c) continuous monitoring of the dynamic associations between Virtual Entities and IoT Services and updates of their status in case existing associations are not valid any more.

(5) IoT process management functional group

The IoT Process Management FG aims at supporting the integration of business processes with IoT-related services. It consists of two FCs:

The Process Modeling FC provides that right tools for modeling a business process that utilizes IoT-related services.

The Process Execution FC contains the execution environment of the process models created by the Process Modelling FC and executes the created processes by utilizing the Service Organization FG in order to resolve high-level application requirements to specific IoT services.

(6)Service Organization functional group

The Service Organization FG acts as a coordinator between different Services offered by the system. It consists of the following FCs:

The Service Composition FC manages the descriptions and execution environment of complex services consisting of simpler dependent services.

The Service Orchestration FC resolves the requests coming from IoT Process Execution FC or User into the concrete IoT services that fulfil the requirements.

The Service Choreography FC is a broker for facilitating communication among Services using the Publish/Subscribe pattern. Users and Services interested in specific IoT-related services subscribe to the Choreography FC, providing the desirable service attributes even if the desired services do not exist.

(7)Security functional group

The Security FG contains the necessary functions for ensuring the security and privacy of an IoT system. It consists of the following FCs:

The Identity Management FC manages the different identities of the involved Services or Users in an IoT system in order to achieve anonymity by the use of multiple pseudonyms.

The Authentication FC verifies the identity of a User and creates an assertion upon successful verification. It also verifies the validity of a given assertion.

The Authorization FC manages and enforces access control policies. It provides services to manage policies (CUD), as well as taking decisions and enforcing them regarding access rights of restricted resources.

The Key Exchange & Management is used for setting up the necessary security keys between two communicating entities in an IoT system. This involves a secure key distribution function between communicating entities.

(8)Management functional group

The Management FG contains system-wide management functions that may use individual FC management interfaces. It is not responsible for the management of each component, rather for the management of the system as a whole. It consists of the following FCs:

The Configuration FC maintains the configuration of the FCs and the Devices in an IoT system. The component collects the current configuration of all the FCs and devices, stores it in a historical database, and compares current and historical configurations.

The Fault FC detects, logs, isolates, and corrects system-wide faults if possible. This means that individual component fault reporting triggers fault diagnosis and fault recovery procedures in the Fault FC.

The Member FC manages membership information about the relevant entities in an IoT system.

The State FC is similar to the Configuration FC, and collects and logs state information from the current FCs, which can be used for fault diagnosis, performance analysis and prediction, as well as billing purposes. This component can also set the state of the other FCs based on system-wise state information.

The Reporting FC is responsible for producing compressed reports about the system state based on input from FCs.

Q-18 Information view

purposes of connected and smart objects in the IoT is the exchange of information between each other and also with external systems.

The information view helps to generate an overview about static information structure and dynamic information flow.

The information view consists of

- (a) the description of the information handled in the IoT System,

- (b) the way information is handled, OR the information lifecycle and the information handling components.

Information description

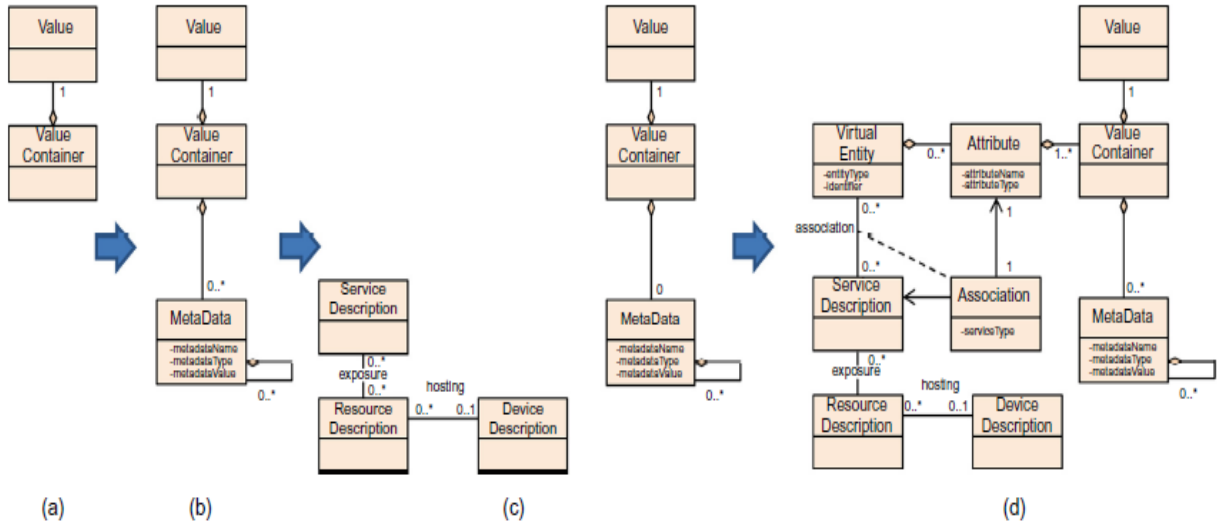
The pieces of information handled by an IoT system complying to an ARM are

- Virtual Entity context information
- IoT Service output itself
- Associations between Virtual Entities and related IoT Services.
- Virtual Entity Associations with other Virtual Entities
- IoT Service Descriptions, which contain associated Resources, interface, descriptions, etc.
- Resource Descriptions, which contain the type of resource (e.g. sensor), identity, associated Services, and Devices.

Information flow and lifecycle

The flow of information in an IoT system follows two main directions.

- From devices that produce information such as sensors and tags, information follows a context-enrichment process until it reaches the consumer application or part of the larger system, and
- From the application or part of a larger system information it follows a context-reduction process until it reaches the consumer types of devices (e.g. actuators).

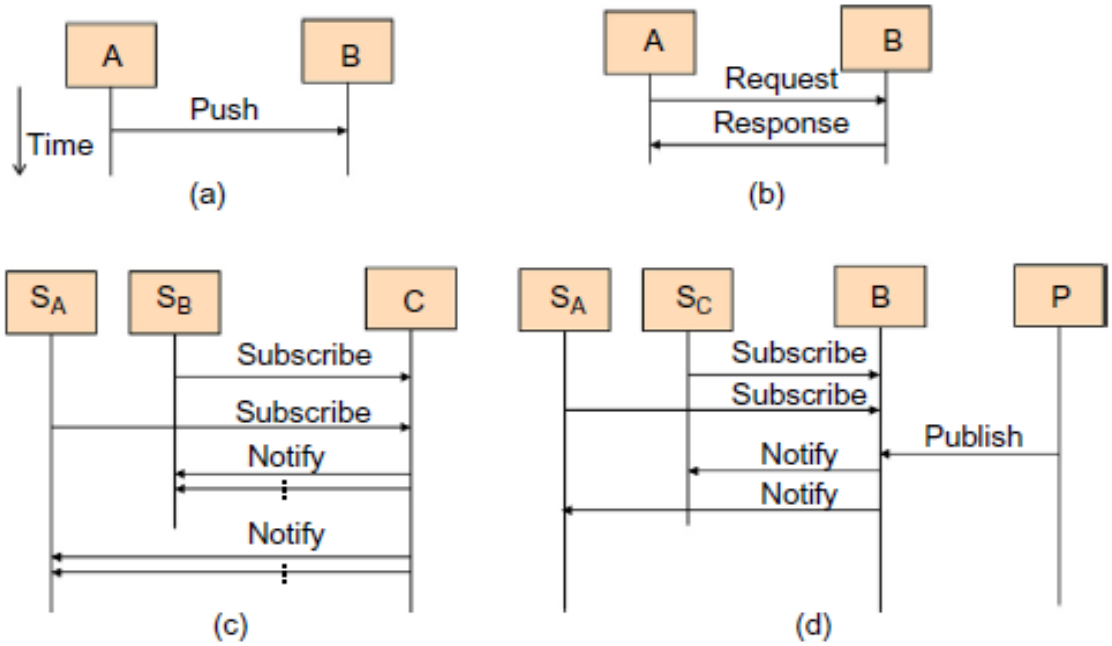


Information-enrichment process

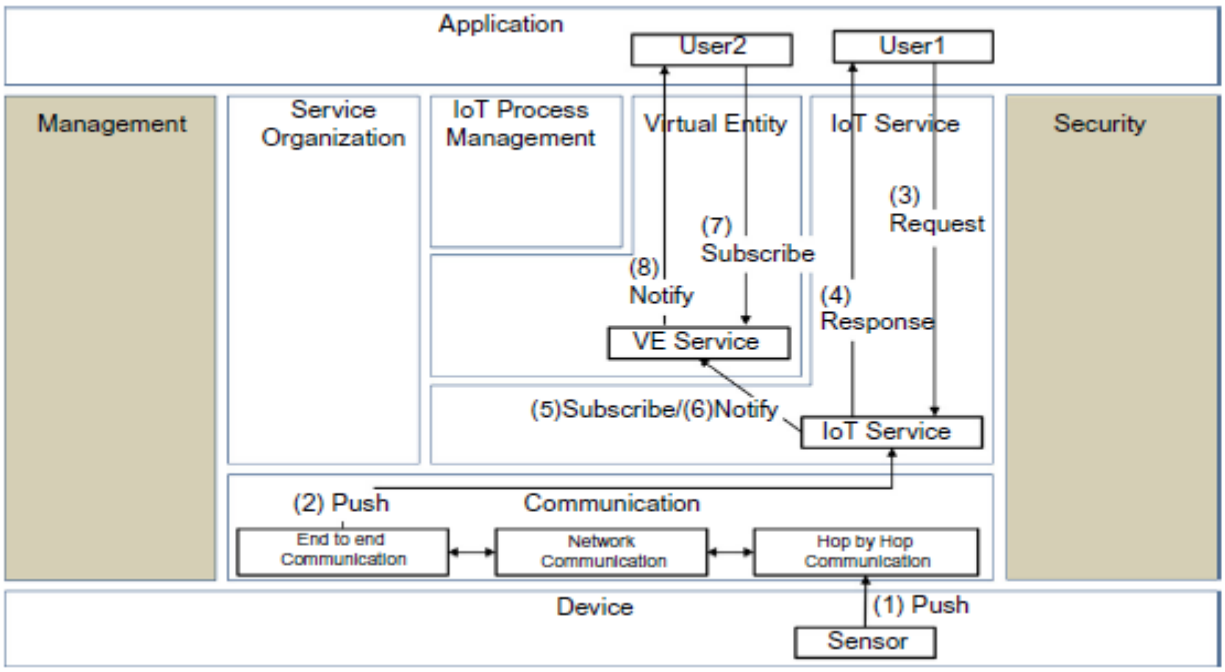
Information handling

The presentation of information handling in an IoT system assumes that FCs exchange and process information.

The exchange of information between FCs follows the interaction patterns below

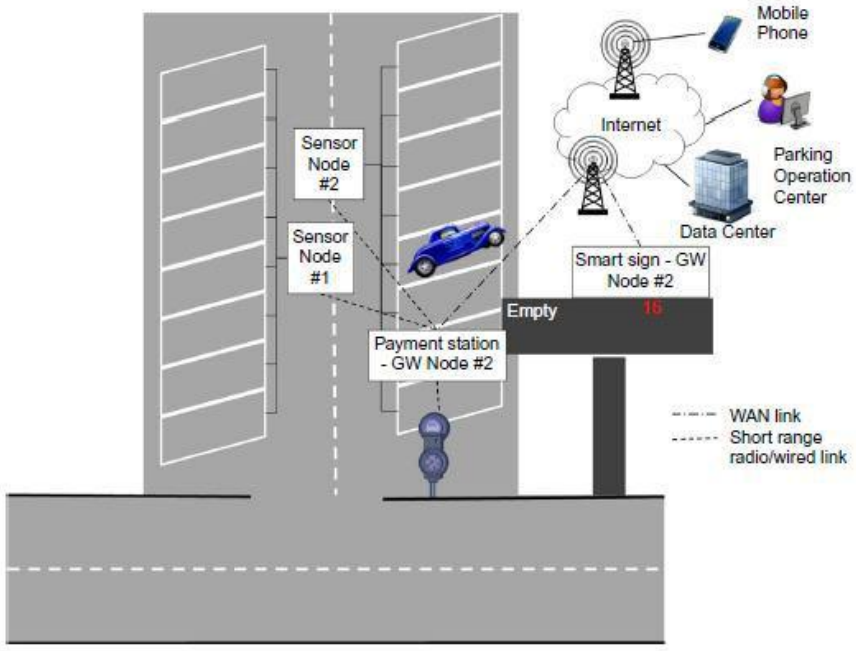


Information exchange patterns



Device, IoT Service, and Virtual Entity Service Interactions

Q-19 Deployment and Operational View



The Deployment and Operational View depends on the specific actual use case and requirements, and therefore we present here one way of realizing the Parking Lot example seen earlier.

Above Figure depicts the Devices view as Physical Entities deployed in the parking lot, as well as the occupancy sign.

There are two sensor nodes (#1 and #2), each of which are connected to eight metal/car presence sensors.

The two sensor nodes are connected to the payment station through wireless or wired communication.

The payment station acts both as a user interface for the driver to pay and get a payment receipt as well as a communication gateway that connects the two sensor nodes and the payment interface physical devices (displays, credit card slots, coin/note input/output, etc.)

The occupancy sign also acts as a communication gateway for the actuator node (display of free parking spots),

The physical gateway devices connect through a WAN technology 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 a Service configuration.

The two main applications connected to this management system are human user mobile phone applications and parking operation center applications. We assume that the parking operation center manages several other parking lots using similar physical and virtual infrastructure.

Figure shows two views super imposed, the deployment and functional views, for the parking lot example

Services appear in the figure because an IoT system is typically part of a larger system. Starting from the Sensor Devices, as seen earlier,

Sensor Node #1 hosts Resource #11_#18, representing the sensors for the parking spots #01_#08, while earlier

Sensor Node #2 hosts Resource #21_#28, representing the sensors for the parking spots #09_#16.

We assume that the sensor nodes are powerful enough to host the IoT Services #11_#18 and #21_#28 representing the respective resources.

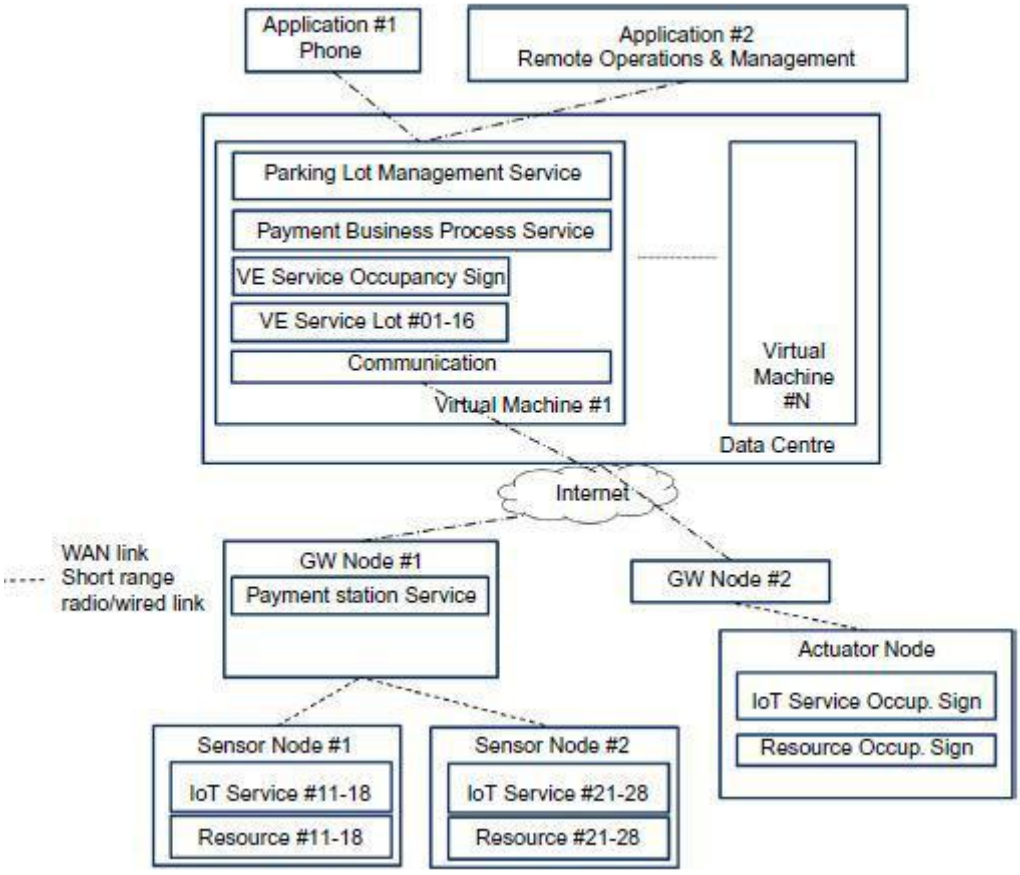


Figure: Parking Lot Deployment & Operational View, Resources, Services, Virtual Entities, Users.

The two sensor nodes are connected to the gateway device that also hosts the payment service with the accompanying sensors and actuators, as seen earlier.

The management system for the specific parking lot, as well as others, is deployed on a virtual machine on a data center.

The virtual machine hosts communication capabilities, Virtual Entity services for the parking spots #01_#16, the Virtual Entity services for the occupancy sign, a payment business process that involves the payment station and input from the occupancy sensor services, and the parking lot management service that provides exposure and access control to the parking lot occupancy data for the parking operation center and the consumer phone applications.

As a reminder, the Virtual Entity service of the parking lot uses the IoT Services hosted on two sensor nodes and performs the mapping between the sensor node identifiers (#11_#18 and #21_#28) to parking spot identifiers (spot#01_#16).

The services offered on these parking spots are to read the current state of the parking spot to see whether it is "free" or "occupied." The Virtual Entity corresponding to the occupancy sign contains one writable attribute: the number of free parking spots.

Starting from the IoT Domain Model, we attempt to perform a high level mapping between the different classes/entities of the model and their realization.

The physical sensors, actuators, tags, processors, and memory, which are parts of a Device, are deployed close to the Physical Entities of Interest, the ones whose properties are monitored or controlled.

Q-20 Explain IOT application for Industry.

IoT technologies capable to improve and easy adapt.

- industrial manufacturing processes,
- enable new and efficient ways to do operate and interact in production plants,
- create new service or supervision means for industrial installations offer an optimized infrastructure,
- reduce operational cost and energy consumption or improve human safety in industrial areas.

Values and benefits

- Value from visibility identification, location tracking
- Value form IoT-supported safety in hard industrial environments
- Value from right information providing or collecting
- Value form improved industrial operation and flows in industry
- Value from reduced production losses
- Value from reduced energy consumption
- Value from new type of processes made possible by IoT applications
- Value form new type of maintenance and lifetime approaches
- Value enabled by smart objects, connected aspects
- Value from sustainability.

IOT applications requirement and capabilities

- **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 adapted to the task and hard working conditions.

- **Reasonable cost.**

  Cost aspects are essential and should be fully justifiable and adapted to the benefit. It is basically about the right balance between cost and benefit rather than low cost.

- **Security and safety.**

  Security requirements are related to the cyber security threats and have to be part of the entire security strategy of the company.

  Safety is mainly related to the device construction and the area of use.

- **Optimal and adaptive set of features.**

  The IoT application should allow to perform desired task with the sufficient, not-richer-then-necessary, set of features

- **Low/No maintenance.**

  Maintenance free or reduced maintenance IoT applications and devices over operational life would be ideal. Maintenance over lifetime is an important aspect impacting the life cycle costs of IoT based solutions.

- **Standardization.**

  IoT devices and applications should be using a set of standards to support interoperability of IoT devices, easy exchange and multivendor possibilities.

- **Integration capabilities**

  Easy integration in the IT and automation and process landscape of the industrial plant are required and may decide if a IoT solution will be used.

- **Reach sensing and data capabilities**

IoT applications will relay more and more on complex sensing allowing distributed supervision and data collection and data capabilities.

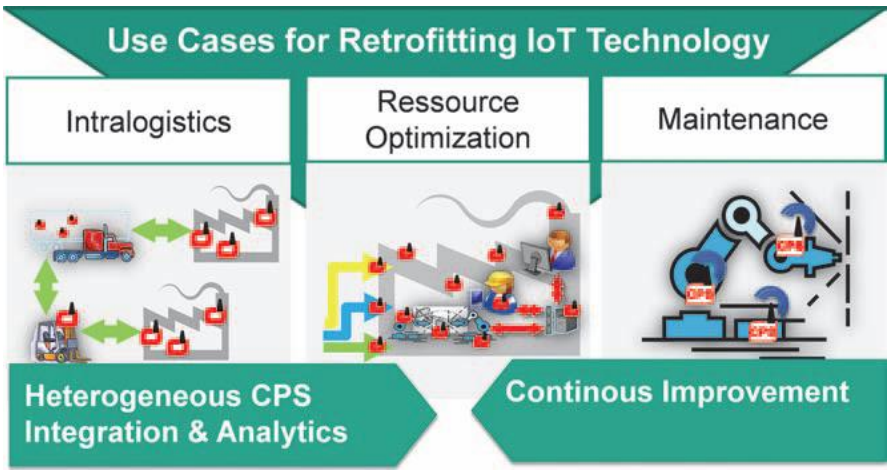
Challenges faced by IoT industry applications

- IoT device technical challenges
- Lifetime and energy challenge
- Data and information challenge
- Humans and business

Q-21 Explain Brownfield of IOT.

The Internet of Things aims to be a disruptive technology in many ways and may change how future industry will work. However, enabling technologies like RFID orWireless Sensor Networks are in place, it is often hindered by the fact that huge investments are needed and the local value is considered too low for adoption. The creation of a global network of various ubiquitous networks is one of the driving technological vision behind the Internet of Things. The economical vision of creating domain-and network-wide business fields and usage scenarios by pervasive information networking uses the "Internet" both as a technical and economical analogon. On one hand, as the global IP-based network that connects over 5 billion devices of different networks, and on the other the resulting economic growth and business cases.

Industrial infrastructures are often older that the networks that formed the initial Internet. They can by no means be considered a green field, but consists of a large installed base with machinery that has lifetimes of up to 40 years. Thus many of the applications of IoT technology that we consider to have high potential value involve retrofittingindustrial systems with IoT systems. These "brownfield" use cases are all targeted towards optimizing existing processes by decreasing the gap between the realworld and the virtualworld. They are thus examples for an evolutionary approach towards an "Industry 4.0" that builds upon IoT Technology



➢ Cost-effective Technical Integration of IoT Devices

A developer of IoT technology has to take various technical requirements into account such as energy, communication bandwidth, communication topology or processing resources of different IoT systems. Additionally the interoperability is crucial to the value of the system. Assuming that in the future the service technician interconnects with a whole range of different types of wireless measurement systems and smart machines of different manufacturers, the analysis application must be aware of the semantics of all interfaces. Furthermore, the ability of the system which consists of heterogeneous components to integrate in the field, to configure and calibrate crucial for the application of adhoc networked sensor system in the maintenance scenario. Loosely coupled, document-based Web services provide a well-defined path to configuration and measurement data from wireless ad hoc systems and automation systems, however, have the disadvantage of a very high runtime overhead.

➢ Cost-effective Process Integration of IoT Devices

Not only the integration but also the IoT enabled processes needs to be costeffective by design and well integrated. Our approach is evolving around existing processes and scaling with the human information consumer, rather than solely relying on big data analytics and total connectivity.

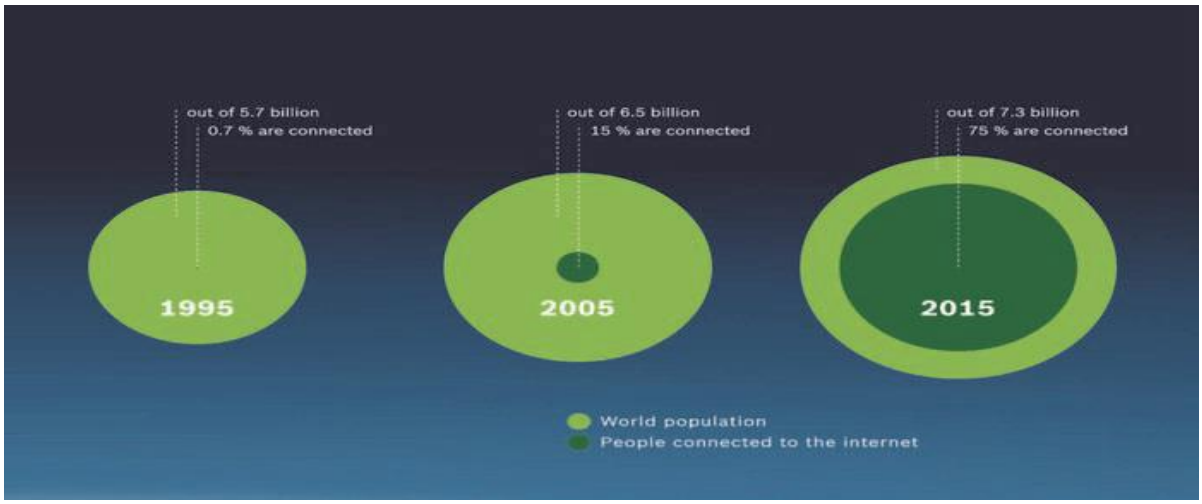
1. Opportunistic data collection through local infrastructures and adhoc mobile access
2. Context-aware interlinking of heterogeneous data starting from existing processes
3. Human agility and expertise supported by a human-centered information design

Global interoperability in contrast to global connectivity and the use of
mobile devices can enable the user to access IoT services ad-hoc. Users are informed in-situ by distributed sensing system, heterogeneous linked data sources and social media paradigms. Building a sensing enterprise from existing technology will require a considerable jump forward in terms of sensing system deployment and configuration, reasoning on linked data, human-computer interaction and adaptable work flows. New approaches are needed for context-aware annotation, synchronization, visualization and triggers on local and remote data.

Q-22 Four Aspects in your Business to Master IoT

1) Internet Conquering Product Business

The Internet of Things & Services is merging the physical and virtual world. Impressive is the growth that is seen in internet access. Whereas in 1995, less than 1% of the world's population was online, this number has exploded: 2.3 billion people were online in 2011, while for the year 2015 we expect 5.5 billion people to have internet access (source: ITU). This equates to around 75% of the world's population, Figure 3.13. Expected devices connected to internet have been estimated by Bosch Software Innovations, to 6.593 billion by 2015,



2) Strategic Business Aspects

Four Aspects of the Internet of Things & Services

[1] Technology:

The internet and its technology are offering an established platform for interconnecting billion things —

from tiny sensors, smart phones, PCs, to high performance computers.

[2] Business Innovation:

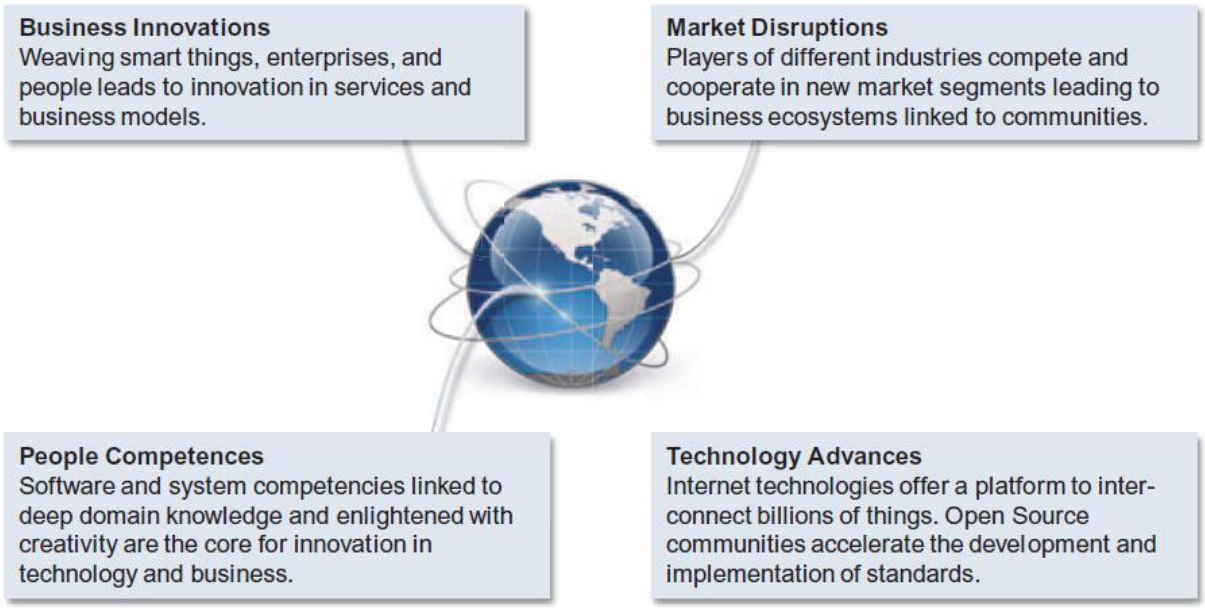
The spirit of internet business models is turning up in traditional product business

[3] Market:

Different industries meet the first time as the Internet of Things & Services crosscuts some of today's separate markets.

[4] Competencies:

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



3.) Vertical Business Domains for IoT

The value of the Internet of Things & Services technology is delivered in vertical application domains

Connected energy

We are currently witnessing a paradigm shift in today's energy market. From the dogma of a production structure with large power plants to a world of many small, distributed power generation systems. Low voltage networks are especially affected by these changes and are facing new challenges. Today, the many distributed power generation systems are connected to the low voltage grid, but not transparently. Consequently, distribution grid operators are forced to react instead of being able to act in order to ensure network stability. While large power plants operate based on accurate and agile schedules, decentralized power generation plants are often operated along subsidy policies and not according to the forces of the electricity market.

4.) Reference Architecture and the Core Competence for Business

The business success in one vertical domain is the key entry point, but successful architectures will reach out to other verticals later. Only architectures that can cover multiple domains will be

successful in the long run, as the domain "silos" of the past still prevents a lot of innovation between the domains: e.g., between automotive and energy in electromobility.

Q-23 Give details about Value Creation from Big Data and Serialization.

Refer any case study paper

Q-24 Explain IOT for Retailing Industry.

Refer any case study paper

Q-25 Explain IOT For Oil and Gas Industry.

Refer any case study paper

Q-26 Give Opinions on IOT Application and Value for Industry.

Refer any case study paper

Q-27 Introduction about on Overview of Governance, Privacy and Security Issues.

The European Research Cluster on the Internet of Things has created a number of activity chains to favour close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges.

The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives.
IERC Activity Chain 05 is a cross-project activity focused on making a valued contribution to IoT privacy, security and governance in the area of Internet of Things.the challenge to define a common agreed definition for Governance of IoT. the concepts of security and privacy do not have a uniform definition in literature even if there is a common agreement on these concepts.

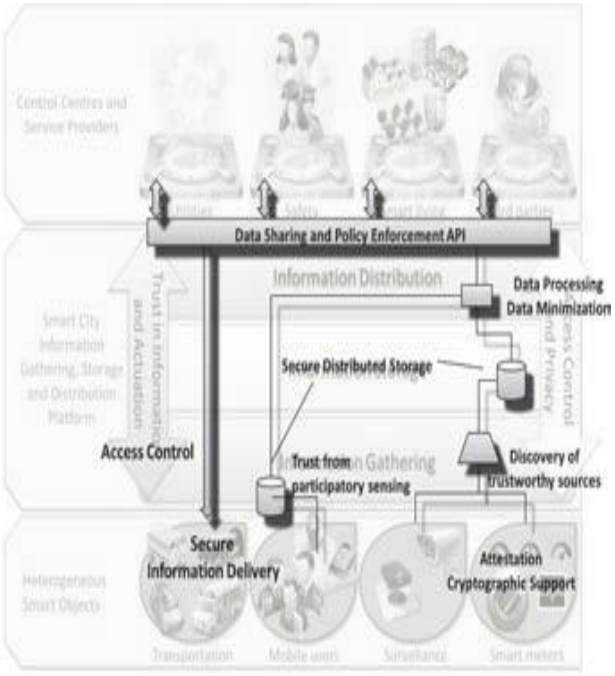
the main objective of the Activity Chain 05 is to identify research challenges and topics, which could make IoT more secure for users (i.e. citizen, business and government), to guarantee the

privacy of users and support the confident, successful and trusted development of the IoT market.

Q-28 Explain Privacy and Trust in IOT-Data- Platforms for Smart Cities.

Aim: Smart City technologies is to provide different optimization mechanisms for different aspects of data management.

Data is gathered from various sources owned by different administrative domains.



The information needs to cross multiple administrative boundaries and can be used for multiple purposes — in fact it could be used for, at the time of gathering, unknown purposes. Also actuation decisions can be taken in a coordinated way between multiple control centres or data providers.

There is a need of an information sharing platform in which data flows from various sources and from different administrative boundaries need to be treated in a secure and privacy preserving way.

To ensure this, security and privacy need to be part of the platform by design and may not be added later on.

The design goal and challenge is allowing user/service control of the data accessible and at the same time providing solution for easily configured management of the process.

All parties involved in the overall systems such as sensors and actuators, end users, data owners but also service providers need strong mechanisms for reliability and trust.

Users and residents of the system will require finegrained access and data privacy policies they want to enforce.

Example:

a user might be willing to share location information with family and friends and make the information available in aggregated form for improvement of the public transport.But the same user might not want the information to be used by other 3rd-party service providers. New applications and synergies are possible if the data is shared between multiple domains. However, several challenges need to be overcome to make this possible.

Q-29 Explain Data Aggregation for the IOT in Smart Cities.

Refer any Case study paper