Internet of Things - Unit 1

vedveethi.co.in/eNote/IoT/CS-6005 Unit 1 - Internet of Things.htm

Department of Computer Science and Engineering Subject Notes

CS-6005 Elective-II (1) Internet of Things

Unit -1

Topics to be covered

Introduction: Definition, Characteristics of IOT, IOT Conceptual framework, IOT Architectural view, Physical design of IOT, Logical design of IOT, Application of IOT.

Definition-The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects. By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves. 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. Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. From any time, any place connectivity for anyone, we will now have connectivity for anything.

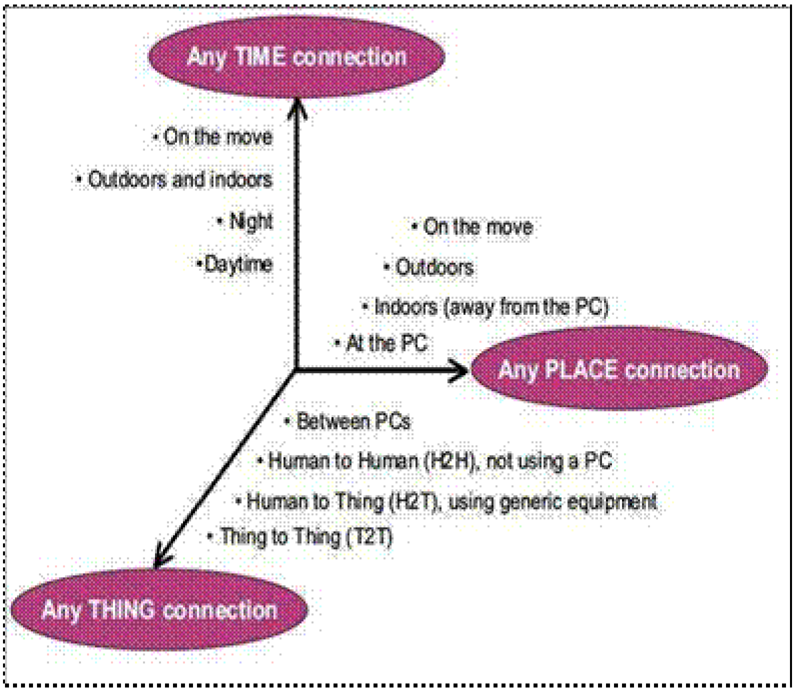

Fig. 1.1 Internet of Things Accessibility

Characteristics of IOT-The no-need-to-know in terms of the underlying details of infrastructure, applications interface with the infrastructure via the APIs.The flexibility and elasticity allows these systems to scale up and down at will utilizing the resources of all kinds CPU, storage, server capacity, load balancing, and databases The "pay as much as used and needed" type of utility computing and the "always on!, anywhere and any place" type of network-based computing. The fundamental characteristics of the IoT are as follows:

· **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

· **Things-related services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

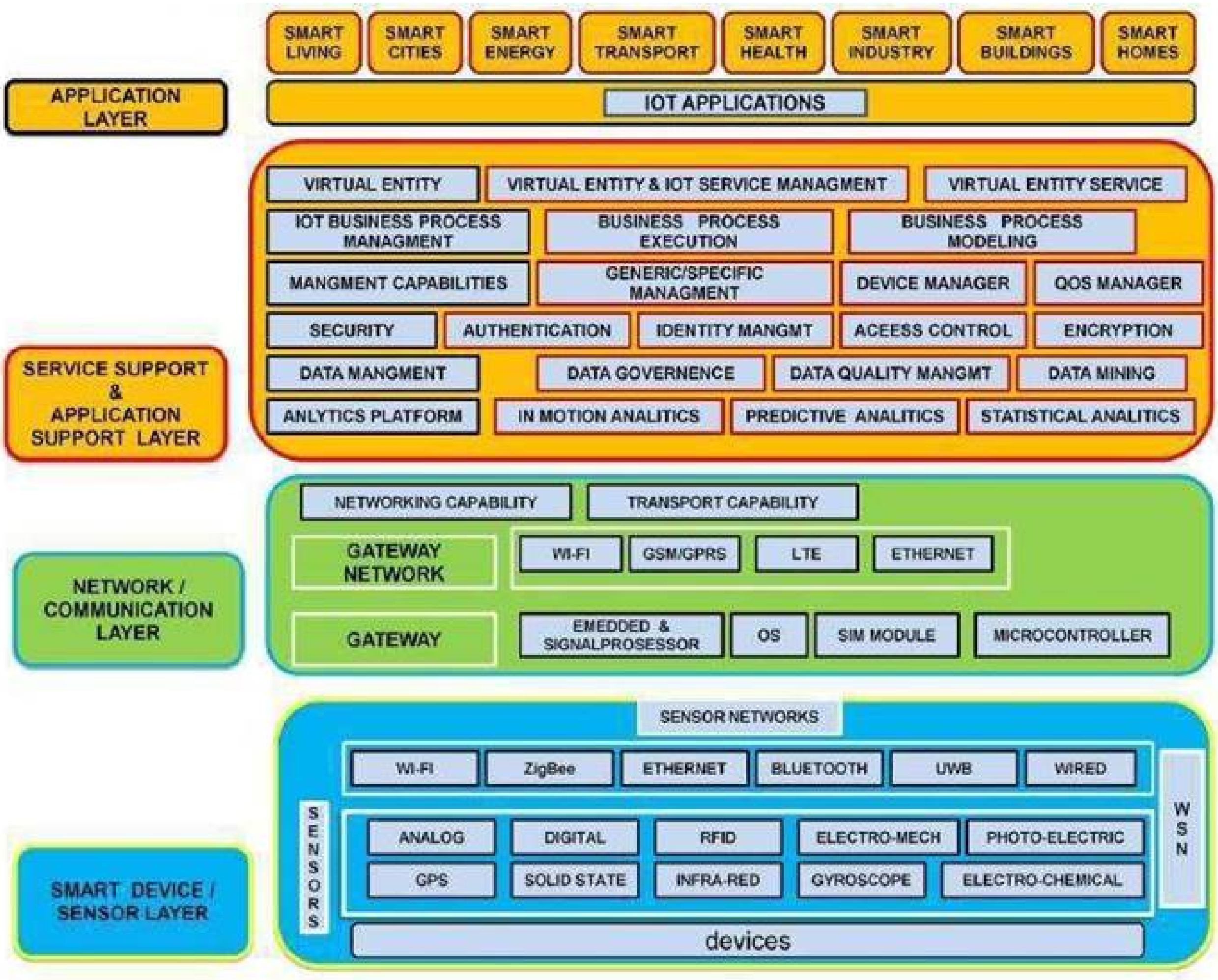

Fig. 1.2 IoT Architecture

IOT conceptual view-

· The main tasks of this framework are to analyze and determine the smart activities of these intelligent devices through maintaining a dynamic interconnection among those devices. The proposed framework will help to standardize IoT infrastructure so that it can receive e-services based on context information leaving the current infrastructure unchanged. The active collaboration of these heterogeneous devices and protocols can lead to future ambient computing where the maximum utilization of cloud computing will be ensured.

· This model is capable of logical division of physical devices placement, creation of virtual links among different domains, networks and collaborate among multiple application without any central coordination system. IaaS can afford standard functionalities to accommodate and provides access to cloud infrastructure. The service is generally offered by modern data centers maintained by giant companies and organization. It is categorized as virtualization of resources which permits a user to install and run application over virtualization layer and allows the system to be distributed, configurable and scalable.

·	Total infrastructure system can be categorized into 4 layers to receive context supported e-services out of raw data from the Internet of Things. These 4 layers establish a generic framework that does not alter the current network infrastructure but create an interfacing among services and entities through network virtualization.

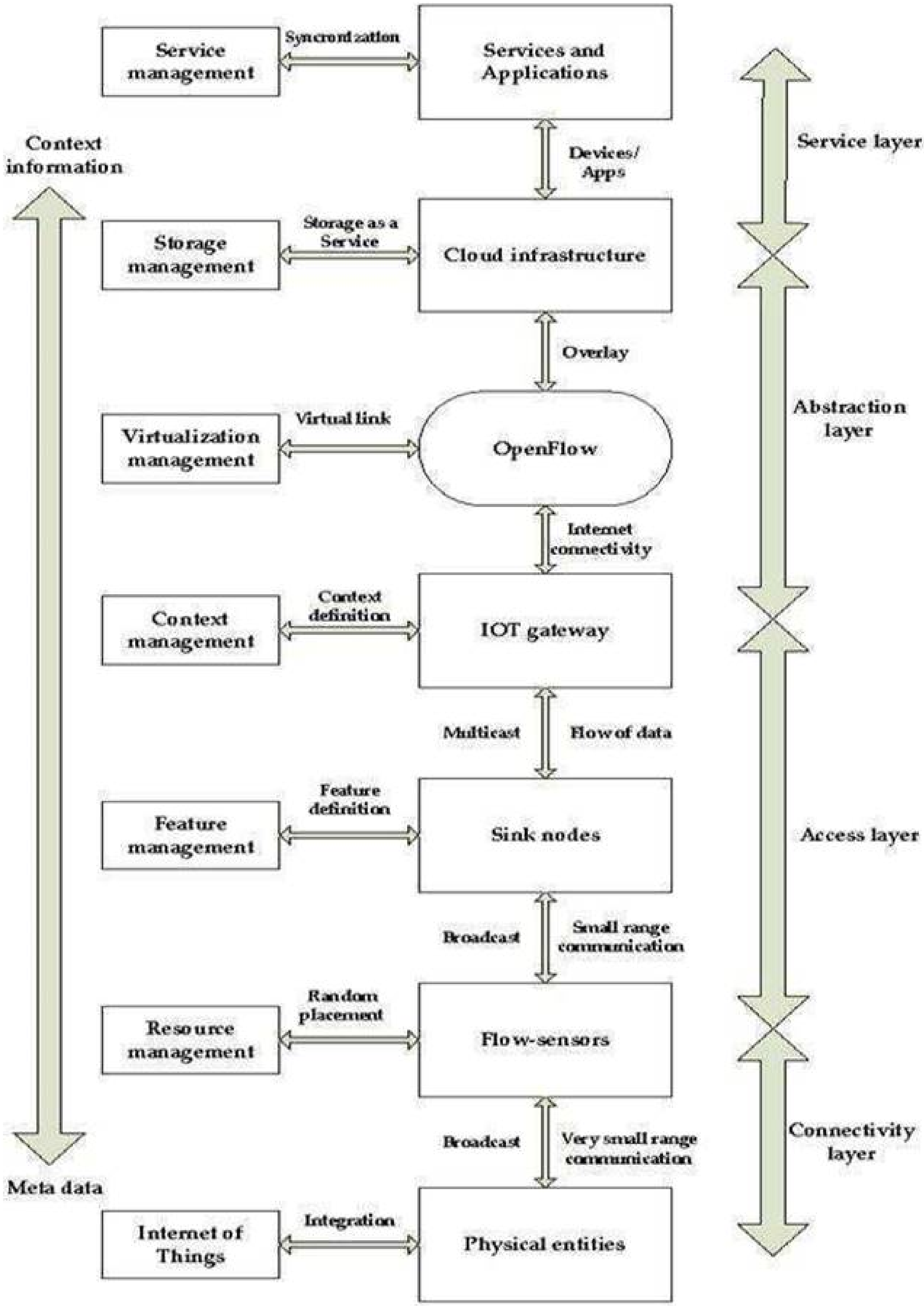

Fig. 1.3 IoT Conceptual View

1. Connectivity Layer-

This layer includes all the physical devices involved in the framework and the interconnection among them. Future internet largely depends on the unification of these common objects found everywhere near us and these should be distinctly identifiable and controllable.

This layer also involves assigning of low range networking devices like sensors, actuators, RFID tags etc and resource management checks the availability of physical resources of all the devices and networks involved in the underlying infrastructure. These devices contain very limited resources and resource management ensures the maximum utilization with little overhead. It also allows sharing and distribution of information among multiple networks or single network divided into multiple domains.

2. Access Layer-

· Context Data will be reached to internet via IoT Gateway as captured by short range devices in form of raw data. Access layer comprises topology definition, network initiation, creation of domains etc. This layer also includes connection setup, intra-inter domain communication, scheduling, packet transmissions between flow-sensors and IoT gateway. The simulation was run later in this paper for different scenario based on this layer. Feature management contains a feature filter which accepts only acceptable context data and redundant data are rejected. Large number of sensor maintains lots of features but only a small subset of features is useful generate a context data.

· Feature filter helps to reduce irrelevant data transmission, increases the data transfer rate of useful data and reduce energy and CPU consumption too. Number of features can be different based on the application requirements and context data types.

3. Abstraction Layer-

· One of the most important characteristics of OpenFlow is to add virtual layers with the preset layers, leaving the established infrastructure unchanged. A virtual link can be created among different networks and a common platform can be developed for various communication systems. The system is fully a centralized system from physical layer viewpoint but a distribution of service (flow visor could be utilized) could be maintained. One central system can monitor, control all sorts of traffics. It can help to achieve better band-width, reliability, robust routing, etc. which will lead to a better Quality of Services (QoS).

· In a multi-hopping scenario packets are transferred via some adjacent nodes. So, nodes near to access points bears too much load in comparison to distant nodes in a downstream scenario and inactivity of these important nodes may cause the network to be collapsed. Virtual presence of sensor nodes can solve the problem where we can create a virtual link between two sensor networks through access point negotiation. So, we can design a three a three layer platform, where common platform and virtualization layer are newly added with established infrastructure. Sensors need not to be worried about reach-ability or their placement even in harsh areas. Packet could be sent to any nodes even if it is sited on different networks.

4. Service Layer-

· Storage management bears the idea about all sorts of unfamiliar and/or important technologies and information which can turn the system scalable and efficient. It is not only responsible for storing data but also to provide security along with it. It also allows accessing data effectively; integrating data to enhance service intelligence, analysis based on the services required and most importantly increases the storage efficiency. Storage and management layer involves data storage & system supervision, software services and business management & operations. Though they are included in one layer, the business support system resides slightly above of cloud computing service whereas Open-Flow is placed below of it as presented to include virtualizations and monitor management.

· Service management combines the required services with organizational solutions and thus new generation user service becomes simplified. These forthcoming services are necessitated to be co

interrelated and combined in order to meet the demand socio- economic factors such as environment analysis, safety measurement, climate management, agriculture modernization etc.

IOT Functional View-The Internet of Things concept refers to uniquely identifiable things with their virtual representations in an Internet-like structure and IoT solutions comprising a number of components such as

(1) Module for interaction with local IoT devices. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.

(2) Module for local analysis and processing of observations acquired by IoT devices.

(3) Module for interaction with remote IoT devices, directly over the Internet. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.

(4) Module for application specific data analysis and processing. This module is running on an application server serving all clients. It is taking requests from mobile and web clients and relevant IoT observations as input, executes appropriate data processing algorithms and generates output in terms of knowledge that is later presented to users.

(5) User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries. The Designs are shown below:

Physical Design of IOT-The Internet of Things will become part of the fabric of everyday life. It will become part of our overall infrastructure just like water, electricity, telephone, TV and most recently the Internet. Whereas the current Internet typically connects full-scale computers, the Internet of Things (as part of the Future Internet) will connect everyday objects with a strong integration into the physical world.

1. Plug and Play Integration

· If we look at IoT-related technology available today, there is a huge heterogeneity. It is typically deployed for very specific purposes and the configure requires significant technical knowledge and may be cumbersome. To achieve a true Internet of Things we need to move away from such small- scale, vertical application silos, towards a horizontal infrastructure on which a variety of applications can run simultaneously. This is only possible if connecting a thing to the Internet of Things becomes as simple as plugging it in and switching it on. Such plug and play functionality requires an infrastructure that supports it, starting from the networking level and going beyond it to the application level. This is closely related to the aspects discussed in the section on autonomy.

· On the networking level, the plug & play functionality has to enable the communication, features like the ones provided by IPv6 are in the directions to help in this process. Suitable infrastructure components have then to be discovered to enable the integration into the Internet of Things. This includes announcing the functionalities provided, such as what can be sensed or what can be actuated.

2. Infrastructure Functionality-The infrastructure needs to support applications in finding the things required. An application may run anywhere, including on the things themselves. Finding things is not limited to the start-up time of an application. Automatic adaptation is needed whenever relevant new things become available, things become unavailable or the status of things changes. The infrastructure has to support the monitoring of such changes and the adaptation that is required as a result of the changes.

3. Semantic Modeling of Things-To reach the full potential of the Internet of Things, semantic information regarding the things, the information they can provide or the actuations they can perform need to be available. It is not sufficient to know that there is a temperature sensor or an electric motor, but it is important to know which temperature the sensor measures: the indoor temperature of a room or the temperature of the fridge, and that the electric motor can open or close the blinds or move something to a different location. As it may not be possible to provide such semantic information by simply switching on the thing, the infrastructure should make adding it easy for users. Also, it may be possible to derive semantic information, given some basic information and additional knowledge, e.g. deriving information about a room, based on the information that a certain sensor is located in the room. This should be enabled by the infrastructure.

4. **Physical Location and Position-**As the Internet of Things is strongly rooted in the physical world, the notion of physical location and position are very important, especially for finding things, but also for

IOT applications-Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The IoT application covers smart environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy. Below are some of the IoT applications.

· **IOsL (Internet of smart living)-Remote Control Appliances:** Switching on and off remotely appliances to avoid accidents and save energy, Weather: Displays outdoor weather conditions such as humidity, temperature, pressure, wind speed and rain levels with ability to transmit data over long distances, "mart Home Appliances: Refrigerators with LCD screen telling what's inside, food that's about to expire, ingredients you need to buy and with all the information available on a Smartphone app. Washing machines allowing you to monitor the laundry remotely, and. Kitchen ranges with interface to a Smartphone app allowing remotely adjustable temperature control and monitoring the oven's self-cleaning feature, Safety Monitoring: cameras, and home alarm systems making people feel safe in their daily life at home, Intrusion Detection Systems: Detection of window and door openings and violations to prevent intruders, Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.

· **IOsC (Internet of smart cities)-Structural Health:**
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments, Lightning: intelligent and weather adaptive lighting in street lights, Safety: Digital video monitoring, fire control management, public announcement systems, Transportation: Smart Roads and Intelligent High-ways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams, Smart Parking: Real-time monitoring of parking spaces availability in the city making residents able to identify and reserve the closest available spaces, Waste Management: Detection of rubbish levels in containers to optimize the trash collection routes. Garbage cans and recycle bins with RFID tags allow the sanitation staff to see when garbage has been put out.

· **IOsE (Internet of smart environment)-**Air Pollution monitoring: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms, Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones, Weather monitoring: weather conditions monitoring such as humidity, temperature, pressure, wind speed and rain, Earthquake Early Detection, Water Quality: Study of water suitability in rivers and the sea for eligibility in drinkable use, River

Floods: Monitoring of water level variations in rivers, dams and reservoirs during rainy days, Protecting wildlife: Tracking collars utilizing GPS/GSM modules to locate and track wild animals and communicate their coordinates via SMS.

· **IOsI (Internet of smart industry)-**Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines, Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety, Monitoring of water, oil and gas levels in storage tanks and Cisterns, Maintenance and repair: Early predictions on equipment malfunctions and service maintenance can be automatically scheduled ahead of an actual part failure by installing sensors inside equipment to monitor and send reports.

· **IOsH (Internet of smart health)-Patients Surveillance:** Monitoring of conditions of patients inside hospitals and in old people's home, Medical Fridges: Control of conditions inside freezers storing vaccines, medicines and organic elements, Fall Detection: Assistance for elderly or disabled people living independent, Dental: Bluetooth connected toothbrush with Smartphone app analyzes the brushing uses and gives information on the brushing habits on the Smartphone for private information or for showing statistics to the dentist, Physical Activity Monitoring: Wireless sensors placed across the mattress sensing small motions, like breathing and heart rate and large motions caused by tossing and turning during sleep, providing data available through an app on the Smartphone.

· **IOsE (internet of smart energy)-Smart Grid:** Energy consumption monitoring and management, Wind Turbines/ Power house: Monitoring and analyzing the flow of energy from wind turbines & power house, and two-way communication with consumers' smart meters to analyze consumption

· **Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

· **Dynamic changes:** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

· **Enormous scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

· **Safety:** As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

· **Connectivity:** Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

IOT architectural view-IoT architecture consists of different layers of technologies supporting IoT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IoT deployments in different scenarios. The functionality of each layer is described below:

· **Smart device / sensor layer:** The lowest layer is made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. In some cases, they may also have a degree of memory, enabling them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telemetric sensors, etc

· **Gateways and Networks-**Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications. With demand needed to serve a wider range of IoT services and applications such as high speed transactional services, context- aware applications, etc, multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security. Various gateways (microcontroller, microprocessor) & gateway networks (WI-FI, GSM, GPRS).

· **Management Service Layer-**The management service renders the processing of information possible through analytics, security controls, process modeling and management of devices. One of the important features of the management service layer is the business and process rule engines. IoT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to post-processing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IoT system.

· **Application Layer-**The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy.

deriving knowledge. Therefore, the infrastructure has to support finding things according to location (e.g. geo-location based discovery). Taking mobility into account, localization technologies will play an important role for the Internet of Things and may become embedded into the infrastructure of the Internet of Things.

5. Security and Privacy-In addition, an infrastructure needs to provide support for security and privacy functions including identification, confidentiality, integrity, non-repudiation authentication and authorization. Here the heterogeneity and the need for interoperability among different ICT systems deployed in the infrastructure and the resource limitations of IoT devices (e.g., Nano sensors) have to be taken into account.

Logical design of IOT-

· The Logical design of IoT is however too abstract to be used for building directly concrete architectures. In order to implement a compliant IoT solutions, Reference Architectures must be defined, describing essential building blocks as well as design choices able to select specific constructs able to deal with converging requirements regarding functionality, performance, deployment and security, to name a few. Interfaces among different technological functional blocks should be standardized; best practices in terms of functionality and information usage need to be provided.

· Existing literature provides methodologies for dealing with system architectures (hereafter called Concrete Architectures) based on Views and Perspectives. The way that the IoT-A project illustrates the Reference Architecture (RA) is through a *matrix* that provides clear technological choices in order to develop concrete architectures. To establish the contents of this matrix we need to analyze all possible functionalities, mechanisms and protocols that can be used for building any concrete IoT-related architecture and to show how interconnections could take place between selected design and technological choices. A system architect should then have a tool to make a rational selection of protocols, functional components, and architectural options, needed to build specific IoT systems.

· The IoT-A project sees views as a representation of one or more structural aspects of an architecture that illustrates how the architecture addresses one or more concerns held by one or more of its stakeholders. Some typical examples for viewpoints are Functional, Information, Concurrency, Development, Deployment and Operational viewpoints. However, architectural decisions often address concerns that are common to more than one view. These concerns are often related to non-functional or quality properties.

· The approach that the project is following is to define special perspectives to address these aspects of a concrete architecture, emphasizing the importance of stakeholder requirements. Therefore we are define a perspective as a collection of activities, tactics, and guidelines that are used to ensure that a system exhibits a particular set of related quality properties that require consideration across a number of the system's architectural views, where a quality property is defined as an externally visible, non-functional property of a system such as performance, security, or scalability.

—

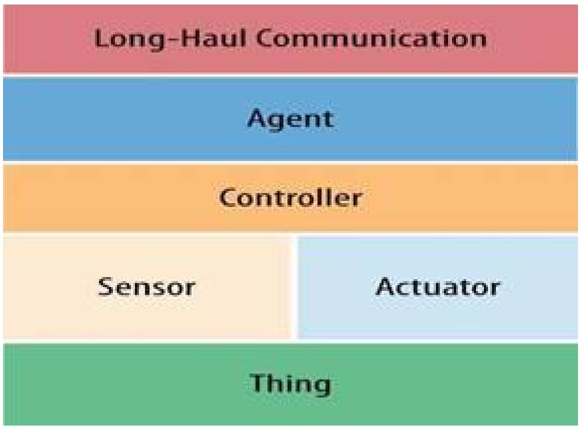

Fig. 1.4 IoT Logical View

patterns, Power Supply Controllers: Controller for AC-DC power supplies that determines required energy, and improve energy efficiency with less energy waste for power supplies related to computers, telecommunications, and consumer electronics applications, Photovoltaic Installations: Monitoring and optimization of performance in solar energy plants.

· **IOsA (internet of smart agriculture)-Green Houses:** Control micro-climate conditions to maximize the production of fruits and vegetables and its quality, Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants, Animal Farming/Tracking: Location and identification of animals grazing in open pastures or location in big stables, Study of ventilation and air quality in farms and detection of harmful gases from excrements, Offspring Care: Control of growing conditions of the offspring in animal farms to ensure its survival and health, field Monitoring: Reducing spoilage and crop waste with better monitoring, accurate ongoing data obtaining, and management of the agriculture fields, including better control of fertilizing, electricity and watering.

Physical View-It defines different layered level component required to create the device as mentioned in diagram.

—

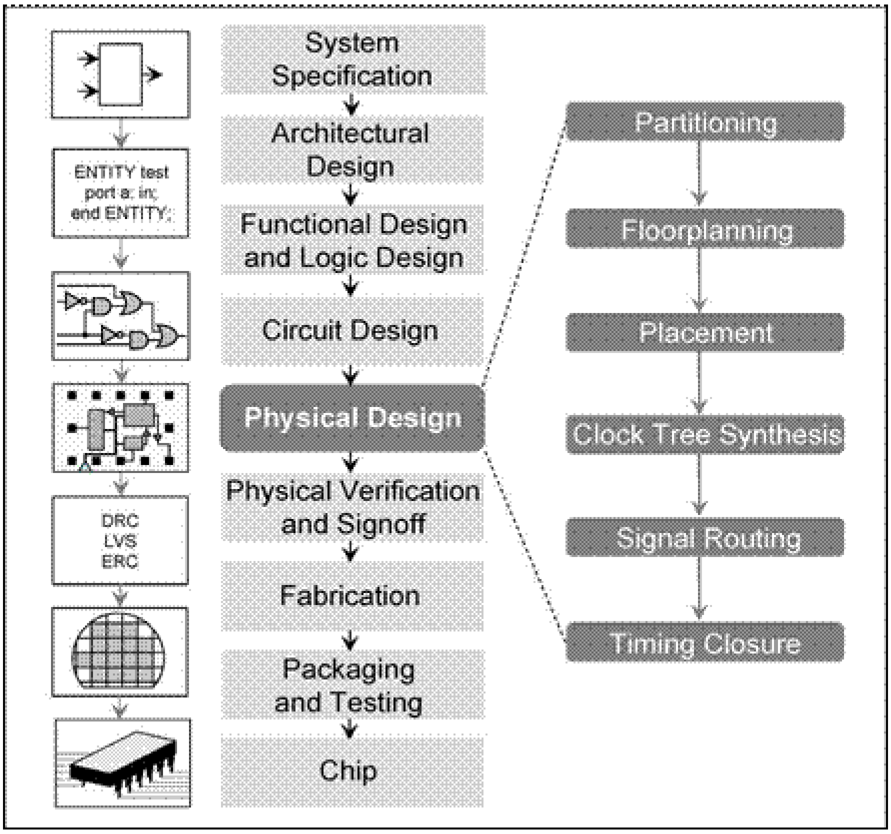

Fig. 1.5 Physical View