Internet of Things (IoT)

Picture: IoT

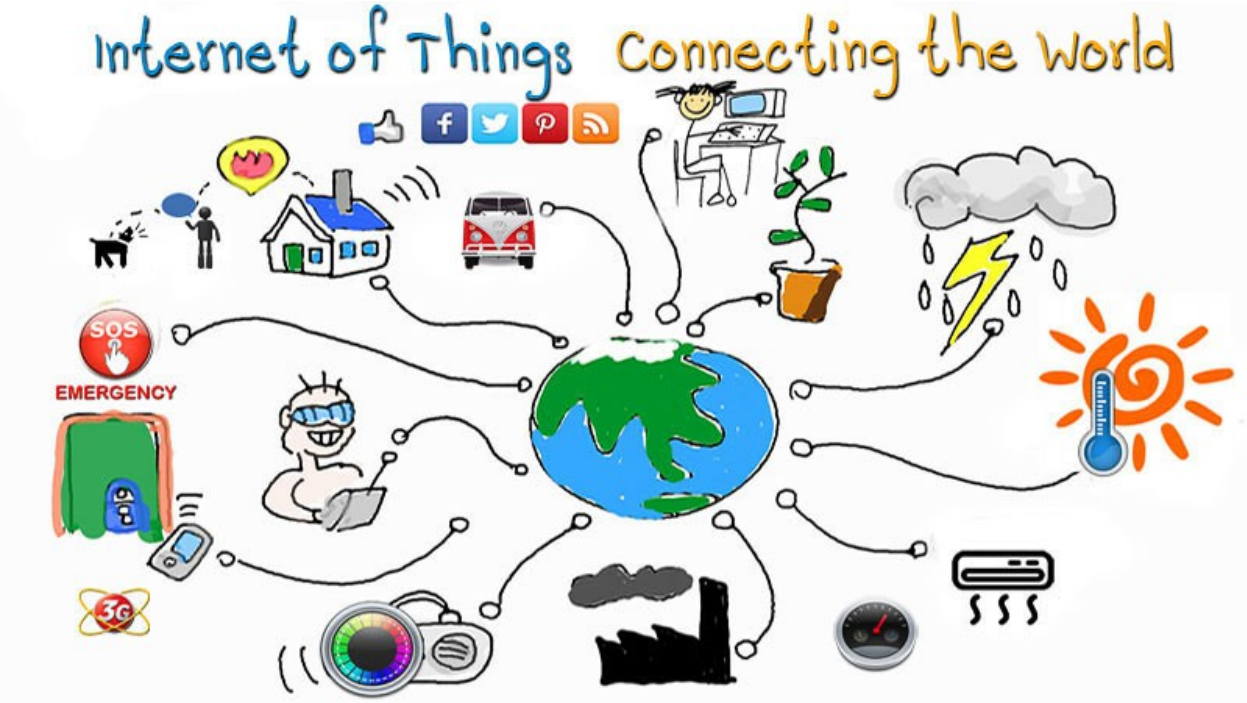
The report "Internet of Things Technology Market by Hardware (Processor, Sensor, Connectivity Technology), Device Management Platform, Application Management Platform, Network Management Platform Software Solutions, and Services, Application, and Geography - Forecast to 2022", published by Markets and Markets, The IOT technology market size, in terms of value, is expected to grow from USD 130.33 Billion in 2015 to USD 883.55 Billion by 2022, at a CAGR of 32.4% between 2016 and 2022.

Internet of Things (IoT)

Imagine Innovate Inspire

The increasing business demand for enhancing operation efficiency and cost-savings would make IoT a dominant model for organizations across verticals in the future.

The Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment.



Picture: IoT –Connecting the world

Internet of Things (IoT)

Imagine Innovate Inspire

A big part of the Internet of Things isn't so much about smart devices, but about sensors. Wireless Sensor Network (WSN) technologies mark across many areas of modern day living. These offer the ability to measure, and understand environmental indicators, from delicate ecologies and natural resources to urban environments.

Picture: Sensors

Internet of Things (IoT)

Imagine Innovate Inspire

Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet.

The Internet of Things demands:

1. A shared understanding of the situation of its users and their appliances,
2. Software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant, and
3. The analytics tools in the Internet of Things that aims for autonomous and smart behavior.

IoT elements:

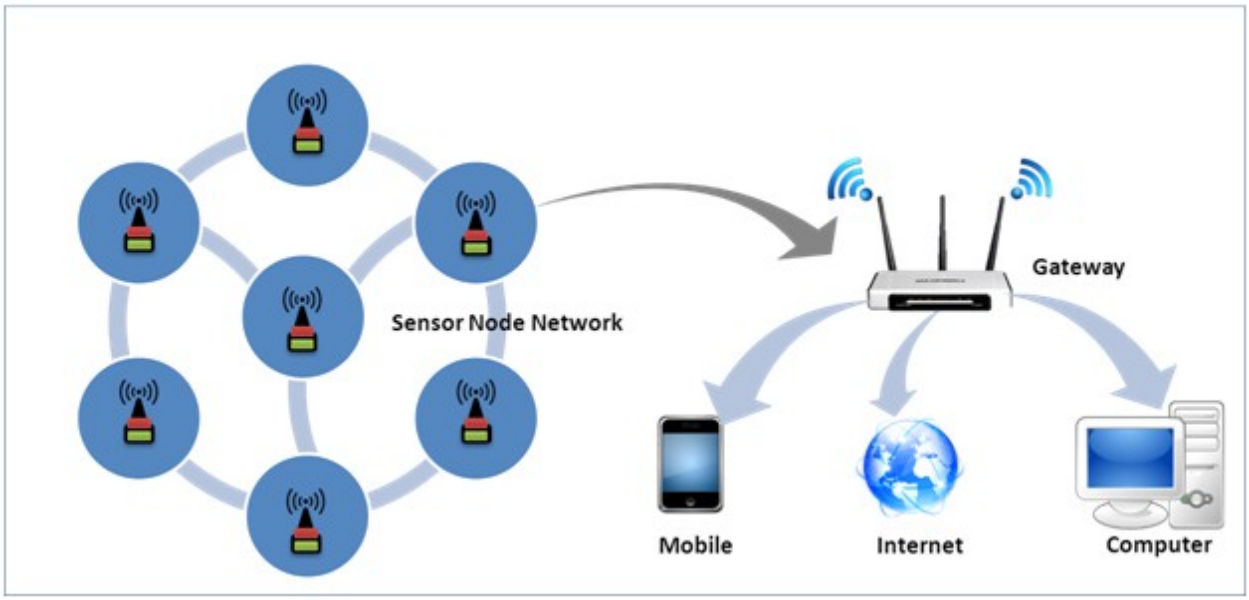
There are three IoT components:

- Hardware — made up of sensors, actuators and embedded communication hardware
- Middleware — on demand storage and computing tools for data analytics
- Presentation — to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

Sensors have always been an integral part of the factory setup for security, automation, climate control, etc. This will eventually be replaced by a wireless system giving the flexibility to make changes to the setup whenever required. This is nothing but an IoT subnet dedicated to factory maintenance.

Wireless Sensor Networks (WSN)

Recent technological advances in low power integrated circuits and wireless communications have made available efficient, low cost, low power miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments.



Picture: IoT –Analytics

Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics. The components that make up the WSN monitoring network include:

Hardware — Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. And more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.

Communication stack — The nodes are expected to be deployed in an ad-hoc manner for most applications. Designing an appropriate topology, routing and MAC layer is critical for the scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.

Middleware — A mechanism to combine cyber infrastructure with a Service Oriented Architecture and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner. This is based on the idea of isolating resources that can be used by several applications. A platform independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method.

Secure Data aggregation — An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors. Node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

Data storage and analytics:

One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. The internet consumes up to 5% of the total energy generated today and with these types of demands, it is sure to go up even further. Hence, data centers that run on harvested energy and are centralized will ensure energy efficiency as well as reliability.

The data have to be stored and used intelligently for smart monitoring and actuation. It is important to develop artificial intelligence algorithms which could be centralized or distributed based on the need. They also have a modular architecture both in terms of hardware system design as well as software development and are usually very well suited for IoT applications.

More importantly, a centralized infrastructure to support storage and analytics is required.

Applications

There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact. We categorize the applications into four application domains: (1) Personal and Home (2) Enterprise (3) Utilities and (4) Mobile.

Framework:

The new IoT application specific framework should be able to provide support for

- reading data streams either from sensors directly or fetch the data from databases
- easy expression of data analysis logic as functions/operators that process data streams in a transparent and scalable manner on Cloud infrastructures,
- If any events of interest are detected, outcomes should be passed to output streams, which are connected to a visualization program.

Using such a framework, the developer of IoT applications willable to harness the power of Cloud computing without knowing low level details of creating reliable and scale applications.

Future challenges:

The challenges include IoT specific challenges such as privacy, participatory sensing, data analytics, GIS based visualization and Cloud computing apart from the standard WSN challenges including architecture, energy efficiency, security, protocols, and Quality of Service.