Key IoT Technologies

List of Technologies are:

- **Device Intelligence**
- Communication Capabilities
- Mobility Support
- Device Power
- Sensor Technology
- RFID Technology
- Satellite Technology

Key IoT Technologies Device Intelligence
In order for the IoT to become a reality, Objects should be able to intelligently sense and interact with the environment Possibly store some passive or acquired data Communicate with the world around them Object-to-gateway device communication or even direct object-to-object communication is desirable

These intelligent capabilities are necessary to support ubiquitous networking to provide seamlessly interconnection between humans and objects Some have called this mode of communication Any Services, Any Time, Any Where, Any Devices, and Any Networks (also known as "5-Any")

Key IoT Technologies Communication Capabilities
It is highly desirable for objects to support ubiquitous end- to-end communications To achieve ubiquitous connectivity for human-to-object & object-to-object communications, networking capabilities will need to be implemented in the objects ("things")IP is considered to be key capability for IoT objects Self-configuring capabilities, especially how an IoT device can establish its connectivity automatically without human intervention, are also of interestIPv6 auto-configuration & multihoming features are useful, particularly scope-based IPv6 addressing features

Key IoT Technologies Mobility Support
Another consideration related to tracking and mobility support of mobile object Mobility-enabled architectures & protocols are required Some objects move independently, while others will move as one of group Therefore, according to the moving feature, different tracking methods are required. It is important to provide ubiquitous and seamless communication among objects while tracking the location of objects. Mobile IPv6 (MIPv6) offers several capabilities that can address this requirement.

Key IoT Technologies Device Power
Related to the powering of the "thing" Especially for mobile devices or devices that do not have intrinsic powerM2M/IoT applications are always constrained by following factors: Devices have ultra-low-power capabilities Devices must be of low cost Devices must have small physical size & light in weight

The following factors that must be considered in selecting the most suitable battery for a particular application :Operating voltage level Load current and profile Duty cycle—continuous or intermittent Service life Physical requirement Size Shape Weight Environmental conditions Temperature Pressure Humidity Vibration Shock Safety and reliability Shelf life Maintenance and replacement Environmental impact and recycling capability Cost

Key IoT Technologies Sensor Technology

A sensor network is an infrastructure comprising sensing (measuring), computing, communication, data collection, monitoring, surveillance, and medical telemetry. Sensor network technology, specifically, with embedded networked sensing, ships, aircrafts, and buildings can "self-detect" structural faults (e.g., fatigue-induced cracks).Earthquake-oriented sensors in buildings can locate potential survivors and can help assess structural damage; tsunami-alerting sensors can certainly prove useful for nations with extensive coastlines. Sensors also find extensive applicability in battlefield for reconnaissance and surveillance

There are four basic components in a sensor network:(i) an assembly of distributed or localized sensors(ii) an interconnecting network (usually, but not always, wireless based) (iii) a central point of information clustering(iv) a set of computing resources at the central point (or beyond) to handle data correlation, event-trending, querying, and data mining. Because the interconnecting network is generally wireless, these systems are known as wireless sensor networks (WSNs).WSN have the potentially large quantity of data collected, algorithmic methods for data management play an important role in sensor networks. In-network processing is desirable in sensor networks; furthermore, node power (and/or battery life) is a key design consideration.

Sensors can be described as "smart" inexpensive devices equipped with multiple on- board sensing elements: they are low cost, low power, untethered multifunctional nodes that are logically homed to a central sink node. Sensor utilize the Internet or some other network for long-haul delivery of information to a point (or points) of final data aggregation and analysis. Sensors are typically internetworked via a series of multi hop short-distance low power wireless links called "sensor field". Sensors are typically deployed in a high density manner and in large quantities: a WSN consists of densely distributed nodes that support sensing, signal processing, embedded computing, and connectivity; sensors are logically linked by self-organizing means (sensors that are deployed in short-hop point-to-point master-slave pair arrangements are also of interest).

New wireless design methodologies are needed across a set of disciplines, information transport, network and operational management, confidentiality, integrity, availability, and in-network/local processing, low battery status, other wireless sensor malfunction and lightweight protocol stack. Physical size can range from nanoscopic-scale devices to mesoscopic-scale devices at one end; from microscopic-scale devices to macroscopic-scale devices at the other end. Nanoscopic (nanoscale) in the order of 1–100 nm in diameter; Mesoscopic scale refers to objects between 100 and 10,000 nm in diameter The microscopic scale ranges from 10 to 1000 microns The macroscopic scale is at the millimeter-to-meter range. Biological sensors, small passive microsensors (such as "smart dust"), and "lab-on-a-chip" assemblies The miniaturized ones that are directly embedded in some physical infrastructure, as "microsensors."

Sensors may be passive and/or be self-powered; further along in the power consumption chain, some sensors may require relatively low power from a battery or high power. Low power consumption for transmission over low bandwidth channels and low power-consumption logic to pre-process and/or compress data. Power efficiency in WSNs is generally accomplished in three ways:(i) Low duty cycle operation(ii) Local/in-network processing to reduce data volume (and, hence, transmission time)(iii) Multihop networking (this reduces the requirement for long-range transmission since signal path loss is an inverse power with range/distance) each node in the sensor network can act as a repeater, thereby reducing the link range coverage required, and, in turn, the transmission power

Key IoT Technologies RFID Technology
RFIDs are electronic devices associated with objects ("things") that transmit their identity (usually a serial number) via radio links. RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. RFID and barcode facilitate the global supply chain and impact all subsystems within that overall process, including material requirement planning (MRP), just in time (JIT), electronic data interchange (EDI), and electronic commerce (EC).

Contactless smart cards (SCs) are more sophisticated than RFID tags RFID tags are typically less expensive than SCs. When an RFID tag or contactless SC passes within a defined range, a reader generates electromagnetic waves; the tag's integrated antenna receives the signal and activates the chip in the tag/SC, and a wireless communications channel is set up between the reader and the tag enabling the transfer of pertinent data.

There are a number of standards for RFIDs. Some of the key ones include the following: The ISO 14443operating frequency of MHz that embed a CPU; power consumption is about 10mW; data throughput is about 100 Kbps and the maximum working distance (from the reader) is around 10 cm. The ISO 15693operating at MHz frequency, but it enables working distances as high as 1 m, with a data throughput of a few Kbps. The ISO 18000with frequency such as 135 KHz, MHz, 2.45 GHz, 5.8 GHz, 860–960 MHz, and 433 MHz. The ISO 18000–6 standard uses the 860–960MHz range and is the basis for the Class-1 Generation-2 UHF RFID, introduced by the EPC global Consortium.

Typically, EPC codes used for active RFIDs or IP addresses are transmitted in clear form Provide strong privacy for the IoT. The host identity protocol (HIP) with this protocol, active RFIDs do not expose their identity in clear text, but protect the identity value (e.g., an EPC) using cryptographic procedures.

An RFID system is logically comprising several layers, as follows: the tag layer, the air interface (also called media interface) layer, the reader layer; Tag (device) layer: Architecture and EPC global Gen2 tag finite state machine Media interface layer: Frequency bands, antennas, read range, modulation, encoding, data rates Reader layer: Architecture, antenna configurations, Gen2 sessions, Gen2

Key IoT Technologies RFID Technology- standards in the EPC global environment
An interface is the UHF Class-1 Gen-2 tag air interface, which specifies a radio-frequency communications protocol by which an RFID tag and an RFID reader device may interact. A component is an RFID tag that is the product of a specific tag manufacturer. An EPC Network Service is the ONS,

which provides a logically centralized registry through which an EPC may be associated with information services.

Key IoT Technologies	**Satellite Technology**
Ability to support mobility in all geographical environments (including Antarctica)	Global reach Offers interesting commercial possibilities