Fundamental IoT Mechanisms and Key Technologies

1. Identification of IoT Objects and Services

- Sensors
- Actuators
- Gateways
- Embedded Systems
- Tags & Beacons
- Wearable Devices
- Smart Appliances
- Industrial Equipment

IOT Services

- Data Collection and Storage
- Data Processing and Analytics
- Device Management
- Security and Privacy
- Integration and Interoperability
- Visualization and User Interfaces

2. Structural aspects of the IoT

1. Physical Components
   - Sensors and Actuators
   - Embedded Systems
   - Gateways
   - Network Infrastructure
2. Architecture Layer
   - Perception Layer
   - Network Layer
   - Middleware Layer
   - Application Layer

3. Data Flow and Processing
    - Data Collection
    - Data Processing
    - Data Storage
4. Security and Privacy
    - Authentication and Authorization
    - Data Encryption
    - Access Control
    - Device Management
5. Interoperability and Standards
    - Protocols and Standards
    - APIs and Integration

2.1 Environmental Characteristics

1. Physical Environment
   - Temperature
   - Humidity
   - Dust & Particulate Matter
   - Vibration & Shock
   - Water & Moisture
   - Electromagnetic Interference
2. Operational Environment
   - Power Supply
   - Network Connectivity
   - Latency and Response Time
   - Scalability and Flexibility

Operational Environment

3. Contextual Environment
    - Location and Geography
    - Regulatory Compliance
    - Cultural and Social Factors
    - Economic Considerations

2.2 Traffic Characteristics

1. Data Volume and Velocity
   - Large-Scale Data
   - Real-Time Data
   - Bursty Traffic
2. Traffic Patterns and Flows
   - Machine-to-Machine (M2M) Communication

     periodic reporting, event-triggered updates, or request-response interactions
   - Asymmetric Traffic
   - Multicast and Broadcast Traffic
3. Quality of Service (QoS) Requirements
   - Reliability
   - Low Latency
   - Scalability
4. Communication Protocols and Technologies
   - IoT Protocols (MQTT, CoAP, AMQP, HTTP, and WebSocket)
   - Wireless Technologies (Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, and LTE-M)

2.3 Scalability

1. Device Scalability
2. Network Scalability
3. Data Scalability
4. Application Scalability
5. Management Scalability
6. Security and Privacy Scalability

2.4 Interoperability

1. Diverse Ecosystem
2. Integration and Compatibility
3. Scalability and Flexibility
4. Improved User Experience
5. Data Sharing and Collaboration
6. Ecosystem Growth and Innovation

2.5 Security and Privacy

1. Data Encryption
2. Authentication and Access Control
3. Device Security
4. Network Security
5. Data Privacy
6. Security Updates and Patch Management
7. Security Monitoring and Incident Response
8. Regulatory Compliance

2.6 Open Architecture

The goal is to support a wide range of applications using a common infrastructure, preferably based on a service-oriented architecture (SOA) over an open service platform, and utilizing overly networks (these being logical networks defined on top of a physical infrastructure).

In an SOA environment, objects expose their functionalities using a protocol such as SOAP or REST application programming interface (API).

These devices may provide their functionality as a WS that can in turn be used by other entities (other devices or other business applications).

3. Key IoT Technologies

3.1 Device Intelligence

- the objects should be able to intelligently sense and interact with the environment
- possibly store some passive or acquired data
- and 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 the 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”)

3.2 Communication Capabilities

- To achieve ubiquitous connectivity human-to-object and object-to-object communications, networking capabilities will need to be implemented in the objects (“things”)
- In particular, IP is considered to be key capability for IoT objects
- IPv6 auto-configuration and multihoming features are useful
- using simple sensors and/or where is there a very large number of dispersed sensors and/or where there is limited remote energizing power, may have a need to support leaner protocols both at the network layer (e.g., route and/or topology management) and at the transport layer (e.g., using UDP)
- minimize energy consumption is a desired
- Hence, there is a need to support heterogeneous (IP and non-IP) networking interfaces, at least in the short term

3.3 Mobility Support

- Some objects move independently, while others will move as one of group
- according to the moving feature, different tracking methods are required
- Mobile IPv6 (MIPv6) offers several capabilities that can address this requirement

3.4 Device Power

- A key consideration relates to the powering of the “thing,” especially for mobile devices or for devices that otherwise would not have intrinsic power
- A number of devices operate with a small battery, while other devices use a self-energizing energy source, for example a small solar cell array
- The so-called “coin batteries,” also known as “button batteries,” are typical in many IoT applications.
- There are a number of 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
  - Pressure
- Safety and reliability
- Shelf life
- Maintenance and replacement
- Environmental impact and recycling capability
- Cost

3.5 Sensor Technology

- A sensor network is an infrastructure comprising sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment
- 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 and

  (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).

- 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.
- 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 line feed.
- At the high end of the power-consumption chain, some sensors may require very high power feeds (e.g., for radars).
- Chemical-, physical-, acoustic-, and image-based sensors can be utilized to study ecosystems (e.g., in support of global parameters such as temperature, microorganism populations, and so on).
-

3.6 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
- Contactless smart cards (SCs) are more sophisticated than RFID tags, being that they contain a microprocessor that enables

  (i) on-board computing

  (ii) two-way communication including encryption, and

  (iii) storage of predefined and newly acquired information

-

- An RFID system is logically comprising several layers, as follows:
  - the tag layer
  - the air interface (also called media interface) layer, and
  - the reader layer

additionally there are network, middleware, and application aspects

3.7 Satellite Technology

- Due to its global reach and the ability to support mobility in all geographical environments (including Antarctica), satellite communications can play a critical role in many broadly distributed M2M applications