Internet of Everything (IoE)

IoT

Def:

The Internet of Things (IoT) is a network of ‘smart’ devices that connect and communicate via the Internet.

How does the IoT work?

Smart devices collect and exchange information machine to machine (M2M) and with us.

- Remote control and monitoring
- Operate automatically through software, cameras and sensors

What sectors use the IoT?

1. Manufacturing 2. Transportation 3. Retail 4.Science and Technology
5. IT and Communications 6. Education 7. Healthcare 8. Energy
9. Construction 10. Agriculture

IoT business developments:

1. **Retail**
   - Automated checkout
   - Inventory and warehouse management

2. **Manufacturing**
   - Operations efficiencies
   - Asset management and maintenance

3. **Consumers**
   - Entertainment
   - Health and fitness

4. **Offices and Government**
   - Productivity and energy saving
   - Security and surveillance

5. **Transportation**
   - Automation and traffic control
   - Fleet management

6. **Healthcare**
   - Monitoring
   - Automated administration of treatment

Risks to Information Security:

1. **Possible consequences of an information breach:**
   - Loss of reputation/credibility
   - Loss of revenue and time
   - Lead to legal challenges

2. **Direct cyber incidents:**
   - Remote control and monitoring
   - From head office, to supply chain, to customers

3. **Indirect cyber incidents (viral threats, malware):**
   - Downstream effects on IT security infrastructure
   - A malware attack on the IoT device manufacturer could affect your IoT devices

Risks to Privacy:

1. **Business, employee, and client information could be:**
   - Destroyed
   - Altered
   - Stolen and exposed
   - Held for ransom

2. **Understand IoT device data collection policies:**
   - What information is gathered?
   - How long is data kept?
   - What is your data used for (marketing research, etc.)?

Risks to Safety:

1. **IoT device malfunction or manipulation could cause:**
   - Physical damage to data
   - Physical damage to equipment
   - Physical harm

2. **Possible consequences of IoT device malfunction or manipulation:**
   - Costly repairs to systems, assets, and equipment
   - Legal impact of harm to staff, customers or public
   - Loss of reputation

Before implementation:

- ❑ Research devices before you purchase. Read reviews and get recommendations; research their security capabilities.
- ❑ Have a point of contact with the manufacturers for any issues down the road.
- ❑ Read device materials: operator’s manuals, instructions, support forums.
- ❑ Create a Bring Your Own Device (BYOD) and IoT policies for employees.
- ❑ Assess against your existing IT security policies and standards.

During implementation:

- ❑ Secure your wireless network.
- ❑ Change device default usernames and passwords, and use strong passwords.
- ❑ Keep networks with sensitive information isolated. Consider using separate networks for IoT devices.
- ❑ Ensure the device has system reset capability in order to permanently eliminate sensitive configuration information.
- ❑ Control who can access your network and from where.
- ❑ Encrypt data, commands and communications, both at rest and in transit.

- ❑ Where possible, set operating system, software, and firmware to update automatically. Establish periodic manual updates as required.

After implementation:

- ❑ Implement a repeatable process to validate all safeguard and countermeasures in your implementation.
- ❑ Conduct ‘cyber incident’ tests and audits regularly to ensure the integrity of your network.
- ❑ Backup data regularly using secure and redundant storage solutions, such as multiple storage units and/or the cloud. Test your recovery process regularly.

Adhere to your company’s Bring Your Own Device/ IoT policy

- ❑ Understand what information is being collected by devices and why, before you download or buy.
- ❑ Use a lock screen password, use strong passwords.
- ❑ Backup data regularly on multiple storage units and the cloud.
- ❑ Connect only to secure Wi-Fi networks.
- ❑ Use safe websites, cloud storage, etc.

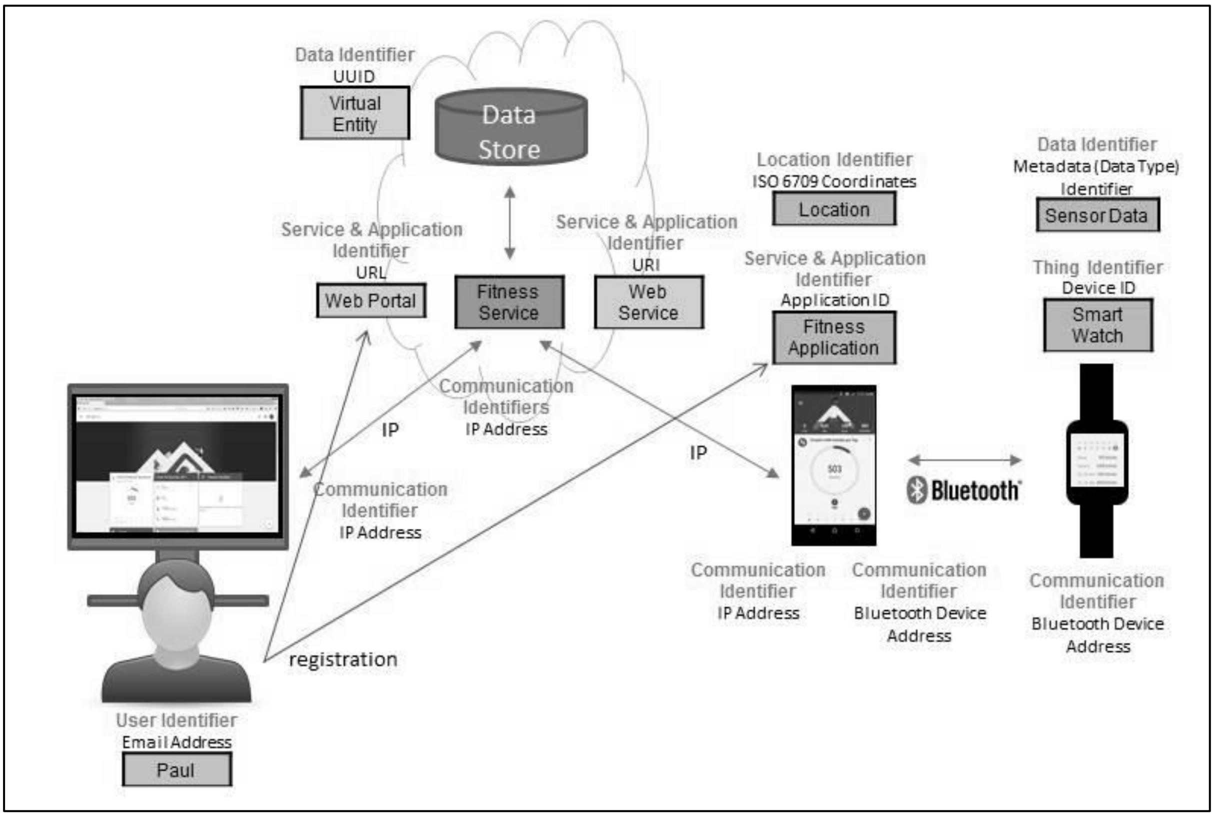
Identifier in the IoT

- **Identifier:** It is a pattern to uniquely identify a single entity or a class of entities within a specific context. That can be inherent patterns of the thing itself like finger prints and facial structures or patterns added by technical means like printed serial numbers, bar codes or Radio Frequency Identification (RFIDs) tags.

  Within IoT Systems identifiers are used for different purposes that go beyond just the identification of things and users.

  For the design, but also for the use of IoT solutions, it is important to know the various usages of identifiers, the related requirements, interoperability, security and privacy issues and which standards are available for them.

  Due to the below mentioned diversity of identifier and use cases the Alliance for Internet of Things Innovation (AIOTI) working group on IoT Standardization (WG03) decided a year ago to perform a thorough analysis of identification needs in IoT and related standardization.



IoT identifiers – what are we naming?

1. Physical device
   a. Changes if new board or repair replacement
   b. MAC address
2. Logical device
   a. may move, but same owner until sold
   b. "the heart rate monitor worn by X"
   c. cf. mobile phone number
3. Functional device

    a. identified by logical function
    b. location, service, …

IoT identifiers – requirements:

1. Clear semantics
    a. invariants (location? device hardware? owner? role?)
    b. suitable for program logic
    c. one or “anycast”?
2. Securable
    a. entity needs to be able to prove its identity (via X.509 cert)
    b. get certificates for identifiers
    c. automated assignment (see IETF ACME protocol)
3. Clear reachability
    a. local network only or from anywhere on the Internet?
4. Low-infrastructure
    a. federated; avoid single global directory
    b. enable local queries without server setup (multicast query)
5. Simplicity
    a. low conceptual overhead for programmers (e.g., not become an RDF or SPARQL expert)

Communication identifiers:

Property	URL owned	URL provider	E.164	Service-specific
Example	alice@smith.name sip:alice@smith.name	alice@gmail.com sip:alice@ilec.com	+1 202 555 1010	www.facebook.com/alice.example
Protocol-independent	no	no	yes	yes
Multimedia	yes	yes	maybe (VRS)	maybe
Portable	yes	no	somewhat	no
Groups	yes	yes	bridge number	not generally
Trademark issues	yes	unlikely	unlikely	possible
Privacy	Depends on name chosen (pseudonym)	Depends on naming scheme	mostly	Depends on provider “real name” policy

Technologies in IOT

1. IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct.
2. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

NFC and RFID

- RFID (radio-frequency identification) and NFC (near-field communication) provide simple, low-energy, and versatile options for identity and access tokens, connection bootstrapping, and payments.
- RFID technology employs 2-way radio transmitter-receivers to identify and track tags associated with objects.
- NFC consists of communication protocols for electronic devices, typically a mobile device and a standard device.

Low-Energy Bluetooth

- This technology supports the low-power, long-use need of IoT function while exploiting a standard technology with native support across systems.

Low-Energy Wireless

- This technology replaces the most power-hungry aspect of an IoT system. Though sensors and other elements can power down over long periods, communication links (i.e., wireless) must remain in listening mode. Low-energy wireless not only reduces consumption, but also extends the life of the device through less use.

Radio Protocols

- ZigBee, Z-Wave, and Thread are radio protocols for creating low-rate private area networks. These technologies are low-power, but offer high throughput unlike many similar options. This increases the power of small local device networks without the typical costs.

LTE-A

- LTE-A, or LTE Advanced, delivers an important upgrade to LTE technology by increasing not only its coverage, but also reducing its latency and raising its throughput. It gives IoT a tremendous power through expanding its range, with its most significant applications being vehicle, UAV, and similar communication.

Wi-Fi-Direct

- Wi-Fi-Direct eliminates the need for an access point. It allows P2P (peer-to-peer) connections with the speed of Wi-Fi, but with lower latency. Wi-Fi-Direct eliminates an element of a network that often bogs it down, and it does not compromise on speed or throughput.