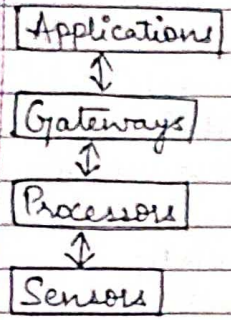
Dr. Rahul Bhandari
Dept. of CSE

Chapter 2
IoT Application for Industry

- Value Creation and challenges
- IoT Today
- IoT as a Network of Networks
- Why IoT important
- IoT : Critical for human progression
- Challenges and barriers to IoT

Basic Block Diagram of IoT



1) Sensors : These form the front end of IoT devices. These are so called "Things" of the system. The main purpose is to collect data from its surrounding (sensors).
These have to be uniquely identifiable devices with a unique IP address so that they can be easily identifiable over a large network
eg:- gas sensor, water quality sensor, moisture sensor etc.

2) Processors :
Processors are the brain of IoT system. Their main function is to process the data captured by the sensors and process them so as to extract the valuable data from enormous data i.e raw data collected

Dr. Rahul Bhandari
Dept. of CSE

Processors mostly work on real-time basis and can be easily controlled by applications. These are also responsible for securing data - that is performing encryption and decryption of data.
Embedded hardware devices, microcontroller, etc are the ones that process the data because they have processors attached to it.

3) Gateways :

Gateways are responsible for routing protocols the processed data and send it to proper locations for its proper utilization.

It helps in to and fro communication of the data. It provides network connectivity to the data. Network connectivity is essential for any IoT system to communicate.
eg:- LAN, WAN, PAN etc are examples of network gateways.

4) Applications
Applications form another end of the IoT system. Applications are essential for proper utilization of all the data collected.
These cloud-based applications which are responsible for rendering the effective meaning to the data collected. Applications are controlled by users and are a delivery point of particular services.
eg :- home automation apps, industrial controlling hub etc.

Components of IoT eco-system

There are 7 components of ~~eco~~ IoT eco-system

1. IoT devices
2. Network
3. Security
4. Gateway
5. The cloud
6. Application
7. Users.

(1) IoT devices (Sensors, actuators)

Sensors capture electric pulse or primary analogue data sources. They can measure temperature, humdity, light, motion etc.

Sensors detect, and actuators act. Actuators will operate in the reverse direction when trigged by application, they take action. Electric motor, valves etc. are actuators

(2) Network

The network could be Wi-Fi, it could be bluetooth, and the network could be cellular.
This devices connects with network for communication.

(3) Security

Security is a broad concept that needs to be adapted to the usecase.

The general security principles established in IoT and the acronyms used as PKI, public-key cryptography, encryption, mutual authentication, and certificates.

(4) Gateway -

Gateway is used to decide routing the ~~data~~ processed data and send it into proper locations. It provides network connectivity to the data. The network could be Wi-Fi, the network could be cellular. and it could be a lot of technologies.

(5) The cloud -

The data generated by sensors, and these data is send it into network with security and processed through a gateway. That data stored into cloud to for computing. The main advantages of cloud is that it is easily scalable. It is an essential requirement for building an effective IoT system.

(6) Application

When software development companies build software products for IoT ecosystem. An application is where users can interact with internet of things ecosystem. This interact is only made possible by graphical user Interface, where the users can analyses reports, control the system and manage devices.

(7) Users

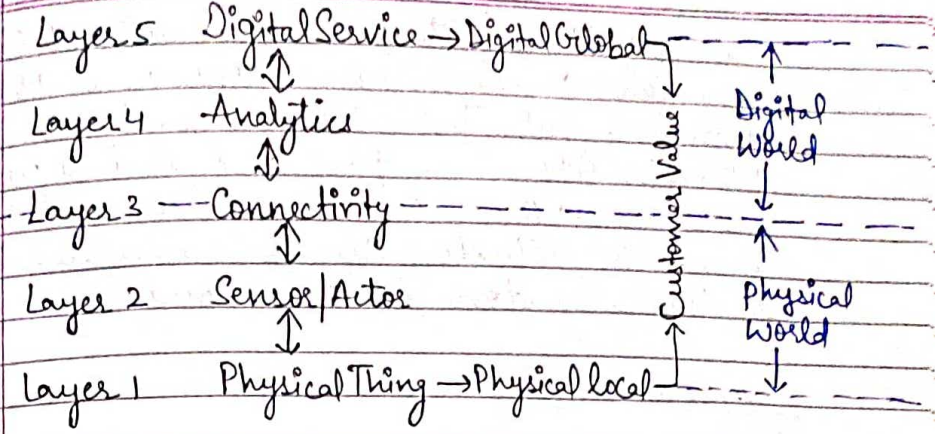
Users are the most important components among the seven components of IoT ecosystem. They use an IoT ecosystem for their needs.

Value Creation for IoT System

Value creation means producing product or provisioning of a platform or service. for eg:- Using ~~RFID~~ RFIDs in tracking service for goods. Value creation means creation of a 'smart tracking & logistics service' from ~~sensor~~ sensed IDs of the RFIDs communication on Internet, data analytics, data ~~visualo~~ visualizations and mobile communication for provisions for SMS to receives and delivery confirmation to the sender.

There are five ~~layers~~ value-creation layers for an IoT application.

1. Physical Thing
2. Sensor/Actor
3. Connectivity
4. Analytics
5. Digital Service



Layer 1 - Physical Thing

The physical component of an application is the value creation layer. On this layer the first tangible benefit is revealed to the user.

Layer 2 - Sensor/Actor

On layer 2, the physical thing is enhanced with a microprocessor, sensors and actuators, allowing local data to be captured and local actions to be performed. The benefit for the user can thus be significantly increased in relation to layer 1, but is still limited to immediate environment.

Layer 3 - Connectivity

This layer gives lower levels access to the Internet. This enable global access to the sensors and actors.

Layer 4 - Analytics

Connectivity on its own does not yet create any value. From layer 4 upwards the sensor data are collected, stored, check for plausibility, classified and linked with data from other online services and the value for actuators can be calculated. This is typically done in the cloud.

Layer 5 – Digital Service

On this layer, digital services are created that can be provided globally in the form of a smartphone application or a web service. They combine the possibilities and functions provided by layer 1 to 4 and are thus inseparably linked to data generating, smart, connected products. The characteristics of a digital bussiness models apply to these digital services.

The bidirectional arrows in the 5 value-creation layers indicate that individual layers cannot be created ~~depend~~ independently of each other. With high quality IoT application, the integration extends down to the level of the physical components and thus represents more than a mere addition of individual layers.

Dr. Rahul Bhandari
Dept. of CSE

Challenges in IoT

There are various types of challenges in front of IoT —

1. Security challenges in IoT
2. Design challenge in IoT
3. Deployment challenge in IoT

1. Security challenges in IoT

- Lack of encryption : Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security challenges.

- Insufficient testing and updating : With the increasing in the number of IoT devices, IoT manufacturers are more eager to produce and deliver their device as fast as they can without giving security too much of. although.
Most of these devices and IoT products do not get enough testing and updates and are prone to hackers and other security issues.

- Brute forcing and the risk of default passwords: Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute force.

- IoT Malware and Ransomware:
Increases with increase in devices.
Ransomware uses encryption to effectively lock out users from various devices & platforms and still use a user's valuable data and information.

- IoT botnet aiming at cryptocurrency
IoT botnet workers can manipulate data & privacy, which could be massive risk for an open crypto market. The exact value and creation of cryptocurrencies code face danger from mal-intentioned hackers.

- ~~Ind~~
- Inadequate device security:
It refers to the lack of proper measure to protect electronic devices such as computers, smartphones, and IoT devices from cyber attacks, hacking, data theft and unauthorized access. This can happen due to outdated software, weak passwords, unpatched vulnerabilities, lack of encryption, and other security risk.

- Lack of Standardization
It refers to the absence of agreed upon specifications or protocols in a particular field ~~industry~~ or industry. ~~This happen due to outdated software~~ This can result in different systems, products, or processes being incompatible with each other, leading to confusion, inefficiency, and decreased interoperability.

- Vulnerability to network attacks:
Vulnerability to network attacks refers to the susceptibility of a network, system or device to being compromised or exploited by cyber criminals. This can happen due to weakness in the network infrastructure, unpatch software, poor password management or a lack of appropriate security measures.

- Unsecured data transmission:
It refers to the transfer of data over a network or the internet without adequate protection. It can occur when data is transmitted over an unencrypted network connection or when data is transmitted over an unencrypted network connection or when insecure protocols are used. IoT devices often transmit sensitive data, which may be vulnerable to ~~er~~ eavesdropping or tampering if not properly secured.

- Privacy concerns:
It refers to issues related to the collection, storage, use, and sharing of personal information. The vast amount of data generated by IoT devices raises privacy concerns, as personal information could be collected & used without concerned.

- Software vulnerabilities:
IoT devices often have software vulnerabilities, which can be exploited by attackers to gain access to devices and networks.

- Insider Threats:
Employees or contractors with access to IoT systems can pose a security risk if they intentionally or unintentionally cause harm.

(2) Design Challenges in IoT
Some of the key design challenges in IoT.

- Interoperability:
It is important for enabling the full potential of the IoT and allowing connected devices to work together effectively and efficiently. Ensuring that different IoT devices can work together seamlessly and exchange data effectively.

- Security:
It is a critical concern in IoT as it involves the protection of sensitive data & systems from unauthorized access, theft or damage.

- Scalability:
In the context of IoT, scalability is a major challenge as the number of connected devices is rapidly growing, leading to an increased volume of data and communication. Scalability challenges in IOT include data management, Network capacity, device management.

- Reliability:
In the context of IOT, reliability is a critical concern, as the failure of even a single IoT device can have significant consequences. Some of the reliability challenges in IoT include device failure, network connectivity and data accuracy.

- Power Consumption
Many IoT devices are designed to be small, low-power, and operate using batteries. Some of the power consumption challenges include battery life, energy efficiency, power management

- Privacy
An IoT devices collect, store and transmit large amount of personal and sensitive information. Some of the privacy challenges in IoT include data collection, data storage, Data sharing,

- Increased cost & time to market.
Designers also need to solve the design time problem & bring the embedded device at the right time to the market.

(3) Deployment challenges in IoT

The deployment of IoT systems can present several challenges include -

- Connectivity
Connected devices that provide useful front and information are extremely valuable. But poor connectivity become a challenge where IoT sensors are required to monitor process data and supply information.

- Cross platform capability
IoT applications must be developed, keeping in the mind the technological changes of the future. Its development requires a balance of hardware & software functions. It is a challenge for IoT application developers to ensure that the device and IoT platforms drivers the best performance despite heavy device rates and fixings.

- Data collection and processing
Along with security and privacy, development teams need to ensure that they plan well for the way data is collected, stored or processed within an environment.

- Lack of skillset -
All of the development challenges can only be handled if there is a proper skilled resource working on IoT application development

- Integration
Ensuring that IoT device and systems integrate seamlessly with existing technology & infrastructure.

- Network infrastructure
Building & maintaining the network infrastructure needed to support the large number of connected IoT device.

- Device Management
Efficiently managing and maintaining the large no. of IoT devices in a deployment

- Data Management
Managing and analyzing the large amounts of data generated by IoT devices and integrating it with existing data systems.

Dr. Rahul Bhandari
Dept. of CSE

M. STATIONERS
Date
Page

- Security
  Ensuring that IoT application deployment is secure from threats such as cyber attacks, data breaches, and unauthorized ~~device~~ access.

- Cost
  Balancing the cost of deploying & maintaining an IoT system with benefits it delivers.