SNS COLLEGE OF TECHNOLOGY

Coimbatore-35.
An Autonomous Institution

COURSE NAME : Internet of Things

III YEAR/ V SEMESTER

UNIT – II Fundamental Mechanism and Key Technologies

Topic: *Key IoT Technology*

Dr.K.Sangeetha
HoD
Department of Computer Science and Engineering

Key IoT Technologies

i) **Device Intelligence**

Any Services,Any Time, Any Where, Any Devices, and Any Networks (also known as "5-Any")

Pervasive computing (also known as ubiquitous computing)

ii) Communication Capabilities

ubiquitous connectivity human-to-object and 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;

IPv6 auto-configuration and multihoming features

iii) Mobility Support

Mobility-enabled architectures and 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.

Key IoT Technologies

Mobile IPv6 (MIPv6) offers several capabilities that can address this requirement

iv) Device Power

M2M/IoT applications are almost invariably constrained by the following factors:
devices have ultra-low-power capabilities,
devices must be of low cost, and
devices generally must have small physical size and be light.
efficient communication mechanisms are needed.

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

Key IoT Technologies

iv) **Sensor Technology**

- **S**ensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment.

- Sensors facilitate theinstrumenting and controlling of factories, offices, homes, vehicles, cities, and the ambiance, especially as commercial off-the-shelf technology becomes available

- Sensor network technology, specifically, with embedded networked sensing, ships, aircrafts, and buildings can “self-detect” structural faults

- 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.

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, wirelessbased);
(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)**.

v) **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 tags have broad applications, including the rapid collection of data in commercial environments

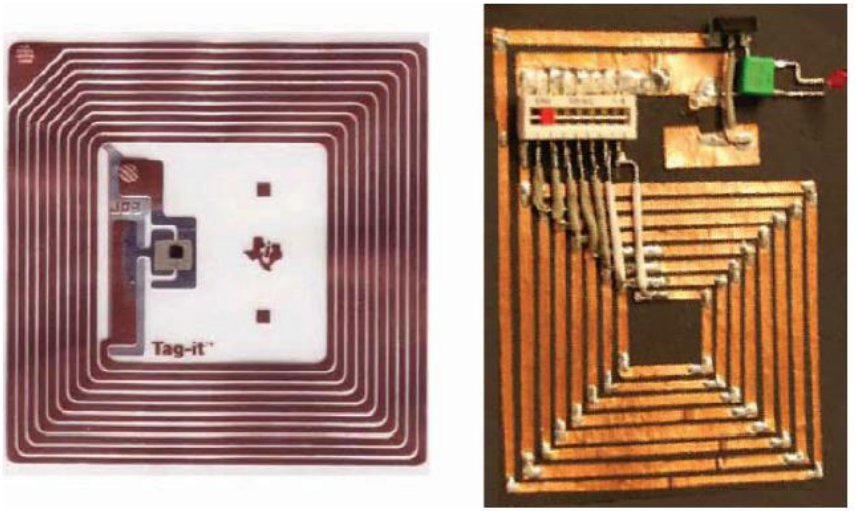


FIGURE 4.1 Illustrative examples of RFIDs.

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

(i) on-board computing,

(ii) (ii) two-waycommunication including encryption, and

(iii) (iii) storage of predefined and newly acquired information

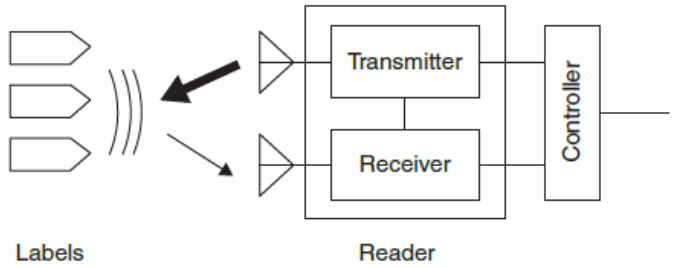


FIGURE 4.2 RFID reader operation.

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.

RFID examples applicable to IoT include but are not limited to the following:

- Warehouse retailer automotive
- Grocery chain transportation
- Distribution center asset management
- Manufacturing
- Inventory management
- Warehousing and distribution
- Shop floor (production)
- Document tracking and asset management
- Industrial applications (e.g., time and attendance, shipping document tracking,
- receiving fixed assets)
- Retail applications

Overview: what happens in RF (radio frequency) communication

1. When a contactless smart card or an RFID tag passes within range, a reader sends out radio frequency electromagnetic waves.
2. The antenna, tuned to receive these waves, wakes up the chip in the smart card or tag.
3. A wireless communications channel is set up between the reader and the smart card or tag.

The contactless smart card contains a microprocessor, a small but real computer that makes calculations, communicates both ways, remembers new information, and actively uses these capabilities for security and many other applications.

Characteristics of a contactless card

- Strong security capacities:
  - mutual authentication before providing access to information
  - access can be further protected via PIN or biometric
  - encryption to protect data on card during exchange
  - hardware and software protection to combat attacks or counterfeiting
- Hundreds of security features mean an individual's personal ID, financial details, payment transactions, transit fares or physical access privileges can be safely stored, managed, and exchanged
- Read and write memory capacity of 512 bytes and up, with very large memory storage possible
- Short-distance data exchange, typically two inches

RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. It is more like a radio-based bar code used mostly for identification (hence "radio frequency identification").

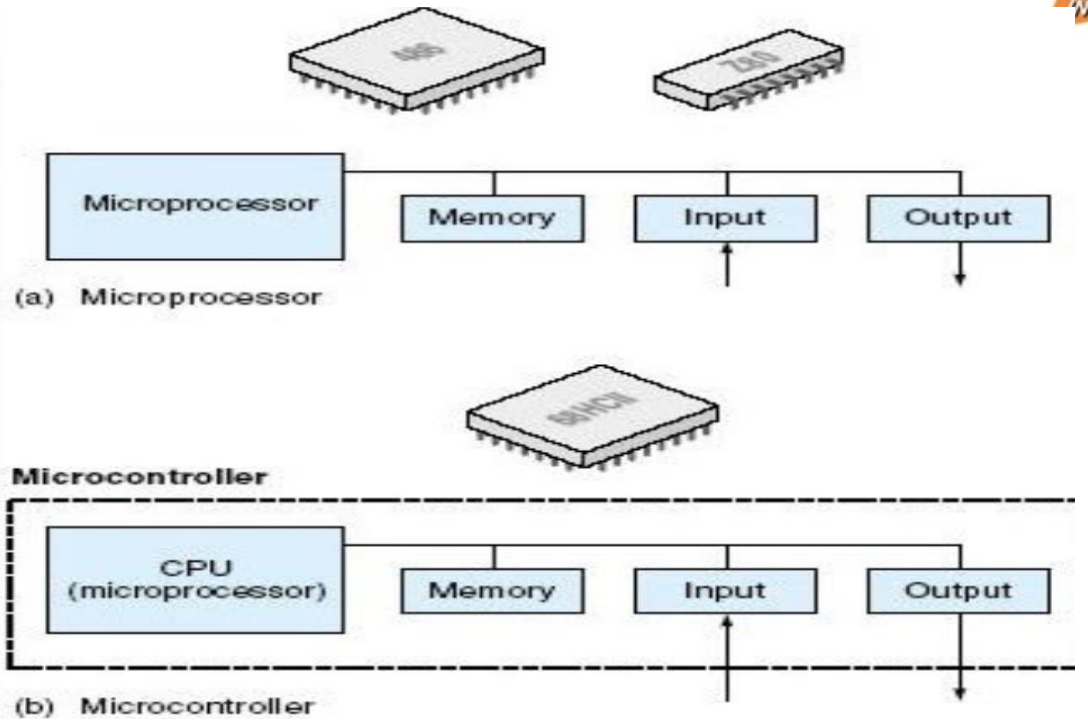
Characteristics of an RFID tag

- Minimal security:
  - one-way authentication; card cannot protect itself
  - insufficient storage for biometrics
  - no on-chip calculations of new information
  - relies on static keys
- Single function; used to help machines identify objects to increase efficiency. Example: inventory control
- Small memory (92 bytes); often read-only
- Larger distance data exchange, typically several yards

Because of their more restricted capabilities, RFID tags are generally cheaper.

Factors to Know

Microprocessor VS Microcontroller



MICROCONTROLLER

MICROPROCESSOR

A Microcontroller board is considered a small computer built on a metal oxide semiconductor circuit chip. All types of microcontrollers consist of the same main building parts:

central processing unit (CPU),

memory, and input/output (I/O) peripherals (programmable).

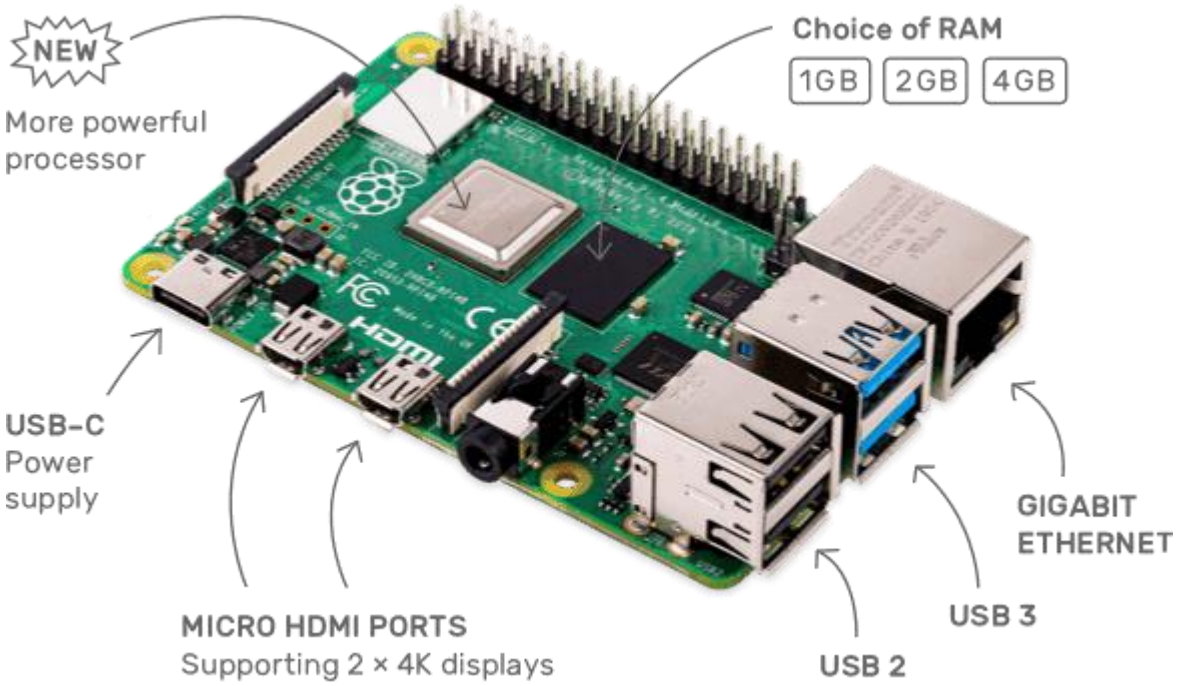
microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, implantable medical devices, remote controls, office machines, appliances, power tools, toys, and other embedded systems.

1 Arduino Uno R3 Microcontroller Board

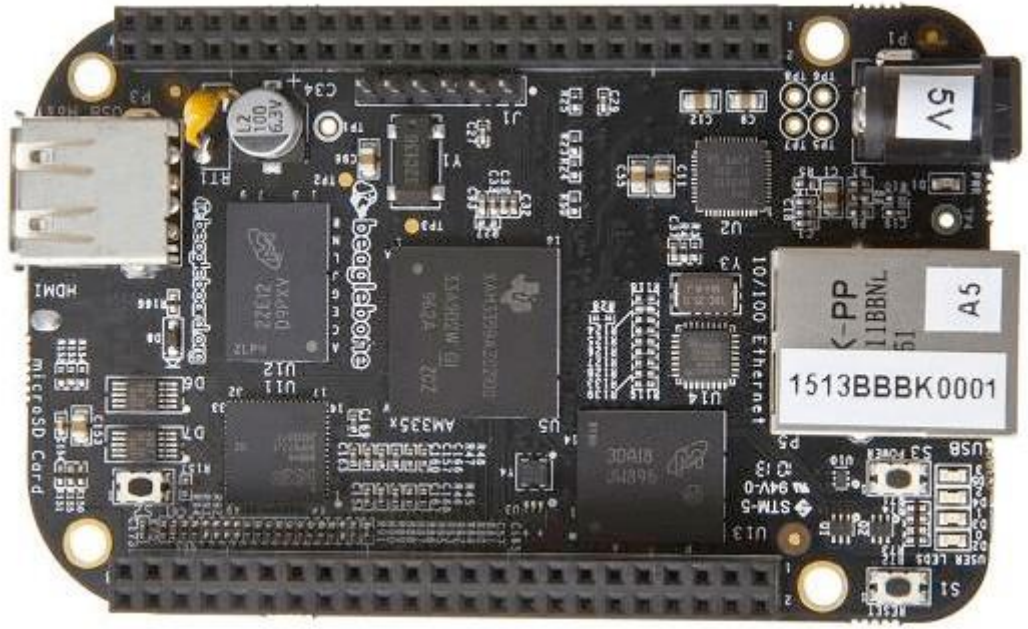
2 Teensy

Arduino Pro Mini 328

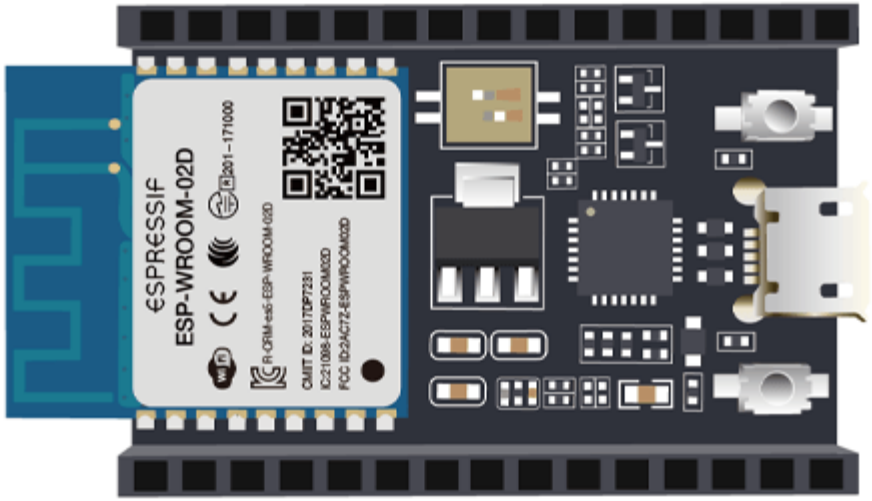
Raspberry Pi 4



BeagleBone Black



ESP8266 Microcontroller Board



References :

1.Daniel Minoli, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, Wiley Publications, First Edition, 2013. (UNIT I-IV)
2. Arsheep Bahga , Vijay Madisetti , Internet of Things: A Hands-On Approach, Universities Press, First Edition , 2014.(UNIT I & V)


Thank You!