Embedded System Chapter 7. IOT and Embedded Systems (3 hrs)

Level: Bachelor
Programme: BE Computer
Semester: III/V

Ishwor Koirala, Ph.D.

Instructor

Outline

Introduction

Books

Course Contents

1. Introduction to Embedded system (3 hrs)
2. Programming for Embedded systems (5 hrs)
3. Real-time operating systems (RTOS) (5 hrs)
4. Embedded System Design using VHDL (5 hrs)
5. Communications Protocals (3 hrs)
6. Pheripherals and Interfacing (4 hrs)
7. **Internet of Things (IoT) and Embedded systems (3hrs)**

Internet of Things

- IoT stands for Internet of Things.
- It refers to the interconnectedness of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data.
- This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.
- **Internet of Things (IoT)** is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment.
- In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives.

Internet of Things

- IOT is a system of interrelated things, computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers.
- And the ability to transfer the data over a network requiring human-to-human or human-to-computer interaction.

History of IOT

- Here you will get to know about how IOT is involved and also from the explanation of each will let you know how IOT plays a role in this innovations !
- 1982 – Vending machine: The first glimpse of IoT emerged as a vending machine at Carnegie Mellon University was connected to the internet to report its inventory and status, paving the way for remote monitoring.

Internet of Things

- 1990 – Toaster: Early IoT innovation saw a toaster connected to the internet, allowing users to control it remotely, foreshadowing the convenience of smart home devices.
- 1999 – IoT Coined (Kevin Ashton): Kevin Ashton coined the term “Internet of Things” to describe the interconnected network of devices communicating and sharing data, laying the foundation for a new era of connectivity.
- 2000 – LG Smart Fridge: The LG Smart Fridge marked a breakthrough, enabling users to check and manage refrigerator contents remotely, showcasing the potential of IoT in daily life.
- 2004 – Smart Watch: The advent of smart-watches introduced IoT to the wearable tech realm, offering fitness tracking and notifications on-the-go.

Internet of Things

- 2007 – Smart iPhone: Apple’s iPhone became a game-changer, integrating IoT capabilities with apps that connected users to a myriad of services and devices, transforming smartphones into hubs.
- 2009 – Car Testing: IoT entered the automotive industry, enhancing vehicles with sensors for real-time diagnostics, performance monitoring, and remote testing.
- 2011 – Smart TV: The introduction of Smart TVs brought IoT to the living room, enabling internet connectivity for streaming, app usage, and interactive content.
- 2013 – Google Lens: Google Lens showcased IoT’s potential in image recognition, allowing smartphones to provide information about objects in the physical world.

Internet of Things

- 2014 – Echo: Amazon’s Echo, equipped with the virtual assistant Alexa, demonstrated the power of voice-activated IoT, making smart homes more intuitive and responsive.
- 2015 – Tesla Autopilot: Tesla’s Autopilot system exemplified IoT in automobiles, introducing semi-autonomous driving capabilities through interconnected sensors and software.

Four Key Components of IOT

- Device or sensor
- Connectivity
- Data processing
- Interface

Internet of Things

- **IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.**
- Over 9 billion ‘Things’ (physical objects) are currently connected to the Internet, as of now.
- In the near future, this number is expected to rise to a whopping 20 billion.

Main Components Used in IoT

- **Low-power embedded systems:** Less battery consumption, high performance are the inverse factors that play a significant role during the design of electronic systems.
- **Sensors:** Sensors are the major part of any IoT application. It is a physical device that measures and detects certain physical quantities and converts it into signal which can be provided as an input to processing or control unit for analysis purpose.

Internet of Things

Different types of Sensors

- Temperature Sensors
- Image Sensors
- Gyro Sensors
- Obstacle Sensors
- RF Sensor
- IR Sensor
- MQ-02/05 Gas Sensor
- LDR Sensor
- Ultrasonic Distance Sensor

Internet of Things

- **Control Units:** It is a unit of small computer on a single integrated circuit containing microprocessor or processing core, memory and programmable input/output devices/peripherals. It is responsible for major processing work of IoT devices and all logical operations are carried out here.
- **Cloud computing:** Data collected through IoT devices is massive, and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
- **Availability of big data:** We know that IoT relies heavily on sensors, especially in real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.

Internet of Things

Networking connection:

- In order to communicate, internet connectivity is a must, where each physical object is represented by an IP address.
- However, there are only a limited number of addresses available according to the IP naming.
- Due to the growing number of devices, this naming system will not be feasible anymore.
- Therefore, researchers are looking for another alternative naming system to represent each physical object.

Internet of Things

Ways of Building IOT

There are two ways of building IoT:

- Form a separate internet work including only physical objects.
- Make the Internet ever more expansive, but this requires hard-core technologies such as rigorous cloud computing and rapid big data storage (expensive).
- In the near future, IoT will become broader and more complex in terms of scope.
- It will change the world in terms of

“anytime, anyplace, anything in connectivity.”

Internet of Things

IoT Enablers

RFIDs: uses radio waves in order to electronically track the tags attached to each physical object.

Sensors: devices that are able to detect changes in an environment (ex: motion detectors).

Nanotechnology: as the name suggests, these are tiny devices with dimensions usually less than a hundred nanometers.

Smart networks: (ex: mesh topology).

Internet of Things

Working with IoT Devices

Collect and Transmit Data : For this purpose sensors are widely used they are used as per requirements in different application areas.

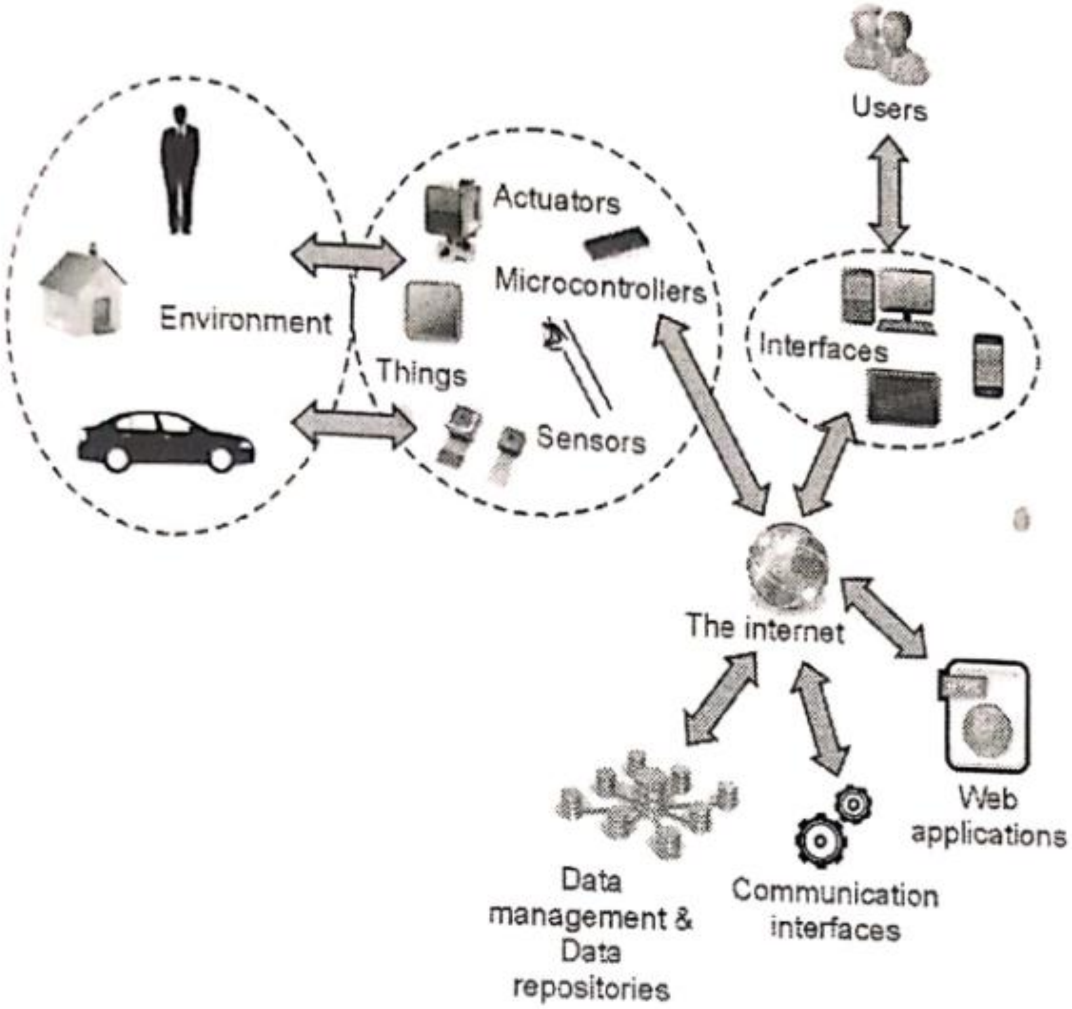
Actuate device based on triggers produced by sensors or processing devices: If certain conditions are satisfied or according to user's requirements if certain trigger is activated then which action to perform that is shown by Actuator devices.

Receive Information: From network devices, users or devices can take certain information also for their analysis and processing purposes.

Communication Assistance: Communication assistance is the phenomenon of communication between 2 networks or communication between 2 or more IoT devices of same or different networks. This can be achieved by different communication protocols like: MQTT, Constrained Application Protocol, ZigBee, FTP, HTTP etc.

Internet of Things

a



Internet of Things

Characteristics of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that do not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

Internet of Things

Desired Quality of any IoT Application

Interconnectivity

It is the basic first requirement in any IoT infrastructure. Connectivity should be guaranteed from any devices on any network then only devices in a network can communicate with each other.

Heterogeneity

There can be diversity in IoT enabled devices like different hardware and software configuration or different network topologies or connections, but they should connect and interact with each other despite so much heterogeneity.

Internet of Things

Dynamic in Nature

IoT devices should dynamically adapt themselves to the changing surroundings like different situations and different prefaces.

Self-adapting and self configuring technology

For example, surveillance camera. It should be flexible to work in different weather conditions and different light situations (morning, afternoon, or night).

Intelligence

Just data collection is not enough in IoT, extraction of knowledge from the generated data is very important. For example, sensors generate data, but that data will only be useful if it is interpreted properly. So intelligence is one of the key characteristics in IoT.

Internet of Things

Because data interpretation is the major part in any IoT application because without data processing we can’t make any insights from data.
Hence, big data is also one of the most enabling technologies in IoT field.

Scalability
The number of elements (devices) connected to IoT zones is increasing day by day. Therefore, an IoT setup should be capable of handling the expansion. It can be either expand capability in terms of processing power, storage, etc. as vertical scaling or horizontal scaling by multiplying with easy cloning.
Identity
Each IoT device has a unique identity (e.g., an IP address). This identity is helpful in communication, tracking and to know status of the things.

Internet of Things

If there is no identification then it will directly affect security and safety of any system because without discrimination we can’t identify with whom one network is connected or with whom we have to communicate. So there should be clear and appropriate discrimination technology available between IoT networks and devices.

Safety

Sensitive personal details of a user might be compromised when the devices are connected to the Internet. So data security is a major challenge. This could cause a loss to the user. Equipment in the huge IoT network may also be at risk. Therefore, equipment safety is also critical.

Architecture

It should be hybrid, supporting different manufacturer’s products to function in the IoT network.

Internet of Things

Application Domains

IoT is currently found in four different popular domains:

1) Manufacturing/Industrial business - 40.2%
2) Healthcare - 30.3%
3) Security - 7.7%
4) Retail - 8.3%

Internet of Things

Modern Applications

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection
- Water flow monitoring
- Traffic monitoring
- Wearables
- Smart door lock protection system

Internet of Things

- Robots and Drones
- Healthcare and Hospitals, Telemedicine applications
- Security
- Biochip Transponders (For animals in farms)
- Heart monitoring implants (Example Pacemaker, ECG real time tracking)
- Agriculture
- Industry

Internet of Things

Advantages of IoT

- Improved efficiency and automation of tasks.
- Increased convenience and accessibility of information.
- Better monitoring and control of devices and systems.
- Greater ability to gather and analyze data.
- Improved decision-making.
- Cost savings.

Internet of Things

Disadvantages of IoT

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- Dependence on technology and potential for system failures.
- Limited standardization and interoperability among devices.
- Complexity and increased maintenance requirements.
- High initial investment costs.
- Limited battery life on some devices.
- Concerns about job displacement due to automation.
- Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.

Internet of Things

The role of embedded systems in the IoT can be summarized as follows:

Sensor Integration:

Embedded systems are responsible for integrating sensors into devices. Sensors are used to detect and measure physical properties such as temperature, pressure, and humidity. These sensors generate data that is processed by the embedded system and transmitted to other devices or the cloud.

Communication:

Embedded systems are responsible for communication between devices. This communication can be wireless or wired, and can use a variety of protocols such as Wi-Fi, Bluetooth, and Zigbee. Embedded systems also handle the routing of data between devices.

Internet of Things

Data Processing:

Embedded systems are responsible for processing the data generated by sensors. This processing can include filtering, normalization, and aggregation. The processed data is then transmitted to other devices or the cloud.

Security:

Embedded systems are responsible for the security of devices in the IoT. This includes securing data transmission, securing access to devices, and protecting against cyber attacks.

Power Management:

Embedded systems are responsible for managing the power consumption of devices in the IoT. This includes managing the power supply, optimizing power usage, and managing battery life.

Internet of Things

Applications of Embedded Systems in IoT

Embedded systems in IoT are responsible for collecting, processing, and transmitting data between various devices and systems, and they play a crucial role in the overall functionality of IoT systems. Here are some of the applications of embedded systems in IoT:

Smart Homes: Embedded systems in IoT are used in smart home applications to automate various functions such as lighting, temperature control, security, and entertainment. These systems are designed to be energy-efficient and cost-effective, and they can be controlled remotely using a smartphone or other internet-enabled devices.

Internet of Things

Industrial Automation: In industrial settings, embedded systems in IoT are used to monitor and control various machines and equipment. These systems enable real-time monitoring of production processes, ensuring that they run smoothly and efficiently. They can also detect and report any anomalies, reducing downtime and improving productivity.

Healthcare: Embedded systems in IoT are used in healthcare applications to monitor vital signs, track medication schedules, and manage chronic conditions. These systems can transmit data to healthcare providers in real-time, allowing for timely intervention in case of emergencies.

Agriculture: Embedded systems in IoT are used in precision agriculture to monitor soil moisture, temperature, and other environmental factors that affect crop growth. These systems enable farmers to optimize irrigation and fertilization, resulting in higher yields and reduced water usage.

Internet of Things

Transportation: Embedded systems in IoT are used in transportation applications to monitor vehicle performance, track routes, and manage logistics. These systems can also be used to monitor traffic conditions and optimize routes, reducing travel time and fuel consumption.

Examples of Embedded Systems in the IoT:

There are many examples of embedded systems in the IoT. Some examples include:

Smart Home Devices:

Embedded systems are used in smart home devices such as thermostats, lighting systems, and security systems. These devices are capable of communicating with each other and with the cloud, and can be controlled by a smartphone or other device.

Internet of Things

Medical Devices:

Embedded systems are used in medical devices such as pacemakers, insulin pumps, and blood glucose monitors. These devices are capable of monitoring the patient’s condition and transmitting data to healthcare providers.

Industrial Automation:

Embedded systems are used in industrial automation systems such as assembly lines, robotics, and process control systems. These systems are capable of monitoring and controlling industrial processes, improving efficiency and productivity.

Internet of Things

Some Possible Challenges of Embedded Systems in IoT

While embedded systems in IoT offer a host of benefits, they also face several challenges that can affect their performance and functionality. Here, we will explore some of the possible challenges of embedded systems in IoT.

Power consumption: One of the most significant challenges of embedded systems in IoT is power consumption. Many of these systems are designed to operate on battery power, making energy efficiency a critical factor in their design. The system must be optimized to consume minimal power while still performing its required functions. Additionally, as the number of devices in an IoT network increases, the power consumption also increases, creating a significant challenge for the design of the overall IoT ecosystem.

Internet of Things

Security: Embedded systems in IoT are also vulnerable to security threats. These systems often collect sensitive data and communicate with other devices, making them an attractive target for hackers. Ensuring the security of embedded systems requires implementing robust encryption, authentication, and access control mechanisms. However, as the number of devices in an IoT network grows, managing the security of each device becomes increasingly complex.

Interoperability: Embedded systems in IoT must be interoperable with other devices and systems. However, achieving interoperability is challenging due to the heterogeneity of devices and communication protocols used in IoT networks. As a result, developing an interoperable IoT ecosystem requires careful consideration of the devices and protocols used.

Internet of Things

Scalability: Another significant challenge for embedded systems in IoT is scalability. As the number of devices in an IoT network grows, the embedded systems must be designed to scale up to support the increased demand. This requires careful consideration of the hardware and software architecture used in the system, as well as the communication protocols and data management mechanisms.

Real-time performance: Many embedded systems in IoT must perform real-time functions, such as controlling and monitoring devices. Achieving real-time performance requires designing the system with low-latency communication and processing mechanisms. However, as the number of devices in an IoT network grows, ensuring real-time performance becomes increasingly challenging.

Internet of Things

MQTT Protocol in IOT:

Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol designed for machine-to-machine (M2M) communication, particularly in environments with high latency and low bandwidth. It is widely used in the **Internet of Things (IoT)** due to its efficiency and simplicity.

Key Principles of MQTT

Publish-Subscribe Model

MQTT operates on a **publish-subscribe model**, where clients (publishers) send messages to a central server called a broker, which then distributes these messages to clients (subscribers) interested in specific topics.

This model decouples the message sender from the receiver, allowing for flexible and dynamic communication patterns.

Internet of Things

MQTT Clients and Broker

Clients: Devices or applications that publish or subscribe to messages. They can perform both roles simultaneously.

Broker: The central server that receives, filters, and distributes messages to the appropriate clients.

Quality of Service (QoS) Levels

MQTT supports three levels of message delivery guarantees:

QoS 0: At most once delivery.

QoS 1: At least once delivery.

QoS 2: Exactly once delivery.

Internet of Things

Retained Messages and Last Will and Testament (LWT)

Retained Messages: Brokers store the last message on a topic and send it to new subscribers immediately upon subscription.

LWT: Clients can specify a message to be published by the broker if they unexpectedly disconnect.

Advantages of MQTT in IoT

Lightweight and Efficient: Minimal bandwidth and processing overhead, making it suitable for resource-constrained devices.

Scalable: Can handle thousands of concurrently connected clients.

Reliable: Built-in features to ensure reliable message delivery even over unreliable networks.

Secure: Supports encryption and authentication mechanisms such as TLS.

Internet of Things

Characteristics of MQTT

Lightweight: MQTT is designed to be lightweight, making it suitable for use in aid-restrained environments inclusive of embedded systems and low-strength devices. The protocol minimizes bandwidth and processing overhead, enabling green communication even on restricted networks.

Publish-Subscribe Model: In the publish-subscribe version, clients (publishers) send messages to subjects, and different clients (subscribers) acquire messages from subjects of interest. This decoupling of producers and purchasers permits for flexible and dynamic conversation styles.

Internet of Things

Quality of Service (QoS) Levels: MQTT supports exclusive stages of message delivery warranty, referred to as Quality of Service (QoS). QoS levels range from 0 to 2, providing various stages of reliability and message transport guarantees, relying at the utility necessities.

Retained Messages: MQTT lets in agents to store retained messages on topics, making sure that new subscribers acquire the maximum latest message posted on a subject right now after subscribing. This characteristic is beneficial for fame updates and configuration settings.

Last Will and Testament (LWT): MQTT clients can specify a Last Will and Testament message to be posted by way of the broker in the occasion of an sudden consumer disconnect. This function affords a mechanism for detecting patron failures and dealing with them gracefully.

Internet of Things

Security: MQTT helps various protection mechanisms, consisting of Transport Layer Security (TLS) encryption and authentication mechanisms which include username/password and consumer certificates. These capabilities make certain the confidentiality, integrity, and authenticity of messages exchanged over MQTT connections.

Internet of Things

Conclusion:

- MQTT is a powerful protocol for IoT applications, offering efficient, reliable, and secure communication between devices.

- Its lightweight nature and support for various QoS levels make it ideal for resource-constrained environments[1]

Overview of Common IOT Hardware Platforms:

Arduino:

- It is an Italian open-source hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices.
- Its hardware products are licensed under a CC BY-SA license, while the software is licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), permitting the manufacture of Arduino boards and software distribution by anyone.
- Arduino boards are available commercially from the official website or through authorized distributors.

Overview of Common IOT Hardware Platforms:

- Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards ('shields') or breadboards (for prototyping) and other circuits.
- The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs. The microcontrollers can be programmed using the C and C++ programming languages (Embedded C), using a standard API which is also known as the **Arduino Programming Language**, inspired by the Processing language and used with a modified version of the Processing IDE. In addition to using traditional compiler tool chains, the Arduino project provides an integrated development environment (IDE) and a command line tool developed in Go.

Overview of Common IOT Hardware Platforms:

- Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards ('shields') or breadboards (for prototyping) and other circuits.
- The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs. The microcontrollers can be programmed using the C and C++ programming languages (Embedded C), using a standard API which is also known as the **Arduino Programming Language**, inspired by the Processing language and used with a modified version of the Processing IDE.
- In addition to using traditional compiler tool chains, the Arduino project provides an integrated development environment (IDE) and a command line tool developed in Go.

Overview of Common IOT Hardware Platforms:

- The Arduino project began in 2005 as a tool for students at the Interaction Design Institute Ivrea, Italy, aiming to provide a low-cost and easy way for novices and professionals to create devices that interact with their environment using sensors and actuators.
- Common examples of such devices intended for beginner hobbyists include simple robots, thermostats, and motion detectors.
- The name *Arduino* comes from a café in Ivrea, Italy, where some of the project's founders used to meet.
- The bar was named after Arduin of Ivrea, who was the margrave of the March of Ivrea and King of Italy from 1002 to 1014.

Overview of Common IOT Hardware Platforms:

Manufacturer	Arduino
Type	Single-board microcontroller
Operating system	None (default) Xinu
CPU	Atmel AVR (8-bit) ARM Cortex-M0+ (32-bit) ARM Cortex-M3 (32-bit) Intel Quark (x86) (32-bit)
Memory	SRAM
Storage	Flash, EEPROM

Arduino Uno SMD R3

Overview of Common IOT Hardware Platforms:

ESP32

- It is a series of low-cost, low-power system-on-chip microcontrollers with integrated Wi-Fi and dual-mode Bluetooth.
- The ESP32 series employs either a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations, an Xtensa LX7 dual-core microprocessor, or a single-core RISC-V microprocessor and includes built-in antenna switches, RF balun, power amplifier, low-noise receive amplifier, filters, and power-management modules.
- Commonly found either on device specific PCBs or on a range of development boards with GPIO pins and various connectors depending on the model and manufacturer of the board.
- ESP32 is created and developed by Espressif Systems, a Chinese company based in Shanghai, and is manufactured by TSMC using their 40 nm process. It is a successor to the ESP8266 microcontroller.

Overview of Common IOT Hardware Platforms:

Features of the ESP32 include the following:[3]

- Processors:
  - CPU: Xtensa dual-core (or single-core) 32-bit LX6 microprocessor, operating at 160 or 240 MHz and performing at up to 600 DMIPS
  - Ultra low power (ULP) co-processor
- Memory: 520 KiB RAM, 448 KiB ROM
- Wireless connectivity:
  - Wi-Fi: 802.11 b/g/n
  - Bluetooth: v4.2 BR/EDR and BLE (shares the radio with Wi-Fi)
- Peripheral interfaces:
  - 34 × programmable GPIOs
  - 12-bit SAR ADC up to 18 channels
  - 2 × 8-bit DACs

Overview of Common IOT Hardware Platforms:

- 10 × touch sensors (capacitive sensing GPIOs)
- 4 × SPI
- 2 × I²S interfaces
- 2 × I²C interfaces
- 3 × UART
- SD/SDIO/CE-ATA/MMC/eMMC host controller
- SDIO/SPI slave controller
- Ethernet MAC interface with dedicated DMA and planned IEEE 1588 Precision Time Protocol support
- CAN bus 2.0
- Infrared remote controller (TX/RX, up to 8 channels)
- Pulse counter (capable of full quadrature decoding)
- Motor PWM
- LED PWM (up to 16 channels), Ultra low power analog pre-amplifier

Overview of Common IOT Hardware Platforms:

- Security:
  - IEEE 802.11 standard security features all supported, including WPA, WPA2, WPA3 (depending on version) and WLAN Authentication and Privacy Infrastructure (WAPI)
  - Secure boot, Flash encryption
  - 1024-bit OTP, up to 768-bit for customers
  - Cryptographic hardware acceleration: AES, SHA-2, RSA, elliptic curve cryptography (ECC), random number generator (RNG)
- Power management:
  - Internal low-dropout regulator
  - Individual power domain for RTC
  - 5 µA deep sleep current
  - Wake up from GPIO interrupt, timer, ADC measurements, capacitive touch sensor interrupt

Overview of Common IOT Hardware Platforms:

Raspberry Pi:

- It is a series of small single-board computers (SBCs) developed in the United Kingdom.
- The original Raspberry Pi computer was developed by the Raspberry Pi Foundation in association with Broadcom.
- Since 2012, all Raspberry Pi products have been developed by Raspberry Pi Ltd, which began as a wholly-owned subsidiary of the Foundation.
- The Raspberry Pi project originally leaned toward the promotion of teaching basic computer science in schools.

Overview of Common IOT Hardware Platforms:

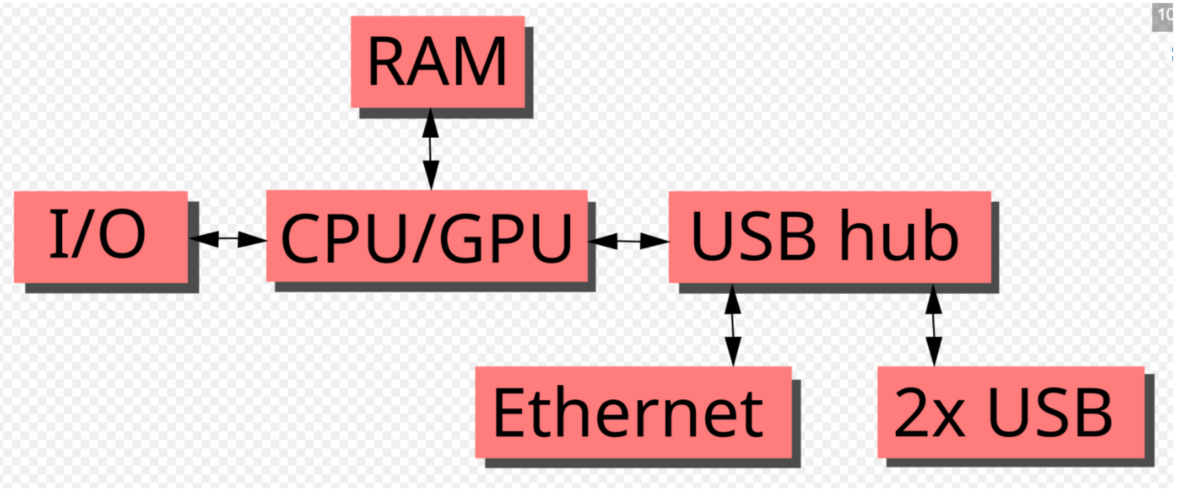
- The original model became more popular than anticipated, selling outside its target market for diverse uses such as robotics, home automation, industrial automation, and by computer and electronic hobbyists, because of its low cost, modularity, open design, and its adoption of the HDMI and USB standards.

Raspberry Pi generations:

- The first-generation **Raspberry Pi Model B** was released in February 2012, followed by the simpler and cheaper **Model A**.
- **Raspberry Pi Model B+**, an improved design, was released in 2014.
- These first-generation boards feature ARM11 processors, are approximately credit-card sized, and represent the standard *mainline* form factor. The **A+** and an improved B model were released within a year.

Overview of Common IOT Hardware Platforms:

- The Raspberry Pi hardware has evolved through several versions that feature variations in the type of the central processing unit, amount of memory capacity, networking support, and peripheral-device support.
- Raspberry Pi provides Raspberry Pi OS (formerly called Raspbian), a Debian-based Linux distribution for download, as well as third-party Ubuntu, Windows 10 IoT Core, RISC OS, LibreELEC (specialised media centre distribution) and specialised distributions for the Kodi media centre and classroom management



Block diagram describing models B, B+, A and A+