

IoT Technologies Wireless Sensor Networks (WSN) Wireless Sensor Networks are all about efficient, affordable, and low-power devices designed for remote sensing applications. They rely on low-power integrated circuits and wireless communication as their core technologies. WSNs involve numerous smart sensors that gather raw data, process and analyze it, and filter it to create usable information. Once the data is in the desired format, it can be put to use. However, there are some key challenges: - IoT and Wireless Sensor Network nodes have limited processing capabilities because they must be energy-efficient and cost-effective. This means they have CPUs with low processing power and limited memory modules. - Large memory modules are not feasible for low-cost devices due to their high cost, leading to storage challenges. This is where Cloud computing support becomes essential. IoT Cloud Computing Support Cloud computing is "the brain" of IoT. Think of it this way: your hands and feet sense and interact with the world, but the decisions are made in your brain. Your brain also stores memories of what you sensed and decided. Similarly, in IoT, sensors gather data, and actuators respond remotely. However, the storage and intelligent decision-making happen in the cloud, which acts as the "brain" of the IoT network. For advanced IoT services, you need a place to collect, analyze, and process raw data into actionable information. Cloud computing provides the necessary support. Many IoT devices lack sufficient processing power and memory. Even if they did have it, relying solely on their data capabilities is not wise. Cloud computing platforms offer reliable, fast, and agile support. They allow IoT devices to overcome software, firmware, memory, and processing limitations. Moreover, not processing at the sensors conserves energy. IoT devices sense, send data, and then go into sleep mode until their next sensing period. Cloud computing has numerous benefits, including energy savings in the sensors, which extends the battery life of devices. Data is securely stored at remote locations, allowing a comprehensive view of all sensor data in a region for intelligent decision-making. In this context, "offloading" means saving a backlog of data and processing it elsewhere to conserve energy. Cloud computing supports offloading not only for IoT devices but also for smartphones, laptops, tablets, augmented reality, and game consoles. To extract information and make intelligent decisions, we require artificial intelligence, machine learning, deep learning, and big data engines. This necessitates significant computing power and a wealth of data. In essence, to become smart, you need to study a lot, and for that, you need a place to store and process the vast amount of information, which is where Cloud computing plays a crucial role. Cloud service models encompass Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). IoT R&D (Research & Development) areas IoT devices are often limited in memory, processing power, and run on batteries. To connect these devices to the Internet, we use IP networks, specifically IPv4 and IPv6. These are the foundational Internet protocols, carrying data in packets through routers and gateways. When we talk about IoT, we're essentially connecting things to the Internet, so IPv4 and IPv6 are essential. IoT will play a big role in the future of the Internet. To make it work effectively, we must ensure the security, privacy, and integrity of the information it handles, as well as user confidentiality. IoT devices, including wearable ones, can collect a lot of personal information. If this data falls into the wrong hands, it can lead to physical and financial harm. That's why keeping this information confidential is vital, as IoT data is all about us. In IoT research, key focus is on device authentication and authorization, as well as user authentication and authorization. 1. Any DEVICE connecting to your network must be authenticated and authorized. 1.1 Without proper checks, there's a risk of hacker devices trying to infiltrate your network for malicious purposes, like launching ransomware attacks or denial of service attacks. This can compromise the network's integrity. Therefore, DEVICE AUTHENTICATION is a must. 1.2 Once a device passes authentication, it needs to be AUTHORIZED. Administrators determine its authorization level, specifying how much access it's granted and which databases it can access. 2. USER authentication is just as important. People accessing IoT systems should also be checked and authorized, ensuring that only authorized individuals can interact with the devices. Public and private key management plays a role in governing authentication and authorization. These keys are used to encrypt and protect sensitive data, ensuring that only authorized users can decrypt and access it. Additionally, there's the concept of THING-TO-THING ACCESS CONTROL, which is crucial for maintaining security and privacy in IoT networks. In a previous lecture, we discussed Machine-to-Machine (M2M) communication, where devices connect with one another.

This is a significant part of the Internet of Things (IoT). Besides M2M, we also have Human-to-Thing (H2T), Thing-to-Human (T2H), and Human-to-Human (H2H) communication, where the "things" are often machines. These options cover the range of interactions. Among these, the M2M domain is the largest, accounting for about 45%. It involves LOW OVERHEAD protocols and SIMPLE processing. We'll delve into wireless personal area network technologies and low-power, low-processing devices used in IoT networks, aiming for efficiency and longevity in specific tasks. Mobility support is crucial for devices like smartwatches, smartphones, tablets, belts, shoes, and glasses that move with us. The network must seamlessly switch connections as we move, ensuring consistent services. This includes not only the connection but also the end-to-end data flow from our devices to servers or other people. Mobile platform-based IoT opens up a wide range of future applications, such as location-based services (LBS), social networking, environment monitoring, and energy/resource management. While challenging to implement, it brings valuable opportunities for various services and interactions. Energy issues are vital in IoT development, and they involve optimizing energy harvesting, conservation, and usage. Let's focus on energy harvesting, which is about making the most of available energy sources. IoT devices can draw power from various sources, like light, wind, microwave radiation, Wi-Fi signals, or mobile communication signals. Some devices even have the capability to pick up and store this energy. Additionally, there are wireless charging options, such as charging pads from different vendors. The concept of energy harvesting involves three key principles: 1. Minimize Waste: Use energy sparingly and efficiently, avoiding unnecessary consumption. 2. Seize Opportunities: Take advantage of any available energy sources for charging. 3. Store and Use Wisely: Save the harvested energy and utilize it when needed. This approach guides research and development efforts in the IoT field, ensuring that devices operate sustainably and efficiently. It's essential to consider various resource constraints in IoT research and development. Factors like wake-up delays, power consumption, battery capacity, and packet sizes all play a crucial role. Identification techniques are also a critical aspect. IoT devices generate their content, which can be shared by authorized users. Therefore, identification and authentication technologies must be integrated and functional on a global scale. This is because IoT devices can connect with entities from anywhere in the world. Managing unique identities for IoT devices is vital, as it's part of the authentication process. Handling multiple identifiers for people and locations is also a necessary consideration in the IoT landscape. This complexity requires a focus on convergence and interoperability to ensure seamless connectivity and security across the diverse IoT ecosystem.

### IoT Hardware Technologies

In the realm of IoT, IoT hardware platforms handle the task of gathering, storing, and processing data over the internet connection. IoT hardware components include:

1. Sensors: they detect changes in the nearby physical environment like temperature, images (motion), infrared, gases, and humidity.
2. Actuators: these are devices such as motors that can be controlled to perform actions with the use of physical force, like opening or closing something.
3. RFID tags: these are tags that activate when an RFID reader comes close, transmitting information stored in the RFID unit. This is used in logistics control and for ID tags on people, machines, robots, and drones.
4. Processors and controllers: they link sensors and actuators to the internet. They can be programmed, including the methods of artificial intelligence.

### Sensor Types

Let's categorize sensor types based on their characteristics:

1. Temperature and Humidity Sensors: These sensors are used to detect temperature and humidity levels. Temperature sensors typically cover a wide range from -40 degrees Celsius to 80 degrees Celsius, while humidity sensors measure from 0 to 100 percent, spanning from dry to rainy conditions.
2. Pressure Sensors: Pressure sensors come in different ranges, depending on the application. They can measure atmospheric pressure, industrial pressure, fluid levels, and other pressure-related parameters. The range varies from 0 kiloPascals to 35 kiloPascals or can extend up to 650 kilopascals, depending on the specific use case.
3. Flow Sensors: These sensors monitor the rate of fluid flow, typically in the range of one to about 30 liters per minute, based on gauge specifications.
4. Image Sensors (cameras): Image sensors convert variable images into signals. They come in various configurations, such as 30 frames per second with a 640 by 480 VGA resolution, resulting in a 0.3-megapixel image. There are image sensors with lower data rates and high-resolution options, including high-definition CCTVs. The choice depends on the specific sensing requirements, and the use of augmented reality-based image processing can also be a factor in decision-making.

### Frames per Second (FPS)

When it comes to image sensors, the frames per

second (FPS) can vary, typically ranging from as low as 8 or 10 FPS to a standard of around 20 FPS, with some capable of reaching up to 30 FPS. Higher FPS value is desired for capturing and transmitting better images, but comes at the cost of higher processing, storage and transmission expenditures.

5. Ultrasonic Sensors: These sensors detect the presence of objects using ultrasonic waves. They operate in the range of about 2 to 400 centimeters distance, providing non-contact measurements. The measurements are typically based on a 40-kiloHertz measurement mechanism, making them suitable for various applications.

Actuators There are different of atuators types, including:

- Electrical Actuators: These convert energy into mechanical torque and are used for tasks like opening and closing doors.
- Mechanical to Linear Actuators: They transform rotary motion into linear motion, serving various functions, including controlling the flow of air, gases, and fluids.
- Hydraulic and Pneumatic Actuators: These actuators convert fluid or gas compression into mechanical motion. They offer different motion types, such as linear, rotary, and oscillatory, among others.

RFID (Radio Frequency Identification) Devices RFID Devices: RFID devices consist of a coil and a chip, and they do not have a built-in battery. When an RFID reader approaches and sends an energy or RF pulse, it activates the RFID device. The antenna coil charges the chip, allowing it to transmit its identification information to the RFID reader, facilitating the exchange of data. These sensor and actuator types contribute to the versatility and functionality of IoT systems, making them adaptable to a wide range of applications and requirements. The RFID technology plays a significant role in data exchange and information management. Some of its key components and applications:

1. RFID Chip: The RFID chip stores information about an object or the item to which the RFID tag is attached. It transfers this data to an RFID reader.
2. Antenna: The antenna receives energy from the RFID reader and is used for both receiving energy (charging) and sending information back to the reader. It serves as a charging unit and a wireless reply-sending unit.
3. RFID Types:
  - Low-Frequency RFID: Operating in the range of 125 to 134.3 kilohertz, these RFID systems have a read range of 10 to 30 centimeters. ISO standards apply to this category.
  - High-Frequency RFID: Operating at 13.56 megahertz, these systems offer a read range of 10 centimeters to one meter. Standards: ISO, ECMA, and Near-Field Communication (NFC) are associated with this category.
  - Ultra-High Frequency RFID: Working in the range of 860 to 960 megahertz, this type provides a much longer read range of up to 12 meters. It's suitable for applications like access control and tracking, following ISO standard ISO 18000-63.

RFID technology is usable in various fields, including:

- Efficient management, tracking, and monitoring processes.
- Logistics and supply chain applications.

Research and development on RFID: focusing on aspects like data stream support, chip design, energy optimization, automatic meter reading, home automation, and vehicle and transportation applications. The versatility of RFID technology makes it valuable for enhancing security and efficiency in a wide range of applications and industries.

### Processors & Microcontrollers

Processors and microcontrollers that support IoT technology are crucial for IoT device platforms. These processors and microprocessors work with hardware, software, sensors, and interfaces. Network modules are also essential components for communication. The central processing unit (CPU), is based on processors or microcontrollers. When we consider the hardware interfaces that connect users to sensors and actuators, it becomes evident that all these require microcontrollers and processors. To ensure smooth operation, operating systems must run on these processors and microcontrollers. This supports software interfaces and controls various hardware resources, including power, memory, and file input/output.

### Arduino

Arduino is an open-source microcontroller board based on a microcontroller chip. The project includes open-source Arduino hardware and software to program and utilize the board. Arduino offers microcontroller boards and kits, known for their flexibility, ease of deployment, and programming. Arduino's board circuit design and integrated development environment (IDE) are available on the Arduino website. Users can develop and upload specific programs using the IDE by connecting their computer to an Arduino board via a USB connection. Let us explore different types of Arduino products, starting with the Arduino Uno R3. This is a versatile circuit board that functions as a single-board computing system. Other examples of Arduino products include

- Arduino Yun, designed for specific IoT applications.
- Arduino Lilypad, tailored for wearable IoT applications.

Arduino boards are often based on Atmel AVR processors, particularly the ATmega series, which we previously discussed as essential components for IoT hardware. Among these, the ATmega328P microcontroller and its variants are noteworthy modules. Atmel Taking a closer

look at the specifications of the ATmega328, you'll find information about the CPU speed, which is at most 20 MIPS (Millions of Instructions Per Second). Each instruction is a command that the processor executes, and this processor can handle up to 20 million assembly instructions per second. The specifications also include details about RAM, program memory (flash memory), data EEPROM, input/output interfaces, timers, temperature range, and operating voltage range. Examining the ATmega328P module, we find that it supports a low-power consumption mode, and its other specifications are generally similar. It is a component adopted in the mainline Arduino and Arduino Uno systems. This module operates at one megahertz with a voltage of 1.8 volts, and the overall current levels are notably low, measured in milliamperes and microamperes. When we consider power consumption, it's a product of voltage and current ( $\text{Power} = \text{Voltage} \times \text{Current}$ ). In this case, both the voltage (1.8V) and the current values are quite small. Low power consumption brings several advantages. First, it extends the battery life significantly. Second, it results in minimal heat radiation and heat generation within the device, enabling compact and tightly packaged designs. Furthermore, the device is less likely to overheat due to its low power consumption. Lastly, it contributes to a longer overall lifespan. When you charge the battery of such a device once, it can operate for an extended period. These reasons highlight the attractiveness of the low-power feature in the ATmega328P modules for IoT applications, as it offers enhanced efficiency, longevity, and compactness.

**Raspberry Pi** Raspberry Pi, developed by the Raspberry Pi Foundation in the UK, serves as an affordable single-board computer designed to promote basic computer science skills in schools. This board is an interesting tool for educational purposes. It supports general computation and web functions. Its hardware specifications include a Broadcom system-on-chip (SoC), an ARM CPU, an on-chip GPU, and the Raspbian OS operating system. There are several Raspberry Pi Models and they are suitable for general IoT functionality. There's also a subline, the Raspberry Pi Zero W, which is smaller and has restricted IO and GPIO capabilities.

**BeagleBoard** Another noteworthy option is the BeagleBoard, an open-source single-board computer produced by Texas Instruments, a major hardware and processor developer. It functions as a fully capable basic computer supporting various operating systems, including Linux and Android, making it an appealing choice, especially for those familiar with Linux and Android on smartphones and tablets. While it may be slightly more expensive than other single-board computers, the additional operating system features and enhanced operational capabilities make it an attractive option.

**Exploring the key features of the BeagleBone Black**, we find that it has very low power requirements, consuming up to about two watts. It includes a programmable real-time unit (PRU) with deterministic latency, achieving an impressive five nanoseconds per instruction, making it ideal for delay-sensitive applications. Furthermore, it boasts an enhanced processor with image and 3D graphics processing capabilities.

### IoT Device Platforms Comparison

Let's compare the three devices we discussed: the Arduino Uno, the Raspberry Pi 3 Model B, and the Beaglebone Black.

**CPU Type:** The Arduino Uno is a microcontroller, while the Raspberry Pi 3 Model B and the Beaglebone Black are single-board microcomputers.

**CPU:** the Arduino Uno uses a 16 megahertz AT Mega 328. The Raspberry Pi 3 Model B employs a Broadcom SOC with a 1.2 gigahertz ARM Cortex CPU, which is quad-core. On the other hand, the Beaglebone Black is based on an ARM Cortex-A8 and has a single-core CPU.

**Memory:** The Raspberry Pi and similar units have 0.5-8 GB of RAM, and support micro SDHC cards. The Beaglebone Black uses DDR with 512 megabytes of DDR3 technology. Arduino, being a microcontroller has much less RAM memory, typically kilobytes of ram and flash memory.

**Input-output:** the Arduino Uno offers 14 digital GPIO interfaces and 6 analog inputs. The Raspberry Pi 3 Model B boasts 40 digital GPIO units and 4 USB 2.0 interfaces. The Beaglebone Black has 69 GPIOs, 4 UART Serial, and 8 PWM modes.

**Size:** the Arduino Uno is the smallest and lightest among the three. The Beaglebone Black is lighter than the Raspberry Pi 3 Model B, and in terms of dimensions, the Raspberry Pi 3 Model B and the Beaglebone Black are quite similar.

**Operating system and programming:** the Arduino Uno uses the Arduino IDE for programming and only has a bootloader preloaded that serves as an elementary operating system. The Raspberry Pi 3 Model B runs on Linux, specifically Raspbian, offering a robust open-source option. On the other hand, the Beaglebone Black supports a range of operating systems, including Unix (Ubuntu, Debian) and even Windows, which provides diverse choices for users.

**Audio:**, the Raspberry Pi 3 Model B features a 3.5-millimeter analog audio output and HDMI audio support, while the Beaglebone Black uses Micro HDMI for audio. The Arduino Uno has no provisions for audio.

**Video:** the

presence of HDMI interfaces can be a significant factor in choosing between these devices. The Arduino Uno lacks video support, and if video is needed, you would have to add an external unit for it. On the other hand, the Raspberry Pi 3 Model B offers HDMI support, and the Beaglebone Black has Micro HDMI interfaces, making them attractive choices for tasks involving audio and video. Networking: The Arduino Uno lacks robust wired or wireless Ethernet capabilities. In contrast, the Raspberry Pi 3 Model B stands out in this regard with features like Bluetooth 4.1, BLE, Ethernet connections, and 2.4 gigahertz Wi-Fi based on 802.11n. The Raspberry Pi 3 Model B and the Beaglebone Black offer compelling options for different use cases. The Raspberry Pi 3 Model B, with its Bluetooth, BLE, and Wi-Fi capabilities, is an excellent choice for remote control and monitoring, making it popular for applications where you want to use your smartphone as a controller and data interface collector. Its connectivity features make it a strong candidate for these scenarios. The Beaglebone Black's wired Ethernet connections, supporting both 10 megabits per second and 100 megabits per second, are highly valuable in desktop or development environments. The ability to connect via Ethernet makes it a preferred choice for situations where you need stable, high-speed network connectivity. Both the Raspberry Pi 3 Model B and the Beaglebone Black offer 10 base T and 100 base T Ethernet connections, providing versatility for different networking needs.