UNIT – 6 : CURRENT TOPICS RELATED TO COMPUTER NETWORK

Software-Defined Networks:

Software-defined Networking (SDN) is an innovative approach to network architecture that separates the control plane from the data plane in networking devices. Traditionally, networking devices such as routers and switches have both control plane and data plane functions integrated into a single device. The control plane determines how network traffic should be forwarded, while the data plane is responsible for actually forwarding the traffic.

In SDN, the control plane is decoupled from the data plane and moved to a centralized software-based controller. This controller communicates with the network devices to program and manage their behavior dynamically.

Why Software-Defined Networking is important?

SDN represents a substantial step forward from traditional networking, in that it enables the following:

- **Increased control with greater speed and flexibility:** Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.
- **Customizable network infrastructure:** With a software-defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.
- **Robust security:** A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

The key difference between SDN and traditional networking is infrastructure: SDN is software-based, while traditional networking is hardware-based. Because the control plane is software-based, SDN is much more flexible than traditional networking. It allows administrators to control the network, change configuration settings, provision resources, and increase network capacity — all from a centralized user interface, without the need for more hardware.

There are also security differences between SDN and traditional networking. Thanks to greater visibility and the ability to define secure pathways, SDN offers better security in many ways. However, because software-defined networks use a centralized controller, securing the controller is crucial to maintaining a secure network.

How does Software-Defined Networking (SDN) work?

Software-Defined Networking (SDN) works by decoupling the control plane from the data plane in network devices, allowing centralized control and programmability of network behavior.

Here's a step-by-step explanation of how SDN works:

1. **Centralized Controller**:
   - In an SDN architecture, a centralized controller serves as the brain of the network. This controller is implemented as software running on a server or cluster of servers.
   - The controller communicates with network devices (e.g., switches, routers) using a standardized protocol, typically OpenFlow, though there are other protocols as well.
2. **Southbound Interface**:
   - The controller communicates with network devices through a southbound interface. This interface allows the controller to instruct the devices on how to forward packets based on predefined policies and rules.
   - Through the southbound interface, the controller can dynamically configure the forwarding behavior of network devices, such as setting up forwarding rules, modifying routing tables, or adjusting Quality of Service (QoS) parameters.
3. **Northbound Interface**:
   - Applications and network services interact with the controller through a northbound interface. This interface provides high-level APIs that allow applications to define network policies and request network resources.
   - The northbound interface abstracts the underlying complexity of the network, allowing applications to focus on their specific requirements without needing to understand the details of individual network devices.

4. **Flow Table Entries**:

- Network devices maintain flow tables, which are used to determine how to handle incoming packets. Each entry in the flow table specifies a flow, which consists of a set of packet attributes (e.g., source/destination IP address, port numbers) and corresponding actions.
- The controller populates these flow tables with forwarding rules and policies based on the requirements specified by applications or network administrators.

5. **Flow-based Forwarding**:

- Instead of traditional destination-based forwarding, SDN enables flow-based forwarding, where packets are forwarded based on predefined flow entries in the devices' flow tables.
- When a packet arrives at a network device, the device matches the packet's attributes against the flow entries in its flow table and applies the corresponding action (e.g., forward, drop, modify).

6. **Dynamic Adaptation**:

- SDN allows for dynamic adaptation of network behavior in response to changing traffic patterns, application requirements, and network conditions.
- The controller continuously monitors the network state and can reconfigure flow table entries or update network policies in real-time to optimize performance, ensure security, and meet service-level objectives.

Components of Software Defining Networking (SDN):

The three main components that make the SDN are:

1. **SDN Applications:** SDN Applications relay requests or networks through SDN Controller using API.
2. **SDN controller:** SDN Controller collects network information from hardware and sends this information to applications.
3. **SDN networking devices:** SDN Network devices help in forwarding and data processing tasks.

What are the different models of SDN?

While the premise of centralized software controlling the flow of data in switches and routers applies to all software-defined networking, there are different models of SDN.

- **Open SDN:** Network administrators use a protocol like OpenFlow to control the behavior of virtual and physical switches at the data plane level.
- **SDN by APIs:** Instead of using an open protocol, application programming interfaces control how data moves through the network on each device.
- **SDN Overlay Model:** Another type of software-defined networking runs a virtual network on top of an existing hardware infrastructure, creating dynamic tunnels to different on-premise and remote data centers. The virtual network allocates bandwidth over a variety of channels and assigns devices to each channel, leaving the physical network untouched.
- **Hybrid SDN:** This model combines software-defined networking with traditional networking protocols in one environment to support different functions on a network. Standard networking protocols continue to direct some traffic, while SDN takes on responsibility for other traffic, allowing network administrators to introduce SDN in stages to a legacy environment.

Advantages of SDN:

- The network is programmable and hence can easily be modified via the controller rather than individual switches.
- Switch hardware becomes cheaper since each switch only needs a data plane.
- Hardware is abstracted, hence applications can be written on top of the controller independent of the switch vendor.
- Provides better security since the controller can monitor traffic and deploy security policies. For example, if the controller detects suspicious activity in network traffic, it can reroute or drop the packets.

Disadvantages of SDN:

- The central dependency of the network means a single point of failure, i.e. if the controller gets corrupted, the entire network will be affected.
- The use of SDN on large scale is not properly defined and explored.

Wireless Sensor Networks (WSNs):

A **Wireless Sensor Network (WSN)** is a collection of sensors that can communicate wirelessly and share data collected from the surrounding environment. The data is routed through numerous nodes and then connects to other networks such as **wireless Ethernet** via a **gateway**. The nodes in a wireless sensor network are equipped with a variety of sensors, including **temperature, humidity, light, motion**, and others. Each sensor node has the following key components: a **transducer**, **microcomputer, transceiver**, and **power supply**.

The **transducer** produces electric signals in response to detected physical phenomena. The **microcomputer** handles sensor data processing and storage. The **transceiver** receives instructions from a central computer and sends data back to it. Power for each node is sourced from batteries. WSNs are used in a variety of fields, including **environmental monitoring, industrial automation, healthcare, agriculture**, and **smart cities**.

Applications of Wireless Sensor Networks (WSNs):

WSNs have nearly endless potential applications across all global industries. These include environmental monitoring and management, medical and healthcare services, as well as location and tracking, localization, and logistics

1. **Environmental Monitoring:** WSNs have a wide range of environmental applications that include monitoring environmental conditions. Some examples are given below.

   - **Air Quality Monitoring:** Wireless sensor networks have been implemented in cities such as London to measure harmful gas concentrations and particulate matter levels. These networks give higher temporal and geographical precision for monitoring air pollution, assisting researchers in better understanding human exposure discrepancies.

   - **Forest Fire Detection:** By deploying a network of sensor nodes throughout the forest, fires can be detected in real-time. These nodes, equipped with temperature, humidity, and gas sensors, can detect indicators of fire, allowing firefighting crews to respond quickly.

   - **Water Quality Monitoring:** Water quality evaluation in bodies of water such as dams, rivers, lakes, and seas is critical for protecting the environment. The use of several wireless dispersed sensors allows for the production of a more precise map of the water condition, as well as the permanent deployment of monitoring stations in difficult-to-reach areas without the need for human data retrieval.

2. **Military Applications:** WSNs are important in military intelligence by facilitating surveillance, reconnaissance, and monitoring tasks. They are integral components of military systems that include intelligence gathering, command and control, communication, computing, frontline surveillance, investigative operations, and target acquisition.

3. **Medical Applications:** WSNs can be used in healthcare for remote patient monitoring, tracking medical equipment, and gathering physiological data such as heart rate, blood pressure, and temperature. They can help in the early diagnosis of medical issues and improve the standard of patient treatment.

4. **Agricultural Application:** WSNs facilitate precision agriculture by monitoring soil conditions, crop growth, and weather patterns. This data assists farmers in optimizing irrigation, fertilization, and pest management, resulting in higher crop output and less resource wastage.

5. **Industrial Applications:** Wireless Sensor Networks (WSNs) play an important role in industrial settings, providing real-time monitoring and data gathering for a wide range of applications. These include industrial automation, predictive maintenance, supply chain management, energy optimization, environmental monitoring, quality control, safety and hazard detection, asset tracking, smart grids, mining and oil exploration, precision agriculture, and water management.

Types of WSN:

The environment determines the network types acceptable for deployment, which can cover underwater, subterranean, terrestrial landscapes, and more. **Wireless Sensor Networks** (WSNs) are classified into several types, including:

1. **Terrestrial WSN:**

    - **Terrestrial Wireless Sensor Networks** (WSNs) easily establish connections with base stations by deploying hundreds to thousands of wireless sensor nodes in either **unstructured** (ad hoc) or **structured** (pre-planned) configurations.
    - In the unstructured approach, sensor nodes are randomly positioned across the target area, typically released from a fixed plane.
    - In the preplanned or structured approach involves methods like **optimal placement, grid arrangement**, and **2D** or **3D placement models**.
    - Despite the limited battery power in these WSNs, solar cells supply additional energy.
    - Energy conservation is achieved through various strategies such as low-duty cycle operations, minimizing delays, and optimizing routing, among others.

2. **Underground WSN:**
   - Underground wireless sensor networks have higher deployment, maintenance, and equipment costs compared to terrestrial alternatives, requiring careful planning and design.
   - These networks utilize hidden sensor nodes buried underground to monitor and gather data on subterranean conditions.
   - Extending data from subterranean nodes to the base station involves the use of additional above-ground sink nodes for relaying information.
   - Recharging batteries for subterranean sensor nodes is challenging due to their placement and limited power capacity, necessitating innovative energy solutions.
   - The underground environment leads to significant signal attenuation and loss, posing difficulties for maintaining reliable wireless communication within the network.
3. **Underwater WSN:**
   - **Underwater wireless sensor networks** contain several sensor nodes and submerged vehicles for data collection.
   - Autonomous underwater vehicles are instrumental in retrieving information from these sensor nodes.
   - Autonomous underwater vehicles play an important role in gathering data from these sensor nodes.
   - One of the main challenges in underwater communication is the significant propagation delay, a limited bandwidth, and the possibility of sensor failure.
   - Underwater WSNs face the limitation of non-rechargeable or replaceable batteries.
   - To address energy-saving problems in such networks, specialized underwater communication and networking solutions must be developed.
4. **Multimedia WSN:**
   - Multimedia wireless sensor networks have arisen to help with event surveillance and observation using multimedia formats such as photos, videos, and sounds.
   - These networks are made up of low-cost sensor nodes fitted with microphones and cameras that communicate through wireless links to perform activities like as data compression, retrieval, and correlation.

- The difficulties associated with multimedia WSNs include significant energy consumption, demanding bandwidth requirements, sophisticated data processing, and effective compression methods.
- Furthermore, the transmission of multimedia content requires a large amount of bandwidth to enable effective and seamless delivery.

5. **Mobile WSN:**

- **Mobile Wireless Sensor Networks** (MWSNs) are made up of sensor nodes that can move independently and interact with their environment.
- The mobile nodes are capable of computing, sensing, and communicating.
- Mobile wireless sensor networks are more versatile than their static alternatives.
- In comparison to static wireless sensor networks, the advantages of MWSNs include expanded coverage, superior energy efficiency, larger channel capacity, and other desirable features.

Classification of Wireless Sensor Networks:

WSNs can be classified according to their application, but their fundamental distinctions arise from their types. Typically, WSNs are often categorized into several categories, as shown below.

1. **Static & Mobile WSN:**

- **Static Wireless Sensor Networks** (WSNs) are made up of stationary sensor nodes that are sensibly deployed to monitor and collect data from their permanent positions. These nodes are commonly placed in various environments to gather data and send it to a central location for processing and analysis.
- **Mobile Wireless Sensor Networks** (MWSNs), on the other hand, involve sensor nodes that can move and interact with the environment. These nodes can change their positions independently or under external monitoring, allowing them to adapt to changing conditions and collect data from various locations.

2. **Deterministic & Nondeterministic WSN:**

- In a deterministic network, the arrangement of sensor nodes can be predetermined and precisely calculated. Such pre-planned sensor node operation may be feasible in specific applications.
- In many applications, determining the exact positions of sensor nodes can be tough due to factors like tough conditions and harsh environments. As a result, these networks are labeled as non-deterministic, which means they need complex control systems to operate effectively.

3. **Single Base Station & Multi Base Station WSN:**

   - A single base station Wireless Sensor Networks (WSNs) use a single central hub, known as the base station or sink node, that serves as the main point of communication and data aggregation for all sensor nodes in the network. This single base station receives and processes all collected data.

   - In **Multi Base Station WSNs**, there are multiple base stations distributed across the network area. These base stations work together to gather, analyze, and manage data from sensor nodes. This approach can enhance network coverage, data redundancy, and reliability.

4. **Static Base Station & Mobile Base Station WSN:**

   - In a **Static Base Station Wireless Sensor Network** (WSN), the base station remains stationary in a preset position during its operation. Sensor nodes in the network send data to this stationary base station for processing, analysis, and further transmission.

   - In a **Mobile Base Station WSN**, the base station is not stationary and can move within the network area. This mobility enables the base station to dynamically move closer to certain sensor nodes or regions of interest, optimizing data collection efficiency and network coverage.

5. **Single-hop & Multi-hop WSN:**

   - In a single-hop network configuration, sensor nodes are directly positioned to establish communication with the base station, ensuring a direct data transmission path.

   - In a multi-hop network, both cluster heads and peer nodes play a role in data transmission, which helps to reduce energy consumption by efficiently distributing the communication load across the network.

6. **Self-Reconfigurable & Non-Self Configurable WSN:**

   - The sensor nodes in a **Self-Reconfigurable Wireless Sensor Network** (WSN) can modify their configurations, such as communication paths, roles, or parameters, autonomously in response to changing conditions or requirements. This adaptability enables the network to optimize its performance dynamically.

   - The sensor nodes in a **Non-Self Configurable WSN** have predefined configurations that are selected during the setup process and stay constant during operation. These nodes are unable to reconfigure themselves in response to evolving circumstances.

7. **Homogeneous & Heterogeneous WSN:**
   - **Homogeneous Wireless Sensor Networks** (WSNs) are made up of sensor nodes with identical capabilities, characteristics, and functionalities. All nodes in such networks have identical hardware, software, and communication capabilities, resulting in a uniform and consistent network structure.
   - **Heterogeneous Wireless Sensor Networks**, on the other hand, are made up of sensor nodes with a wide range of functionalities. The processing capacity, communication range, energy resources, sensing modalities, and computing capabilities of these nodes may differ. The network's heterogeneity allows it to execute specialized tasks, adapt to varied environments, and effectively handle variable workloads.

Components of WSN:

A Wireless Sensor Network (WSN) has the following components:

1. **Sensors:** Sensors are fundamental components that capture environmental variables and convert them into electrical signals. They play a key role in data acquisition within the network.
2. **Radio Nodes:** Radio nodes gather data from sensors and transmit it to the **Wireless Local Area Network** (WLAN) access point. They are composed of components such as microcontrollers, transceivers, external memory, and power sources.
3. **WLAN Access Point:** The WLAN access point receives data wirelessly from radio nodes, often facilitating internet connectivity. It acts as a gateway for the sensor data to be transmitted to remote locations.
4. **Evaluation Software:** Evaluation software processes data received by the WLAN access point. This software analyzes and displays the collected data to users. The data can then be processed, analyzed, stored, and mined for more insights.

Challenges of WSN:

The following are some of the numerous challenges in wireless sensor networks:

- **Fault Performance:** In Wireless Sensor Networks (WSNs), certain sensor nodes may cease operation due to factors like power depletion or physical damage. These failures must not have a significant impact on the sensor network's overall performance. This challenge is addressed through the concept of fault tolerance, which refers to the network's ability to continue functioning even in the face of sensor node failures.

- **Stability:** Stability refers to a network's capacity to sustain constant and dependable performance over time, despite dynamic changes in its operating circumstances. It indicates that the network's behavior, communication, data transfer, and general operation remain predictable and dependable even when confronted with numerous difficulties like node failures, changes in environmental conditions, variations in communication quality, and energy limitations.

- **Cost of Production:** Wireless sensor networks are composed of numerous sensor nodes, with the cost of each node playing a significant part in determining the entire network cost. It is imperative to ensure that the price of each sensor node remains low to maintain cost-effectiveness for the entire network.

- **Operation Environment:** The operation environment of wireless sensor networks encompasses the physical surroundings in which the nodes are deployed. This environment can vary widely, ranging from urban settings to remote and challenging terrains. The network's effectiveness and performance are determined by how effectively the nodes are designed, configured, and optimized to function under these specific operational conditions.

- **Quality of Service:** Quality of Service (QoS) in WSNs pertains to the specific requirements and application demands from the network. These requirements may include things like energy efficiency, network operating time, and data transfer reliability.

- **Data Aggregation:** Data aggregation is the process of combining information gathered from various sources inside a network. This includes functions such as computing averages, maximum and minimum values, and other operations that consolidate the data into more understandable and useful forms.

- **Data Compression:** Data compression is the process of reducing the size of data using various techniques. The goal of this process is to reduce the amount of storage space required for data transmission and storage, making data transport more efficient while preserving critical information.

- **Data Latency:** These factors are regarded as critical influencers in the design of routing protocols. Data latency can arise due to operations like data aggregation and multi-hop relays, which play a significant role in determining the efficiency and performance of the network.

Design Challenges:

- **Energy Efficiency:** WSN nodes are often powered by batteries and have limited energy resources. Routing protocols must consume as little energy as possible to ensure the network's longevity.

- **Location of Sensor:** Sensor location is critical for applications such as environmental monitoring and target tracking. Designing routing protocols that incorporate location awareness can improve the efficiency and efficacy of data routing.
- **Complexity:** WSNs can consist of a large number of nodes and the routing protocols must be designed to manage this complexity effectively.
- **Data Transmission and Transmission Models:** Interference, fading, and attenuation can all have an impact on data transmission in WSNs. As a result, the transmission of data & transmission models is also a challenge while designing the WSNs.
- **Strength:** The reliability and robustness of communication in WSNs are crucial, especially in harsh or dynamic environments. We must create routing protocols that can tolerate signal losses, node failures, and network topology changes while still delivering data.
- **Scalability:** WSNs can accommodate thousands of nodes. Routing protocols must be scalable to support bigger networks without compromising efficiency or incurring unnecessary overhead.
- **Delay:** Some applications in WSNs, such as event detection or real-time monitoring, require low-latency data transmission.

Advantages of WSN:

- **Cost-effectiveness:** WSNs utilize affordable, compact sensors that can be deployed with minimal expense, making them a cost-efficient solution for diverse applications.
- **Wireless Connectivity:** WSNs eliminate the need for intricate wired connections, saving on installation costs and allowing for adaptable network deployment and reconfiguration.
- **Scalability:** WSNs offer the flexibility to easily expand or shrink the network by adding or removing sensors, making them adaptable to various scenarios and settings.
- **Energy Conservation:** By employing energy-efficient devices and protocols, WSNs extend their operational lifespan without frequent battery replacements, promoting sustainability.
- **Real-time Monitoring:** WSNs provide real-time monitoring of environmental factors, providing timely insights for informed decision-making and effective control.

Internet of Things (IoT):

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.

Components of IoT:

- **Devices/Things**: These are physical objects equipped with sensors, actuators, processors, and connectivity modules. IoT devices can range from consumer electronics (e.g., smart home devices, wearables) to industrial equipment (e.g., connected machinery, sensors in manufacturing plants).
- **Sensors and Actuators**: Sensors collect data from the environment, such as temperature, humidity, motion, light, and sound, while actuators enable devices to take actions based on the data received.
- **Connectivity**: IoT devices communicate with each other and with cloud-based services using various wireless and wired communication protocols, including Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, cellular (e.g., 4G/5G), and Ethernet.
- **Cloud-based Services**: Data collected by IoT devices is often processed, stored, and analyzed in cloud-based platforms or edge computing environments. These services provide storage, data analytics, machine learning, and integration with other applications and systems.

Ways of Building IOT:

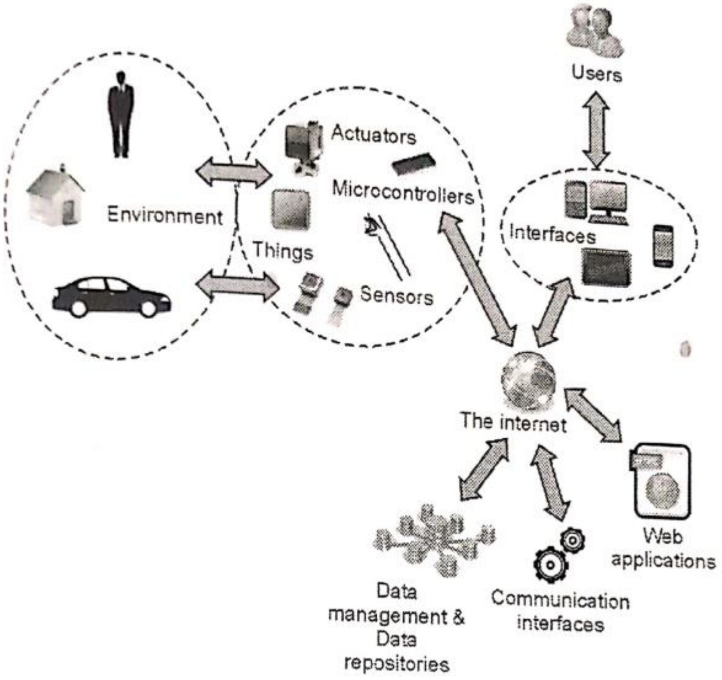
There are two ways of building IoT -

- 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).

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.



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.

Applications of IoT:

- **Smart Home**: IoT enables home automation and smart home systems, including smart lighting, thermostats, security cameras, door locks, and appliances, for increased convenience, energy efficiency, and security.
- **Healthcare**: IoT devices are used in healthcare for remote patient monitoring, wearable health trackers, medical device connectivity, and telemedicine, improving patient care and treatment outcomes.
- **Industrial IoT (IIoT)**: In industrial settings, IoT is used for asset tracking, predictive maintenance, process optimization, supply chain management, and real-time monitoring of equipment and operations.
- **Smart Cities**: IoT technologies are deployed in smart city initiatives for traffic management, waste management, environmental monitoring, public safety, energy management, and urban planning to improve quality of life and sustainability.
- **Agriculture**: IoT solutions in agriculture (AgriTech) enable precision farming, crop monitoring, soil moisture management, livestock tracking, and automated irrigation, leading to increased crop yields, resource efficiency, and sustainability.

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.

Disadvantages of IoT:

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- 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.

Cyber-Physical Systems:

A Cyber-Physical System (CPS) is a system that integrates physical and computational components to monitor and control the physical processes seamlessly.

In other words, A cyber-physical system is a collection of computing devices communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.

These systems combine the sensing, actuation, computation, and communication capabilities, and leverage these to improve the physical systems' overall performance, safety, and reliability.

Examples: CPS includes self-driving cars, The STARMAC is a small quadrotor aircraft.

Features of Cyber-Physical System:

in terms of the cyber-physical system, there are some features that are classified.

1. **Reactive Computation:** Reactive systems, on the other hand, continuously interact with the environment through inputs and outputs. As a classic example of reactive computation, consider a car cruise control program.
2. **Network Connectivity:** CPS systems must utilize the network connectivity basis of communication between the cyber and physical world.
3. **Robustness & Reliability:** In order to ensure safe and effective operation in dynamic environments, CPS must need efficient reliability.
4. **Concurrency:** In cyber-physical systems refers to the simultaneous execution of multiple tasks or processes in a coordinated manner.
5. **Real-Time Computation:** CPS systems have real-time computation capabilities that allow for dynamic decision-making based on physical real-world data.
6. **Safety-Critical Application:** In terms of the CPS applications where the safety of our systems higher priority over the performance and development of the system.

Characteristics of Cyber-Physical System:

- It is a combination of Physics with cyber-Components networked which is interconnected.
- CPS systems are to monitor and control physical processes in a seamless manner.
- In CPS systems sensors and Actuators work in the feedback loop.

- In CPS systems devices are designed to interact with physical processes and control them.
- The CPS systems are more complex compared then IoT devices.

Working Principles of Cyber-Physical System:

- **Sensing and Data Acquisition**: CPS use sensors and actuators to monitor physical processes, collect data about the environment, and control physical entities.
- **Data Fusion and Analysis**: Data collected from sensors are processed, fused, and analyzed to extract useful information, detect patterns, identify anomalies, and make predictions about the behavior of physical systems.
- **Decision Making and Control**: Based on the analysis of sensor data and system models, CPS make decisions and execute control actions to regulate physical processes, optimize performance, ensure safety, and achieve desired objectives.
- **Real-time Communication and Coordination**: CPS rely on real-time communication and coordination between physical components and computational systems to enable timely responses, feedback loops, and adaptive control strategies.
- **Adaptation and Optimization**: CPS continuously adapt and optimize their behavior in response to changes in the environment, system dynamics, and operational requirements, ensuring resilience, efficiency, and robustness.

Application of Cyber-Physical System:

Cyber-Physical systems have the widest application in the real world with technology, cps is mostly applied in many fields as you can see-

- **Agriculture:** Through the cps systems we can develop such kinds of sensors and tractors or harvesters that provide information on soil type and condition.
- **Aeronautics:** Aeronautics is one area that can benefit from CPS integration. In Aeronautics, CPS can be used to improve aircraft control and safety and improve performance and efficiency.
- **Healthcare and Personalized Medicine:** CPS systems have the technology which involves the use of connected medical devices and wearables to monitor patients' health data.
- **Civil Infrastructure:** Cyber-physical systems are using infrastructure improvement with some new efficiency technology. Advanced digital technology like IoT and sensors etc.

- **Manufacturing:** In manufacturing CPS can monitor and control the production process in real-time, improving quality and reducing scrap.
- **Transportation:** In transportation, CPS can improve safety and efficiency through intelligent traffic management systems, vehicle-to-vehicle communications, and self-driving vehicles.

Challenges of Cyber Physical System:

Now that we have seen applications of CPS, there are some difficulties that we face in these CPS. Let’s have a look at the challenges associated with cyber physical systems:

- **Real-Time System Abstraction:** Creating a framework is complex because of the intricate connections between sensors, actuators, and computers in dynamic CPS networks.
- **Durability, Safety, and Security:** CPS faces uncertainties from its interaction with the physical world, demanding intense system resilience, security, and safety.
- **Modeling and Control of Hybrid Systems:** Bridging the gap between real-time changes in the physical world and the distinct logic of cyberspace presents a challenge.
- **Control over Networks:** Designing networked control in CPS faces challenges such as time-based and event-based computing, time-varying delays, and system reconfiguration.
- **Sensor-Actuator Systems:** Current designs lack exploration into the impact of actuators on the entire system, requiring more attention to physical features in system design.
- **Validation and Verification:** Traditional methods like overdesign for safety certification are proving impractical for large-scale complex systems, pushing the need for new models, methods, and tools to ensure comprehensive verification and validation throughout the design cycle.

🧑‍💻