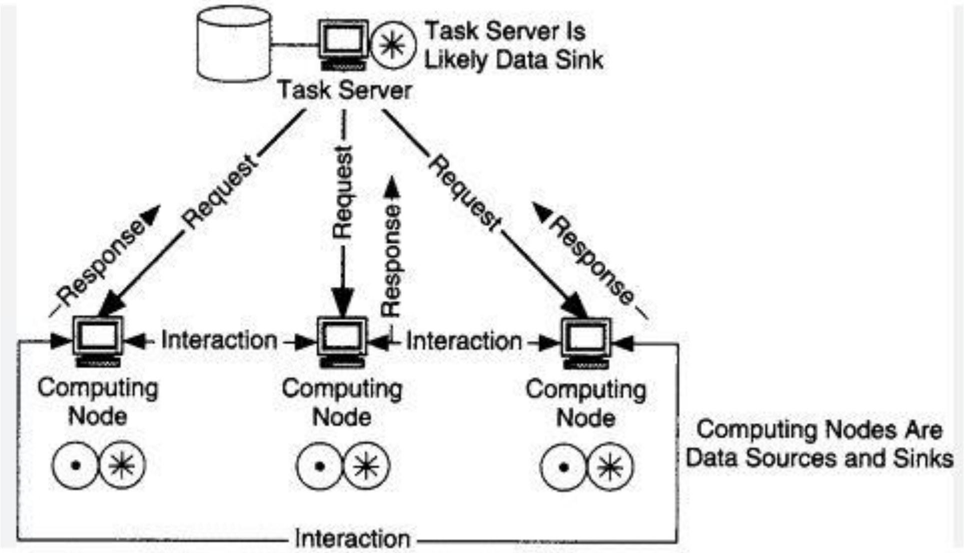
1. What is distributed computing? explain it briefly

Distributed computing is a computing model in which a large computing task is divided into smaller tasks and distributed across multiple computers connected by a network. Each computer, known as a node, works on its assigned task independently, and then the results are combined to produce the final output.

The distributed computing model allows for parallel processing, which means that the workload can be completed faster than if it was processed on a single computer. It also provides fault tolerance, as if one node fails, the task can still be completed by the other nodes.

Distributed computing is used in a wide range of applications, including scientific research, data processing, and web applications. It enables organizations to leverage the computing power of multiple machines and provides a more efficient and scalable way to process large volumes of data.

Examples: 3D Graphics, Video Rendering, Complicated scientific Problems For these works single computer is not enough because its too slow to complete tasks, time consuming process. Distributed computing Concepts is large problem will devide into smaller unit and distribute to the number of computers, they will work as unicell and complete the tasks in less time.



Advantages of distributed computing:

- **Scalability:** Distributed computing allows organizations to scale their computing resources as their needs grow, by adding more nodes to the network.
- **Fault tolerance:** Since the workload is distributed among multiple nodes, if one node fails, the other nodes can continue to work, ensuring fault tolerance.
- **Efficiency:** By dividing the workload among multiple nodes, distributed computing can process tasks faster than a single computer.
- **Cost-effective:** Distributed computing can be more cost-effective than investing in expensive hardware, as it leverages the resources of multiple machines.

Disadvantages of distributed computing:

- **Complexity:** Distributed computing can be complex to set up and maintain, requiring specialized knowledge and skills.

- **Communication overhead:** The nodes in a distributed computing network need to communicate with each other, which can lead to additional overhead and latency.
- **Security:** Distributing data and processing across multiple machines can create security risks if proper security measures are not implemented.
- **Compatibility issues:** The nodes in a distributed computing network may have different hardware, software, and operating systems, which can create compatibility issues

When selecting a task for distributed computing, there are several factors that should be considered:

Task complexity: Tasks that are highly complex and require significant computing resources are good candidates for distributed computing. This could include tasks such as large-scale simulations or data analysis.

Task parallelism: Tasks that can be divided into smaller sub-tasks that can be processed independently are well-suited for distributed computing. This allows the workload to be distributed across multiple nodes, which can significantly reduce processing time.

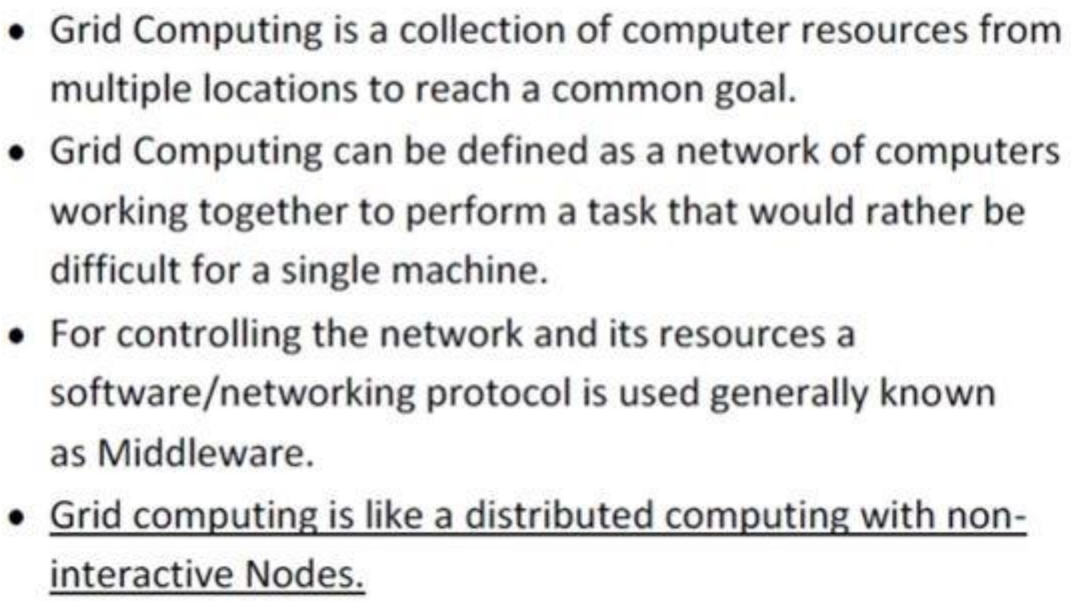
Resource availability: The resources required to process the task should be available in sufficient quantities across the distributed computing network. This could include processing power, storage, and networking resources.

Communication overhead: When selecting a task for distributed computing, it's important to consider the communication overhead between the nodes in the network. If the communication overhead is too high, it may negate the benefits of distributed computing.

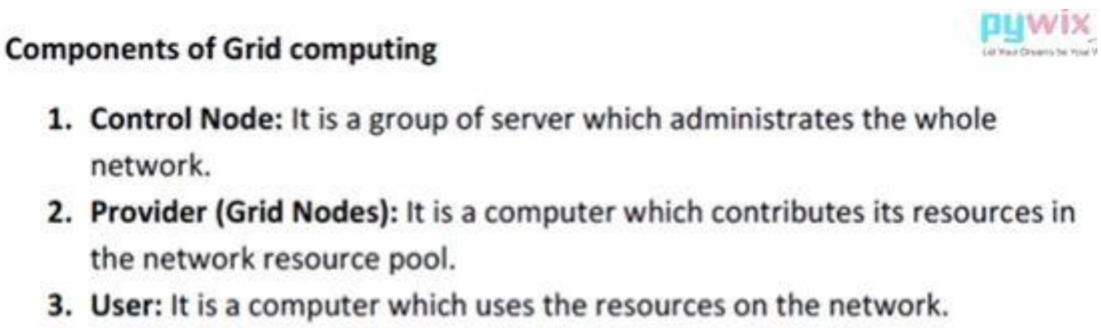
Data transfer: If the task involves significant data transfer between nodes, this should be factored into the selection process. Tasks that involve large amounts of data transfer may not be well-suited for distributed computing.

2. What is grid and cloud computing? Comparison between grid and cloud computing

- **Grid Computing:** Grid computing is a distributed computing model that allows organizations to share computing resources across multiple locations or entities. It involves coordinating and sharing resources such as processing power, storage, and networking across a network of computers. Grid computing is often used in scientific research, where large-scale computing power is required for complex simulations or data analysis.

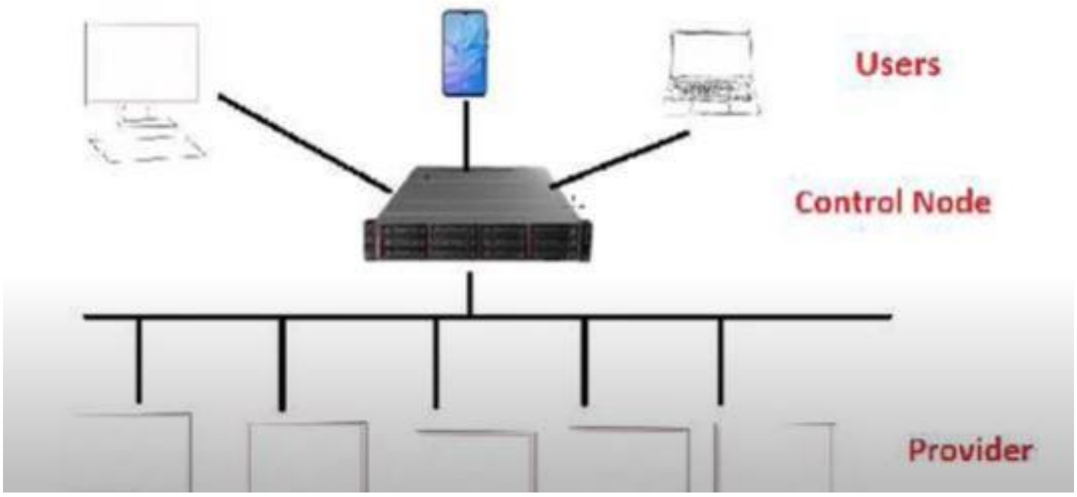


- Grid Computing is a collection of computer resources from multiple locations to reach a common goal.
- Grid Computing can be defined as a network of computers working together to perform a task that would rather be difficult for a single machine.
- For controlling the network and its resources a software/networking protocol is used generally known as Middleware.
- <u>Grid computing is like a distributed computing with non-interactive Nodes.</u>

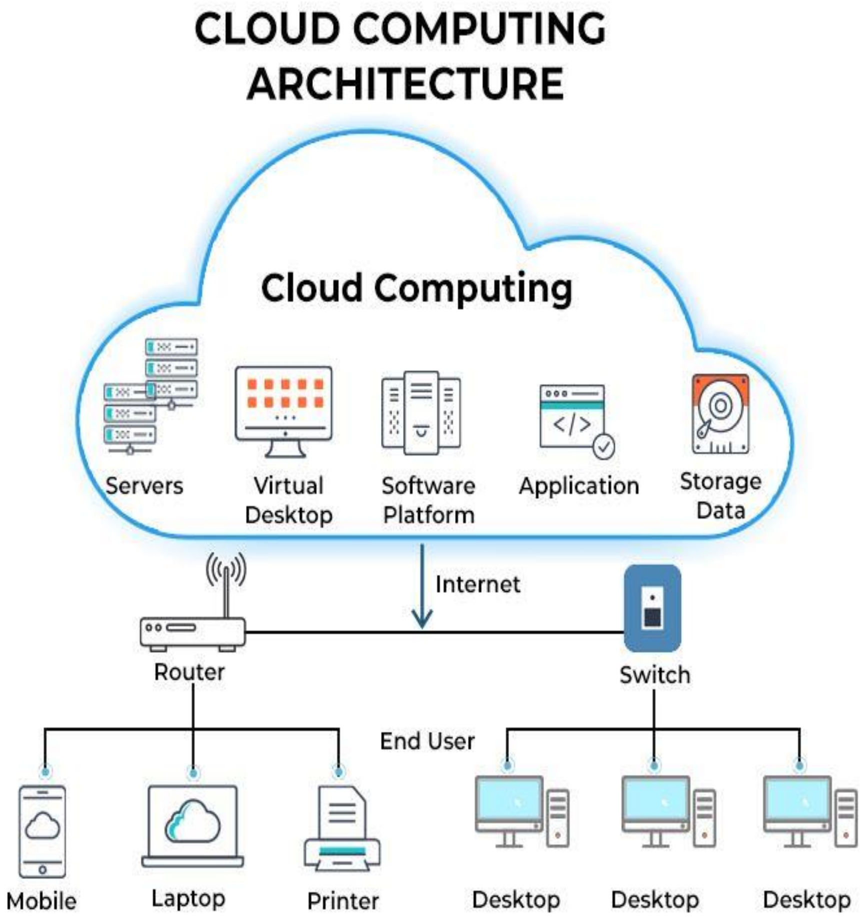


Components of Grid computing

1. **Control Node:** It is a group of server which administrates the whole network.
2. **Provider (Grid Nodes):** It is a computer which contributes its resources in the network resource pool.
3. **User:** It is a computer which uses the resources on the network.



- <u>**Cloud Computing:**</u> Cloud computing is a computing model that involves delivering computing services over the internet. In this model, computing resources such as processing power, storage, and applications are provided by a third-party provider, and users can access these resources on-demand over the internet. Cloud computing is often used in businesses, where it allows organizations to scale their computing resources up or down as needed, without having to invest in expensive hardware and infrastructure.



Examples of cloud computing:

- **Infrastructure as a Service (IaaS)** - Examples include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and IBM Cloud. These services provide virtualized computing resources such as storage, networking, and computing power.
- **Platform as a Service (PaaS)** - Examples include Heroku, Google App Engine, and Microsoft Azure App Service. These services provide a platform for developing, deploying, and running applications.
- **Software as a Service (SaaS)** - Examples include Microsoft Office 365, Salesforce, and Google Apps. These services provide access to software applications that are hosted on the cloud and can be accessed over the internet.
- **Cloud storage** - Examples include Dropbox, Google Drive, and OneDrive. These services provide a place to store and access data from anywhere with an internet connection.
- **Cloud hosting** - Examples include Amazon Elastic Compute Cloud (EC2), Microsoft Azure Virtual Machines, and DigitalOcean. These services allow businesses to host their websites or applications on remote servers, providing scalability and flexibility.
- **Cloud-based databases** - Examples include Amazon Relational Database Service (RDS), Google Cloud SQL, and Microsoft Azure SQL Database. These services provide scalable, managed databases that can be accessed from anywhere with an internet connection.

Comparisons:

- **Architecture:** Grid computing is based on a decentralized architecture, in which resources are shared among multiple organizations or entities, while cloud computing is based on a centralized architecture, in which resources are provided by a single provider.
- **Scalability:** Both grid and cloud computing can scale resources up and down as needed, but cloud computing is generally more scalable, as it can quickly provision resources in response to changing demand.
- **Resource ownership:** In grid computing, the resources are typically owned by the organizations or entities that contribute them, while in cloud computing, the resources are owned by the cloud provider.
- **Cost:** Grid computing can be more cost-effective than cloud computing for certain workloads, as it relies on shared resources and may not require ongoing subscription fees. However, cloud computing can provide cost savings for organizations that require flexible and scalable resources on an ongoing basis.
- **Security:** Grid computing can be more challenging to secure, as it involves sharing resources across multiple organizations or entities, while cloud computing can provide stronger security measures, as the cloud provider can control access to resources.

3.Explain utility computing with an example

Utility computing is a model of computing in which computing resources, such as processing power, storage, and software, are made available to users on an as-needed basis, just like the way we pay for utilities like electricity, gas or water. The users pay only for the resources they consume, rather than purchasing and maintaining their own infrastructure.

An example of utility computing is cloud computing services offered by companies like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. These services provide on-demand access to computing resources such as virtual machines, storage, and databases. Users can scale up or down their usage of these resources as per their requirements, and only pay for what they use.

For instance, a startup may need to host their website or application on a server that can handle a variable amount of traffic. Rather than investing in their own hardware and managing it, they can choose to use cloud computing services and pay only for the resources they need on a pay-as-you-go basis. As the traffic to their website increases, they can easily scale up their usage of computing resources, and as the traffic decreases, they can scale down their usage, which would result in cost savings.

Utility computing allows users to save on costs and resources and to focus on their core business without worrying about the underlying infrastructure.

Utility computing is based on the concept of providing computing resources as a service. It is similar to the way utilities like electricity or water are provided to consumers. Just like you pay for the electricity you consume, in utility computing, users pay for the computing resources they use.

Cloud computing services, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, are examples of utility computing. These services provide users with access to computing resources like virtual machines, storage, and databases on a pay-per-use basis. This means that users can quickly scale up or down their computing resources as needed without having to worry about the underlying infrastructure.

Benefits of utility computing:

- Utility computing offers several benefits to users. One of the main benefits is cost savings. Users only pay for the computing resources they use, which eliminates the need for them to invest in expensive hardware and software. This allows them to allocate their resources more effectively and focus on their core business.
- Another benefit of utility computing is scalability. Users can quickly and easily scale up their computing resources as their needs change. For example, a business may experience a surge in traffic to their website during a holiday season. With utility computing, they can quickly increase their computing resources to handle the extra traffic without having to invest in new hardware.

4.Explain briefly about characteristics of cloud computing.

3. On-demand self-service: Cloud computing resources can be provisioned and deployed by users on an on-demand basis without requiring human intervention from the cloud service provider.
4. Broad network access: Cloud computing resources can be accessed from any device with an internet connection, including desktops, laptops, smartphones, and tablets.
5. Resource pooling: Cloud computing resources are shared among multiple users and dynamically assigned based on demand.
6. Rapid elasticity: Cloud computing resources can be quickly and easily scaled up or down based on changing demand.
7. Measured service: Cloud computing resources usage is monitored and billed based on actual usage, providing users with a pay-per-use model.
8. Multi-tenancy: Cloud computing services are designed to allow multiple users to share a common infrastructure and resources while maintaining security and privacy.
9. Resilient computing: Cloud computing services are built to be highly available and fault-tolerant, providing users with reliable and resilient computing resources.

05/06/2023

Cloud Computing, Definition of Cloud Computing, Characteristics, Service Models, Deployment Models, Cloud Service Models Providers

Definition: Cloud computing refers to the delivery of computing resources over the internet on a pay-per-use basis. It allows users to access a shared pool of configurable computing resources, such as servers, storage, databases, applications, and services, without the need for owning or managing the underlying infrastructure.

Characteristics of cloud computing include:

- On-demand self-service: Users can provision and access computing resources as needed without requiring human intervention from the service provider.
- Broad network access: Cloud services are accessible over the network using standard protocols and devices, such as computers, laptops, tablets, and mobile phones.
- Resource pooling: Computing resources are pooled together to serve multiple users, enabling efficient resource utilization. Users typically have no control or knowledge over the exact location of the resources but may have control over certain parameters, such as storage capacity or performance levels.
- Rapid elasticity: Cloud resources can be scaled up or down quickly and easily based on the user's demand. This allows for flexibility and cost optimization by only utilizing resources when needed.
- Measured service: Cloud providers track and measure resource usage, providing transparency and allowing users to be billed for their consumption accurately. Examples of measured resources include storage, processing, bandwidth, and active user accounts.

Cloud computing can be categorized into three main service models:

- Infrastructure as a Service (IaaS): In this model, the cloud provider offers virtualized computing resources, such as virtual machines, storage, and networks. Users have control over the operating systems, applications, and deployed software, while the cloud provider manages the infrastructure's physical aspects.

- Platform as a Service (PaaS): PaaS provides a platform and environment for developers to build, test, and deploy applications. Users can focus on application development without worrying about managing the underlying infrastructure, including servers, storage, and network resources.
- Software as a Service (SaaS): SaaS provides fully functional applications over the internet. Users can access and use these applications without any requirement for installation or maintenance. The cloud provider manages the infrastructure, platform, and application software.

Cloud computing also has various deployment models:

- Public cloud: Resources are owned and operated by a third-party cloud provider, available to the general public over the internet. These services are typically offered on a pay-as-you-go basis. (Example: Amazon Web Services (AWS), which is a comprehensive cloud computing platform offered by Amazon. AWS provides a wide range of services, including computing power, storage, databases, machine learning, analytics, and more. Users can access these services over the internet on a pay-as-you-go basis.)
- Private cloud: Computing resources are dedicated to a single organization and are not shared with other users. It can be managed by the organization itself or a third-party provider and can be located on-premises or off-site. (Example: VMware vSphere, which is a virtualization platform that allows organizations to create their own private cloud environment. vSphere enables businesses to consolidate their physical servers into a pool of virtualized resources, which can be dynamically allocated and managed based on the organization's needs.)
- Hybrid cloud: This model combines public and private cloud resources, allowing data and applications to be shared between them. It provides flexibility and allows organizations to take advantage of both types of environments. (Example: An example of a hybrid cloud is Microsoft Azure Stack. Azure Stack is an extension of the Microsoft Azure cloud platform that enables organizations to build and deploy applications across both public and private cloud environments seamlessly.)
- Community cloud: Resources are shared between organizations with common interests, such as regulatory requirements or security concerns. It can be managed by the organizations themselves or a third-party provider.(Example: community cloud is the Health Information Exchange (HIE) system. HIE is a community cloud infrastructure that allows healthcare organizations, such as hospitals, clinics, pharmacies, and laboratories, to securely exchange patient health information and collaborate on patient care.)

Cloud service providers include well-known companies like:

1. Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud Platform (GCP)
4. IBM Cloud
5. Oracle Cloud
6. Salesforce
7. Alibaba Cloud
8. VMware Cloud
9. DigitalOcean
10. Rackspace

- Amazon Web Services (AWS): AWS is a comprehensive cloud platform offering a vast range of services, including compute power, storage, databases, analytics, machine learning, and more. It is widely used by businesses of all sizes.
- Microsoft Azure: Azure is Microsoft's cloud computing platform that provides services for building, deploying, and managing applications and services through Microsoft-managed data centers. It offers a wide array of services, including virtual machines, storage, databases, AI, and IoT capabilities.
- Google Cloud Platform (GCP): GCP is Google's cloud computing offering, providing a suite of cloud services similar to AWS and Azure. It includes services like computing, storage, machine learning, big data, networking, and developer tools.
- IBM Cloud: IBM Cloud is an enterprise-grade cloud platform that offers a range of services, including infrastructure, platform, and software services. It focuses on providing services for AI, blockchain, Internet of Things (IoT), and analytics.
- Oracle Cloud: Oracle Cloud is Oracle's cloud infrastructure platform that offers services for computing, storage, networking, databases, and applications. It also includes specific services for enterprise applications, data management, and AI.
- Alibaba Cloud: Alibaba Cloud is the cloud computing arm of Alibaba Group and is one of the leading cloud service providers in China. It offers a wide range of cloud services, including computing, storage, networking, big data analytics, AI, and more.

Advantages and Disadvantages of Cloud Computing:

Advantages of Cloud Computing:

- Scalability: Cloud computing allows for easy and on-demand scalability of computing resources. Users can quickly scale up or down based on their needs, without the need for significant upfront investments or infrastructure changes.
- Cost Savings: Cloud computing eliminates the need for organizations to invest in and maintain their own physical infrastructure. Instead, they can pay for the resources they consume on a pay-as-you-go basis, resulting in cost savings and improved cost predictability.
- Accessibility and Mobility: Cloud services are accessible from anywhere with an internet connection, enabling users to access their data and applications from various devices. This mobility promotes collaboration, flexibility, and remote work opportunities.
- Reliability and Availability: Cloud service providers often offer robust infrastructure and data redundancy measures, ensuring high availability and reliability of services. They typically have multiple data centers spread across different geographic locations, reducing the risk of data loss or service disruptions.
- Rapid Deployment: Cloud services enable rapid deployment of applications and services. Users can provision resources quickly and easily, reducing the time to market for new products or services.

Disadvantages of Cloud Computing:

- Dependency on Internet Connectivity: Cloud computing heavily relies on internet connectivity. Users require a stable and reliable internet connection to access and use cloud services. If the internet connection is slow or disrupted, it can affect productivity and access to critical resources.
- Security and Privacy Concerns: Storing sensitive data and applications in the cloud raises security and privacy concerns. Organizations need to trust cloud service providers with their data and ensure proper security measures are in place to protect against data breaches and unauthorized access.
- Limited Control: With cloud computing, organizations have limited control over the underlying infrastructure and systems. They rely on the service provider to manage and maintain the infrastructure, which can limit customization options and control over certain aspects of the environment.
- Vendor Lock-In: Switching cloud service providers or bringing back services in-house can be challenging and costly. Organizations may face difficulties in migrating their data and applications between different cloud platforms, leading to vendor lock-in.

- Potential Downtime: Although cloud service providers strive for high availability, service disruptions or downtime can occur. If the cloud provider experiences technical issues or outages, it can impact user access and business operations.

Cloud-based Services & Applications.

Cloud-based services and applications refer to software, tools, and services that are hosted and delivered through the cloud computing infrastructure. These services and applications are accessible over the internet, eliminating the need for users to install and run them on their local devices.

Here are some examples of cloud-based services and applications:

- Cloud Storage: Cloud storage services, such as Dropbox, Google Drive, and Microsoft OneDrive, allow users to store and access their files and data in the cloud. These services provide convenient file synchronization, sharing, and backup capabilities.
- Web-based Applications: Many software applications are now delivered as web-based services, accessible through web browsers. Examples include Google Docs (word processing, spreadsheets, presentations), Salesforce (customer relationship management), and Trello (project management).
- Communication and Collaboration Tools: Cloud-based tools facilitate communication and collaboration among individuals and teams. Examples include Slack (team messaging), Microsoft Teams, and Zoom (video conferencing).
- Cloud-based Development Platforms: Platforms like GitHub and GitLab provide cloud-based repositories for version control and collaboration on software development projects. Developers can collaborate, track changes, and manage code repositories without the need for local infrastructure.
- Cloud-based Database Services: Services like Amazon RDS(Relational Database Service), Google Cloud Spanner, and Microsoft Azure SQL (Structured Query Language) Database offer cloud-based database

solutions. These services provide scalable, managed database environments, reducing the need for organizations to manage and maintain their database infrastructure.

- Software as a Service (SaaS) Applications: SaaS applications are fully functional cloud-based software solutions that users can access and use over the internet. Examples include customer relationship management (CRM) systems like Salesforce, project management tools like Asana, and human resources management systems like Workday.
- Cloud-based Analytics and Big Data Services: Cloud platforms offer services for data analytics, processing, and storage. Examples include Amazon Redshift, Google BigQuery, and Microsoft Azure Analytics. These services enable organizations to process large volumes of data and derive insights without investing in on-premises infrastructure.
- Cloud-based Backup and Disaster Recovery: Cloud-based backup and disaster recovery services, such as Carbonite, Acronis, and Druva, provide organizations with secure and scalable backup and recovery solutions. Data is stored in the cloud, offering data redundancy and protection against data loss or system failures.

IOT(Internet Of Things)

IoT stands for the Internet of Things. It refers to a network of interconnected physical devices, vehicles, buildings, and other objects embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. The concept behind IoT is to enable these objects to communicate and interact with each other and with users, creating a smart and interconnected ecosystem.

In IoT, everyday objects can be transformed into "smart" devices by connecting them to the internet, allowing them to gather data, receive instructions, and perform various tasks. These objects can include anything from household appliances and wearable devices to industrial machinery and infrastructure systems.

The data collected by IoT devices can be analyzed and processed to derive insights, enable automation, enhance decision-making, and improve efficiency across different sectors such as healthcare, transportation, manufacturing, agriculture, and more. IoT has the potential to revolutionize industries, enhance quality of life, and drive innovation in numerous applications and domains.

Some key characteristics and benefits of IoT include:

- Connectivity: IoT devices are connected to the internet, enabling seamless communication and data exchange.
- Sensing and Data Collection: IoT devices use sensors to gather data about their environment, such as temperature, humidity, motion, or location.
- Data Analysis and Insights: The collected data can be analyzed to extract meaningful insights, patterns, and trends, enabling informed decision-making.
- Automation and Control: IoT enables automation of processes, allowing devices to respond to data inputs and trigger actions without human intervention.
- Efficiency and Optimization: IoT can optimize resource usage, streamline operations, and improve efficiency in various domains, leading to cost savings and improved productivity.
- Enhanced User Experience: IoT devices can provide personalized experiences, real-time information, and convenient services to users.
- Safety and Monitoring: IoT can enhance safety by monitoring and alerting about potential risks or anomalies in real time.

Examples in different sectors:

1. Healthcare:

- Wearable devices such as fitness trackers and smart watches collect health data like heart rate, sleep patterns, and activity levels, allowing individuals to monitor their well-being.
- IoT-enabled medical devices like remote patient monitoring systems enable healthcare providers to monitor patients' vital signs and health conditions from a distance.
- Smart pill bottles and medication dispensers help track medication adherence and send reminders to patients.

2. Transportation:

- Connected cars use IoT to gather real-time data about the vehicle's performance, location, and driving behavior. This information can be used for maintenance, fuel efficiency, and navigation purposes.
- Smart traffic management systems leverage IoT to monitor traffic flow, optimize signal timings, and manage congestion.
- Logistics and fleet management companies use IoT to track shipments, monitor vehicle conditions, and optimize routes for efficient delivery.

3. Manufacturing:

- Industrial IoT (IIoT) is used to monitor and optimize manufacturing processes, equipment performance, and supply chain operations.
- IoT sensors on machines and assembly lines collect data on production metrics, allowing for predictive maintenance and minimizing downtime.
- Asset tracking systems use IoT to monitor inventory, locate goods, and streamline logistics within manufacturing facilities.

4. Agriculture:

- IoT-enabled smart irrigation systems monitor soil moisture levels and weather conditions to optimize water usage in agriculture.
- Connected sensors provide real-time data on crop health, enabling farmers to make informed decisions about fertilizer application, pest control, and harvesting.
- Livestock monitoring devices equipped with IoT sensors track animal health, location, and behavior, helping farmers manage their herds effectively.

5. Smart Homes:

- IoT devices like smart thermostats, lighting systems, and security cameras allow homeowners to control and monitor their home remotely.
- Connected appliances, such as refrigerators and washing machines, can notify users about maintenance needs, energy consumption, or restocking supplies.
- Voice assistants like Amazon Echo or Google Home use IoT to connect and control various devices in a home through voice commands.

Applications of IOT and Sensors:

Smart Cities:

- IoT and sensor technologies are used to create more efficient and sustainable cities.
- Smart parking systems use sensors to detect available parking spaces, guiding drivers to empty spots and reducing congestion.
- Waste management systems utilize sensors to optimize garbage collection routes, minimizing costs and improving efficiency.
- Environmental monitoring sensors measure air quality, noise levels, and other factors to enable better urban planning and resource allocation.

Healthcare:

- Remote patient monitoring systems employ wearable sensors to collect real-time health data, allowing healthcare providers to monitor patients' conditions remotely and provide timely interventions.
- Smart pill dispensers can track medication adherence and send alerts or reminders to patients.
- IoT-enabled medical devices like insulin pumps or pacemakers provide real-time data and alerts to healthcare professionals for better patient management.

Industrial Automation:

- Industrial IoT (IIoT) and sensors enable real-time monitoring and control of manufacturing processes, improving efficiency and reducing downtime.
- Sensors placed on machinery detect anomalies, allowing predictive maintenance to prevent breakdowns and optimize maintenance schedules.
- Inventory management systems use sensors to track and manage stock levels, reducing waste and ensuring timely restocking.

Agriculture:

- Soil moisture sensors and weather stations help optimize irrigation by providing data on soil conditions and weather patterns.
- Crop monitoring sensors collect data on temperature, humidity, and light levels, enabling farmers to make informed decisions about planting, fertilizing, and harvesting.
- Livestock monitoring sensors track animal health, location, and behavior, assisting farmers in managing their herds effectively.

Environmental Monitoring:

- IoT sensors monitor and collect data on air quality, water quality, noise levels, and other environmental factors, helping identify pollution sources and implement mitigation measures.
- Weather stations equipped with sensors provide real-time weather data, aiding in forecasting and disaster management.

Energy Management:

- Smart meters track energy consumption patterns and enable demand response programs, optimizing energy usage and reducing costs.
- Building management systems utilize sensors to monitor occupancy, temperature, and lighting levels, optimizing energy efficiency in commercial and residential buildings.

Retail:

- IoT sensors and beacons track customer movement and behavior in stores, allowing retailers to analyze data and optimize store layouts and product placements.
- Smart shelves equipped with sensors can monitor inventory levels and send notifications for restocking.

Overview of IOT

- Internet of Things is the network of physical objects or ‘things’ embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

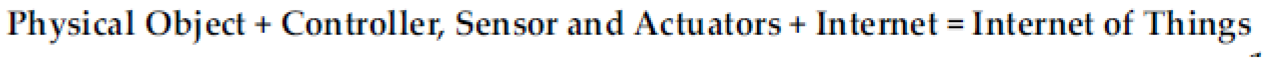
- The concept of IoT began with things classified as identity communication devices. Radio Frequency Identification Device (RFID) is an example of an identity communication device.

- Things are tagged to these devices for their identification in future and can be tracked, controlled and monitored using remote computers connected through the Internet.
- Other examples: GPS-based tracking, controlling and monitoring of devices; machine-to-machine (M2M) communication; connected cars; communication between wearable and personal devices and Industry 4.0.
- The IoT concept has made smart cities a reality and is also made self-driving cars functional.

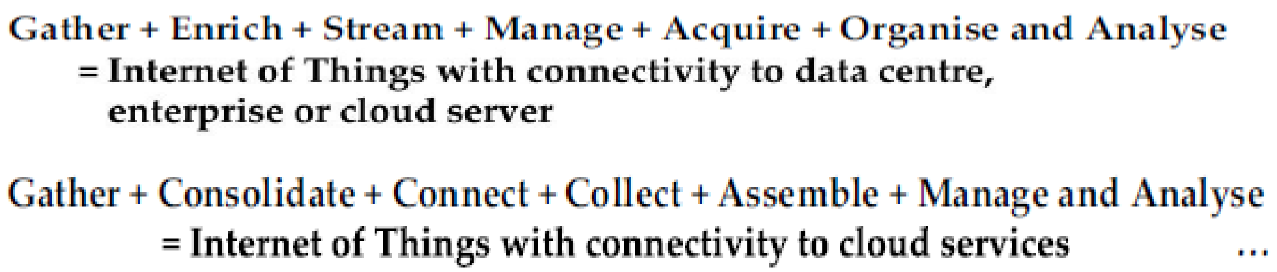
Technology behind IoT:

- Hardware (Arduino Raspberry Pi, Intel Galileo, Intel Edison, ARM mBed, Bosch XDK110, Beagle Bone Black and Wireless SoC)
- Integrated Development Environment (IDE) for developing device software, firmware and APIs(Application Programming Interface)
- Protocols [RPL, CoAP, RESTful HTTP, MQTT, XMPP (Extensible Messaging and Presence Protocol)]
- Communication (Powerline Ethernet, RFID, NFC, 6LowPAN, UWB, ZigBee, Bluetooth, WiFi, WiMax, 2G/3G/4G/5G)
- Network backbone (IPv4, IPv6, UDP and 6LowPAN)
- Software (RIOT OS, Contiki OS, Thingsquare Mist firmware, Eclipse IoT, Things speak)
- Internetwork Cloud Platforms/Data Centre (Sense, ThingWorx, Nimbits, Xively, openHAB, AWS IoT, IBM BlueMix, CISCO IoT, IOx and Fog, EvryThng, Azure, TCS CUP)
- Machine learning algorithms and software.

IOT reference model

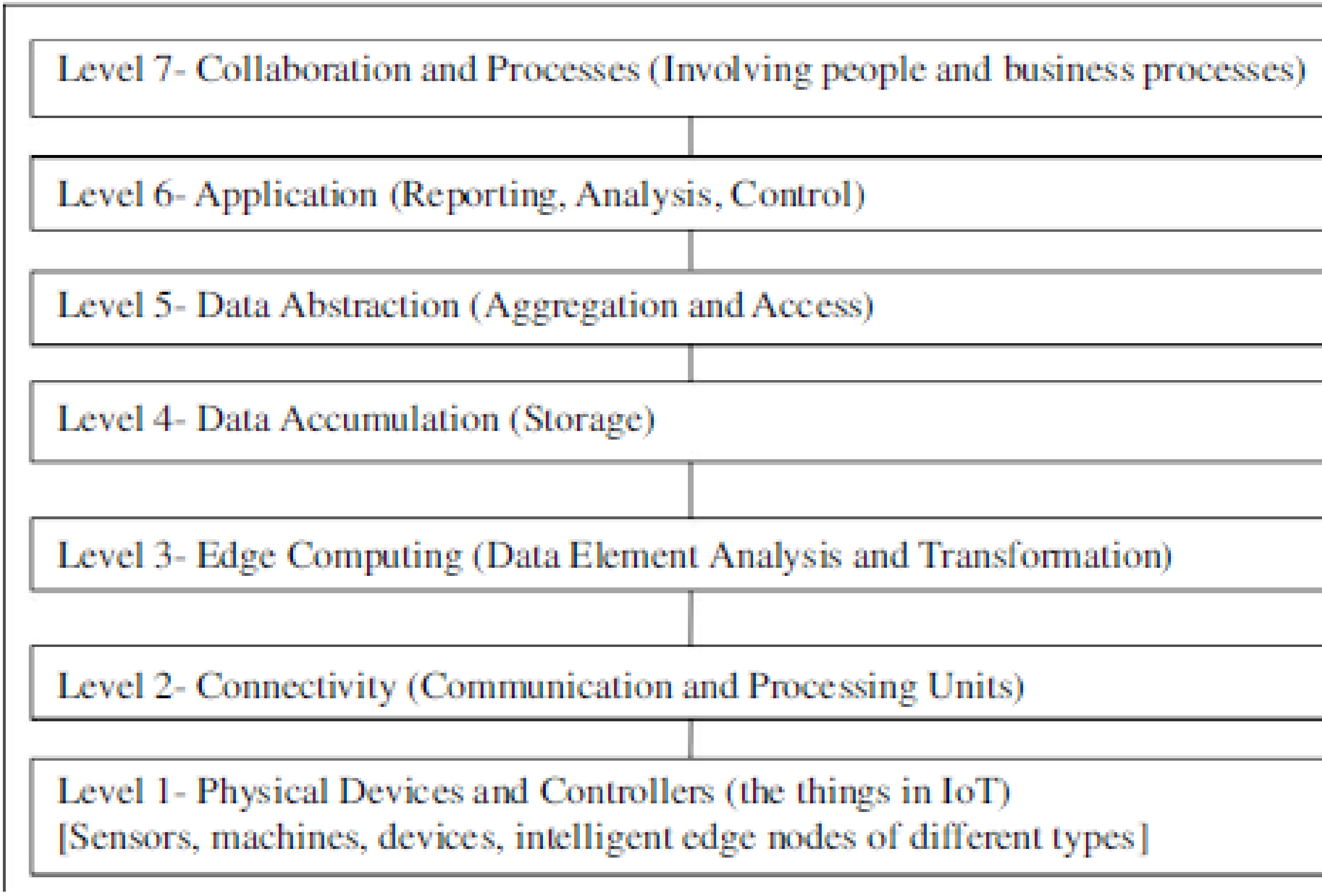


Physical Object + Controller, Sensor and Actuators + Internet = Internet of Things



Gather + Enrich + Stream + Manage + Acquire + Organise and Analyse
= Internet of Things with connectivity to data centre, enterprise or cloud server

Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyse
= Internet of Things with connectivity to cloud services …



Level 7- Collaboration and Processes (Involving people and business processes)

Level 6- Application (Reporting, Analysis, Control)

Level 5- Data Abstraction (Aggregation and Access)

Level 4- Data Accumulation (Storage)

Level 3- Edge Computing (Data Element Analysis and Transformation)

Level 2- Connectivity (Communication and Processing Units)

Level 1- Physical Devices and Controllers (the things in IoT)
[Sensors, machines, devices, intelligent edge nodes of different types]

IOT reference model

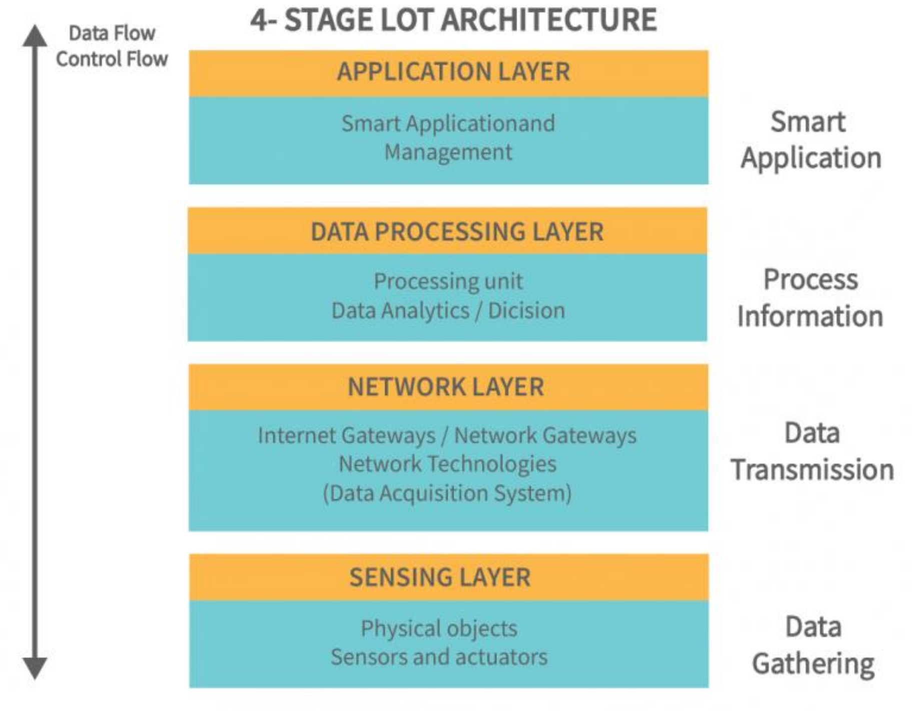
- Sensors: There’s virtually no end to the type of sensor that may be required for various projects, the choices are wide open.
- Network: The primary job of any network is to transfer data, route data traffic and manage throughput.
- Edge: check the data as it comes across and acts upon it where defined.
- Storage: The Cloud is often assumed with IoT projects, but sometimes it should be on premises.

- Data abstraction: collects different data pieces and makes them available for analysis.
- Application: identify which results are reactive, proactive and predictive.

- Reactive risk management is the most basic approach. It involves identifying and responding to risks after they have already occurred. This approach is often used when there is not enough information to identify and mitigate risks before they occur.
- Proactive risk management is a more proactive approach. It involves identifying and mitigating risks before they occur. This approach is often used when there is enough information to identify and assess risks.
- Predictive risk management is the most advanced approach. It involves using data and analytics to anticipate future risks. This approach is often used when there is a lot of data available and when it is important to identify and mitigate risks as early as possible.

- Collaboration and process: the groups that could benefit from the data and services of IoT.

IOT architecture



- Sensing layer: Things (sensors & actuators) or endpoint devices are capable of collecting, accepting, and processing data over the network.

- Network layer: contains Data Acquiring Systems (DAS) ((collecting and aggregating data from sensors, then converting analog data to digital data, etc.) and Internet/Network gateways.
- Processing layer: brain of IoT. data is analyzed, pre-processed, and stored then sent to the data center, accessed by software applications,
- Application layer: User interaction takes place at the application layer, which delivers application-specific services to the user.

The things in IOT: Sensors and Actuators

Sensors:

- A sensor is a device (typically electronic) that detects events or changes in its physical environment (e.g., temperature, sound, heat, pressure, flow, magnetism, motion, chemical and biochemical parameters) and provides a corresponding output.
- Most sensors take analog inputs and deliver digital, often electrical, outputs.
- Sensors are comparable to the human five senses.
- Sensors typically collect data using physical interfaces (inputs) that sense the environment and then convert input signals into electrical signals (outputs) that are understood by the communication and computing devices.
- Output signals are then processed by the gateways and/or by applications of the IoT Platform.

Types of Sensors:

- Temperature sensors: A temperature sensor is an electronic device that measures the temperature of its environment and converts the input data into electronic data to record, monitor, or signal temperature changes, Ex:Thermocouples, Resistance temperature detectors, Thermistors and semi conductor sensor.

- Pressure sensors: measure the pressure of gases or liquids including water level, flow, speed, and altitude. Applications – pressure transducers are used for measuring oil, fuel and brake pressure.
- Flow sensors: to detect and record the rate of fluid flow in a pipe.
- Level sensors: to measure the level of fluids continuously or at point values.
- Imaging sensors: used in digital cameras, medical imaging machines, and night vision equipment.
- Noise sensors: to detect noise pollution.
- Air pollution sensors: to monitor air pollution.
- Proximity & Displacement sensors: presence of objects using EM, light or sound.
- Infrared sensors: heat based motion monitoring.
- Moisture and humidity: hygrometer sensors-humidity in air.
- Speed sensor: speed of vehicles. Eg: wheel speed sensors, speedometers, Doppler radar, and laser surface velocimeter.

Sensor fundamentals and characteristics –Principles of sensing- capacitance - magnetic and electromagnetic induction – resistance - piezoelectric effect – heat transfer-light.

Principles of Sensing:

- Sensors detect and respond to physical, chemical, or biological changes in their environment.
- They convert the measured quantity into an electrical signal for further processing and analysis.
- The principles of sensing vary depending on the type of sensor and the phenomenon being measured.

Capacitance:

- Capacitive sensors measure changes in capacitance to detect the presence, proximity, or position of objects.

- They work based on the principle that the capacitance between two conductive surfaces changes when an object comes in proximity or makes contact with them.
- Capacitive sensors are commonly used in touchscreens, level sensors, and proximity sensors.

Magnetic and Electromagnetic Induction:

- Magnetic sensors detect magnetic fields and their changes.
- They utilize the principle of electromagnetic induction, where the interaction between a magnetic field and a conductor induces a voltage or current in the conductor.
- Magnetic sensors are used in applications such as compasses, position sensors, and magnetic encoders.

Resistance:

- Resistance-based sensors rely on changes in electrical resistance to measure various quantities.
- For example, temperature sensors, such as thermistors or RTDs (Resistance Temperature Detectors), utilize the change in resistance with temperature to measure temperature.
- Strain gauges measure mechanical strain by detecting changes in resistance caused by stretching or compression.

Piezoelectric Effect:

- Piezoelectric sensors generate an electrical charge when subjected to mechanical stress or pressure.
- They work based on the piezoelectric effect, where certain materials (e.g., quartz, ceramics) produce an electric charge in response to applied mechanical stress.
- Piezoelectric sensors are used in applications such as vibration sensing, pressure sensing, and acoustic sensing.

Heat Transfer:

- Heat transfer sensors measure temperature variations through various principles like thermal expansion, thermocouples, or infrared radiation.
- Thermal expansion-based sensors use the expansion or contraction of materials with temperature changes to measure temperature.
- Thermocouples utilize the Seebeck effect, where a voltage is generated when two dissimilar metals are connected at different temperatures.
- Infrared sensors detect the thermal radiation emitted by objects to measure their temperature remotely.

Light:

- Light sensors, such as photodiodes or phototransistors, detect and measure light intensity or changes in light levels.
- They operate by converting incident light energy into an electrical current.
- Light sensors find applications in ambient light sensing, proximity detection, and optical communication.

There are four types of temperature sensors:

1. Thermocouples: Thermocouples are the most common type of temperature sensor. They are made of two different metals, and the voltage generated by the Seebeck effect is proportional to the temperature difference between the two junctions of the thermocouple. Thermocouples are used in a wide variety of applications, including industrial process control, medical diagnostics, and environmental monitoring.

2. Resistance Temperature Detectors (RTDs): RTDs are made of a material whose resistance changes with temperature. The resistance of an RTD is measured by a Wheatstone bridge, and the temperature is calculated from the resistance. RTDs are more accurate than thermocouples, but they are also more expensive.

3. Thermistors: Thermistors are made of a semiconductor material whose resistance changes rapidly with temperature. Thermistors are less accurate than RTDs, but they are also less expensive. Thermistors are often used in applications where accuracy is not critical, such as home thermostats.

4. Semiconductor-Based Sensors: Semiconductor-based sensors are made of a semiconductor material whose electrical properties change with temperature. Semiconductor-based sensors are the most accurate type of temperature sensor, but they are also the most expensive. Semiconductor-based sensors are often used in applications where accuracy is critical, such as medical diagnostics and scientific research.

Classification of light sensors:

1. Photoresistors are the simplest type of light sensor. They are made of a semiconductor material that changes its resistance when exposed to light. Photoresistors are often used in simple light detection applications, such as light switches and burglar alarms.
2. Photodiodes are a type of semiconductor device that converts light into an electrical current. Photodiodes are more sensitive than photoresistors and can be used in a wider range of applications, such as cameras, solar cells, and light meters.
3. Phototransistors are a type of transistor that uses light to control its output current. Phototransistors are more sensitive than photodiodes and can be used in a wider range of applications, such as proximity sensors, light switches, and optical communication devices.
4. Photovoltaic cells are a type of semiconductor device that converts light directly into electrical energy. Photovoltaic cells are used in solar cells to generate electricity from sunlight.

Characteristics of Sensors:

- Data Filtering

- Minimum Power Consumption
- Compact
- Smart detection
- High sensitivity: small change in o/p to i/p.
- Linearity: o/p to i/p linear relation.
- Dynamic range: range of signals converted to electrical signals by sensor.
- Accuracy: maximum expected error b/w measured and ideal.
- Hysterisis: sensor does not return the same output value when the input stimulus is driven up or down
- Limited noise: filter out noise
- Wide bandwidth: The bandwidth of a sensor is the frequency range between the instantaneous change to decay time.
- High resolution: smallest detectable signal fluctuation.
- Minimum interruption
- Higher reliability
- Ease of use

Actuators:

- Actuators are devices or components that convert input signals or energy into physical motion or action. They are commonly used in various systems and machines to control or manipulate physical processes.
- Actuators use sensor-collected and analyzed data as well as other types of data intelligence to control IoT systems.

Types of Actuators:

- **Electrical Actuators:** Electric actuators use electrical energy to generate motion.

Example: DC Motor

Application: Robotic arm movement in industrial automation, electric vehicle propulsion, printer head positioning.

- **Mechanical Linear Actuators:** Mechanical actuators convert rotary motion into linear motion or vice versa..

Example: Screw Jack

Application: Raising and lowering platforms, height adjustment mechanisms in furniture, positioning systems.

- **Hydraulic Actuators:** Hydraulic actuators utilize pressurized fluid, typically oil, to generate force and motion.

Example: Hydraulic Cylinder

Application: Construction machinery (e.g., excavators, cranes), hydraulic presses, heavy-duty lifting equipment.

Pneumatic actuators: Pneumatic actuators use compressed air or gas to generate motion.
Example: Pneumatic Cylinder
Application: Factory automation, pneumatic grippers for pick-and-place operations, air-powered tools.

Manual actuators: are operated by human effort.
Examples: Handwheel: A handwheel is a common type of manual actuator used for rotating or adjusting mechanisms. It typically consists of a circular wheel that can be turned by hand to provide rotational motion.
Examples:
Handwheels are often found in machinery, valves, and equipment that require manual control or adjustment.
Toggle Switch: A toggle switch is a manual actuator that controls the on/off state of an electrical circuit.

Push Button: A push button is a simple manual actuator that operates by pressing or releasing a button. It is commonly used in control panels, machinery, and appliances to initiate specific actions or functions.