SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

Internet of Things

BRANCH: Bachelor’s of Computer Application

SEMESTER: 5^{th}

PREPARED BY: Asst. Prof. Harshil Trivedi

AGENDA

Learning Objectives

Actual Content to be delivered

Summary of the what has been delivered in the lectures

CHAPTER-1

Introduction to Internet of Things:

LEARNING OBJECTIVES

- **Introduction to Internet of Things-**Understanding the basic concept of IoT: Learn what IoT is and its significance in today's world.
- **Evolution of IoT-**Tracing the development of IoT : Explore how IoT has evolved over time and its key milestones.
- **IoT Definition-**Defining IoT : Understand the formal definition of IoT and its various interpretations.
- **IoT Characteristics-**Identifying characteristics of IoT: Learn the main features that define IoT systems.
- **Key Components of IoT System-**Recognizing IoT components: Identify and understand the essential components that make up an IoT system, such as sensors, actuators, and connectivity.
- **Functioning of IoT System-**Explaining how IoT systems work: Understand the processes and interactions that enable IoT systems to function effectively.
- **M2M (Machine to Machine) and IoT-Differentiating between M2M and IoT**: Learn the differences and similarities between Machine to Machine communication and IoT.
- **End to End IoT Architecture-**Understanding IoT architecture: Learn about the comprehensive architecture of IoT systems from end to end, including all layers and components.
- **IoT Levels and Deployment Templates-**Exploring IoT levels and templates: Understand different levels of IoT deployment and standard templates used in IoT projects.
- **Advantages & Disadvantages of IoT-**Evaluating IoT pros and cons: Learn about the benefits and potential drawbacks of implementing IoT solutions.
- **Interdependencies of IoT and Cloud Computing-**Analyzing IoT and Cloud computing relationship: Understand how IoT and cloud computing are interdependent and how they work together to enhance IoT functionalities.

Evolution of IoT

1982 – Vending machine: The first glimpse of IoT emerged as a vending machine at Carnegie Mellon University was connected to the internet to report its inventory and status, paving the way for remote monitoring.

1990 – Toaster: Early IoT innovation saw a toaster connected to the internet, allowing users to control it remotely, foreshadowing the convenience of smart home devices.

1999 – IoT Coined (Kevin Ashton): Kevin Ashton coined the term “Internet of Things” to describe the interconnected network of devices communicating and sharing data, laying the foundation for a new era of connectivity.

2000 – LG Smart Fridge: The LG Smart Fridge marked a breakthrough, enabling users to check and manage refrigerator contents remotely, showcasing the potential of IoT in daily life.

2004 – Smart Watch: The advent of smartwatches introduced IoT to the wearable tech realm, offering fitness tracking and notifications on-the-go.

2007 – Smart iPhone: Apple’s iPhone became a game-changer, integrating IoT capabilities with apps that connected users to a myriad of services and devices, transforming smartphones into hubs.

2009 – Car Testing: IoT entered the automotive industry, enhancing vehicles with sensors for real-time diagnostics, performance monitoring, and remote testing.

2011 – Smart TV: The introduction of Smart TVs brought IoT to the living room, enabling internet connectivity for streaming, app usage, and interactive content.

2013 – Google Lens: Google Lens showcased IoT’s potential in image recognition, allowing smartphones to provide information about objects in the physical world.

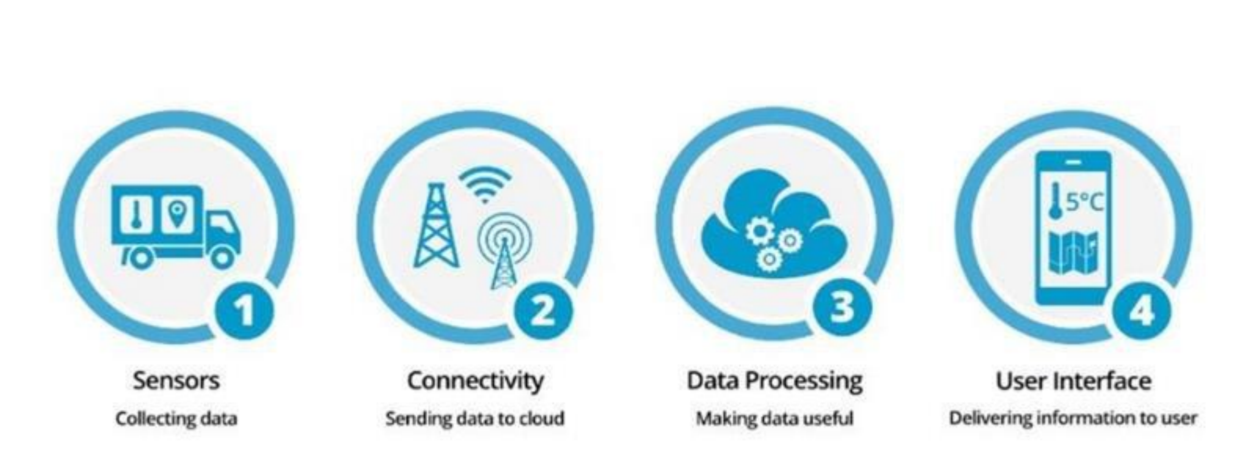
2014 – Echo: Amazon’s Echo, equipped with the virtual assistant Alexa, demonstrated the power of voice-activated IoT, making smart homes more intuitive and responsive.

2015 – Tesla Autopilot: Tesla’s Autopilot system exemplified IoT in automobiles, introducing semi-autonomous driving capabilities through interconnected sensors and software.

Definition of IOT

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the categorical examples where IoT is strongly established.

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



Characteristic of IOT

1. Connectivity

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, the connection between people through Internet devices like mobile phones, and other gadgets, also a connection between Internet devices such as routers, gateways, sensors, etc.

2. Intelligence and Identity

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3. Scalability

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4. Dynamic and Self-Adapting (Complexity)

IoT devices should dynamically adapt themselves to changing contexts and scenarios. Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, and night).

5. Architecture

IoT Architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ‘ products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6. Safety

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at risk. Therefore, equipment safety is also critical.

7. Self Configuring

This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

8. Interoperability

IoT devices use standardized protocols and technologies to ensure they can communicate with each other and other systems. Interoperability is one of the key characteristics of the Internet of Things (IoT). It refers to the ability of different IoT devices and systems to communicate and exchange data with each other, regardless of the underlying technology or manufacturer.

Interoperability is critical for the success of IoT, as it enables different devices and systems to work together seamlessly and provides a seamless user experience. Without interoperability, IoT systems would be limited to individual silos of data and devices, making it difficult to share information and create new services and applications.

To achieve interoperability, IoT devices, and systems use standardized communication protocols and data formats. These standards allow different devices to understand and process data in a consistent and reliable manner, enabling data to be exchanged between devices and systems regardless of the technology used.

Components of IOT

Things or Device

These are fitted with sensors and actuators. Sensors collect data from the environment and give to gateway where as actuators performs the action (as directed after processing of data).

Gateway

The sensors give data to Gateway and here some kind of pre-processing of data is even done. It also acts as a level of security for the network and for the transmitted data.

Cloud

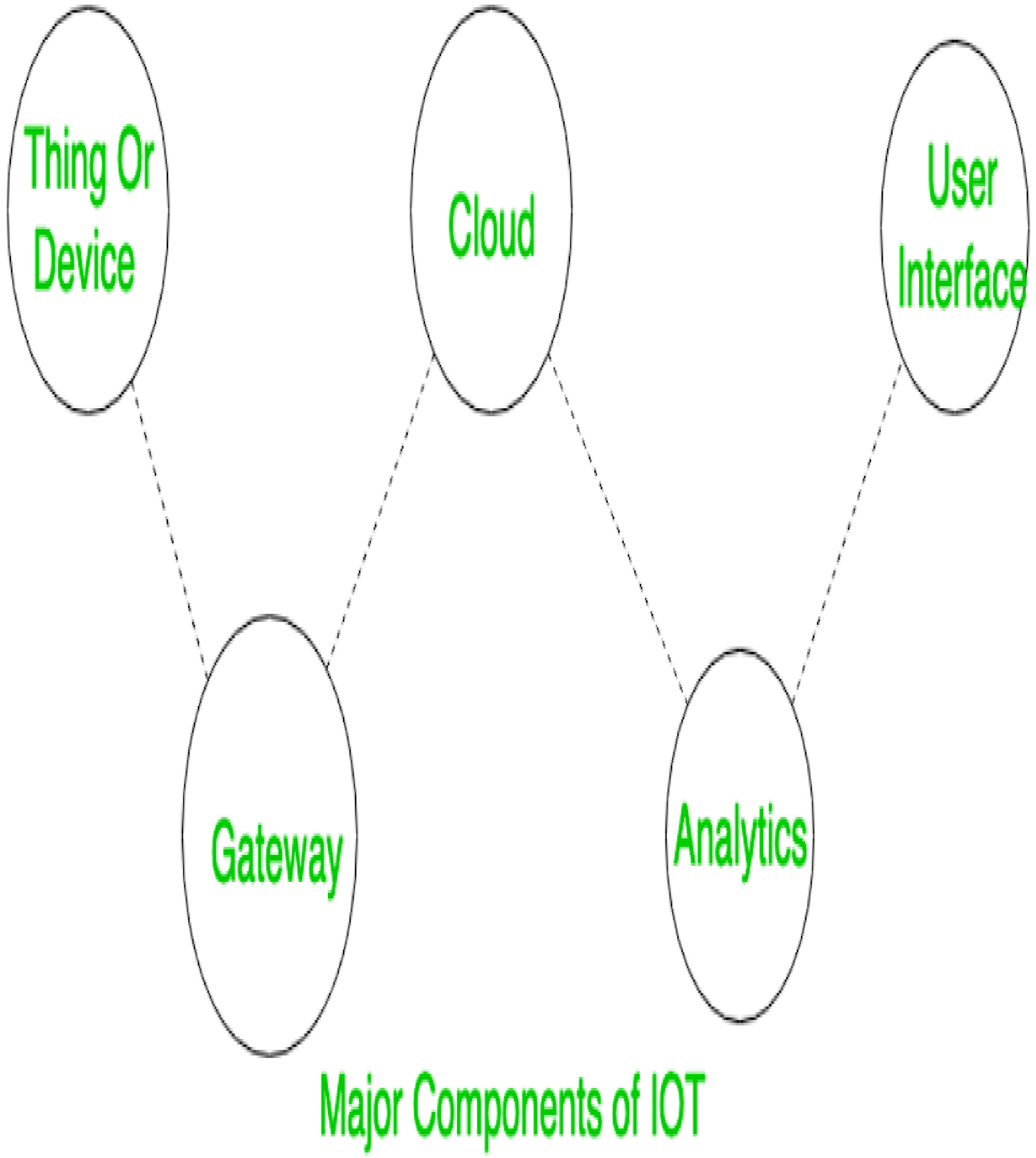
The data after being collected is uploaded to cloud. Cloud in simple terms is basically a set of servers connected to internet 24*7.

Analytics

The data after being received in the cloud processing is done . Various algorithms are applied here for proper analysis of data (techniques like Machine Learning etc are even applied).

User Interface

User end application where user can monitor or control the data.



FUNCTION OF IOT SYSTEM

1. **Data Collection**

Sensing the Environment

IoT devices are equipped with various sensors that gather data from the surrounding environment. Sensors such as temperature sensors, humidity sensors, motion sensors, and light sensors detect and measure specific physical parameters relevant to the device's purpose.

Capturing Real-time Information

IoT devices employ sensors such as accelerometers, gyroscopes, and cameras to capture real-time information about movement, orientation, and visual data. These sensors enable devices to understand their physical context and collect data for analysis.

2. **Data Transmission**

Wireless Communication

IoT devices utilize wireless communication protocols like Wi-Fi, Bluetooth, Zigbee, or cellular networks to transmit the collected data. These communication channels facilitate seamless and rapid data transfer between devices and networks.

Real-time Monitoring

By enabling real-time data transmission, IoT devices allow for continuous monitoring and analysis. This ensures that timely actions can be taken based on the received data, enabling efficient decision-making and responses to changing conditions.

3. **Data Processing and Analysis**

Local Processing

IoT devices often have built-in computing capabilities, allowing them to perform basic data processing and analysis tasks on the device itself. This local processing reduces the need for constant data transmission to external servers or cloud platforms, enabling quicker response times and reducing dependency on network connectivity.

Cloud-based Analysis

IoT devices can also send data to cloud-based platforms for more complex and extensive data processing and analysis. Cloud platforms provide the computational power and storage capacity necessary to handle large volumes of data.

Automation and Decision-making

IoT devices, with their data processing capabilities, can enable automation and intelligent decision-making. Based on predefined rules, algorithms, or machine learning models, IoT devices can autonomously respond to certain conditions or trigger actions, enhancing efficiency, productivity, and user experience.

M2M & IOT

Provide Remote Access- M2M and IOT provides remote access to information without human involvement

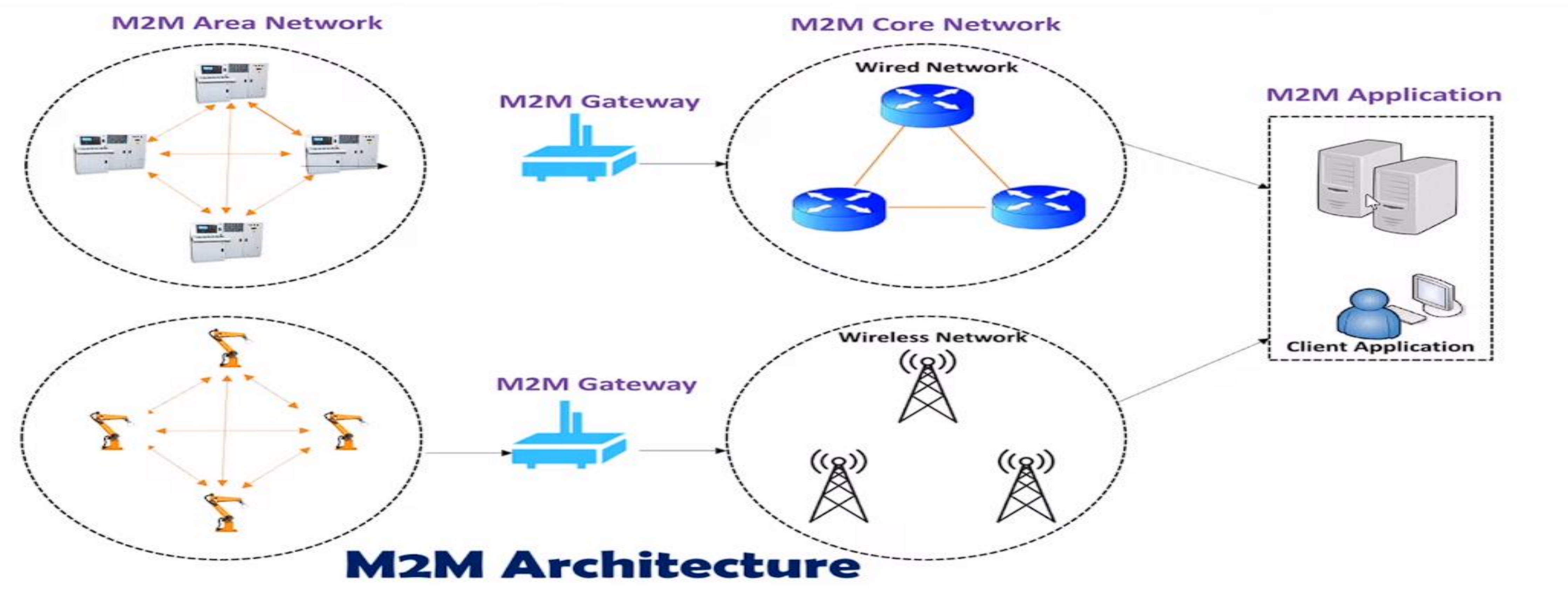
M2M- M2M provide direct communication between individual machines or devices. It is designed to communicate between machines for a specific purpose

IOT- It is broader concept for internet communication between devices. I involves a wide range of device,sensor,actuator,and application that communication with internet

M2M use non IP based proprietary network and iot used broad network protocol based on IP

M2M Architecture

M2M architecture



M2M GATEWAY

SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

M2M gateway act as an intermediary between various devices and system in machine to machine setup

It provides the following functionalities

1.Connection Between Machines

2.Data Exchange between machine

3.Compatibility between different network

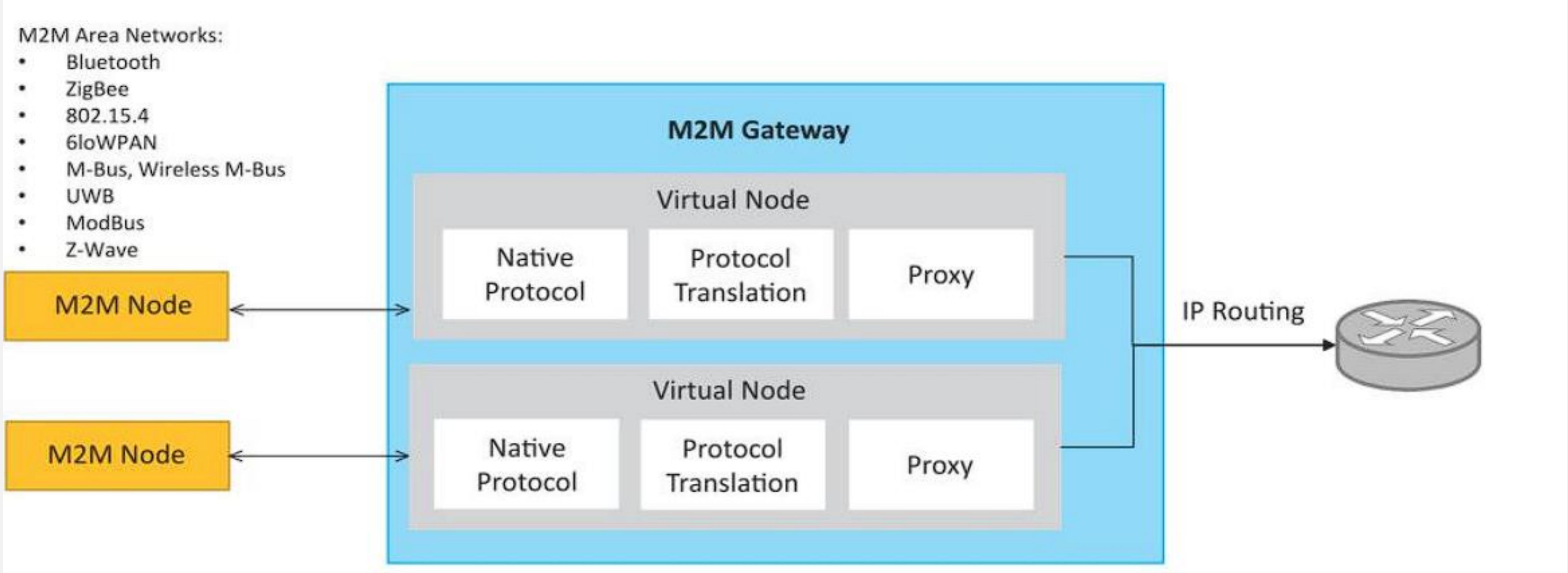
Purpose or Necessity-

Within the network nodes communication with each other

To communicate with remote M2M area network . M2M gateway is required

M2M GATEWAY

GATEWAY



Difference Between M2M & IOT

Main Differences between the IoT and M2M

IoT is a subset of M2M technology. In IoT, the communication between two machines without human instruction, making it a part of the M2M communication system.

The point-to-point communication of M2M is the main difference between M2M and IoT technology. Meanwhile, an IoT system usually locates its devices within a global cloud network that facilitates larger-scale automation and more advanced applications.

Another key difference between IoT and M2M is scalability. IoT is designed to be highly scalable because devices may also be included in the network and integrated into existing networks with minimal issues. In contrast, maintaining and setting up M2M networks could also be more labor-intensive, as new point-to-point connections must be built for each system.

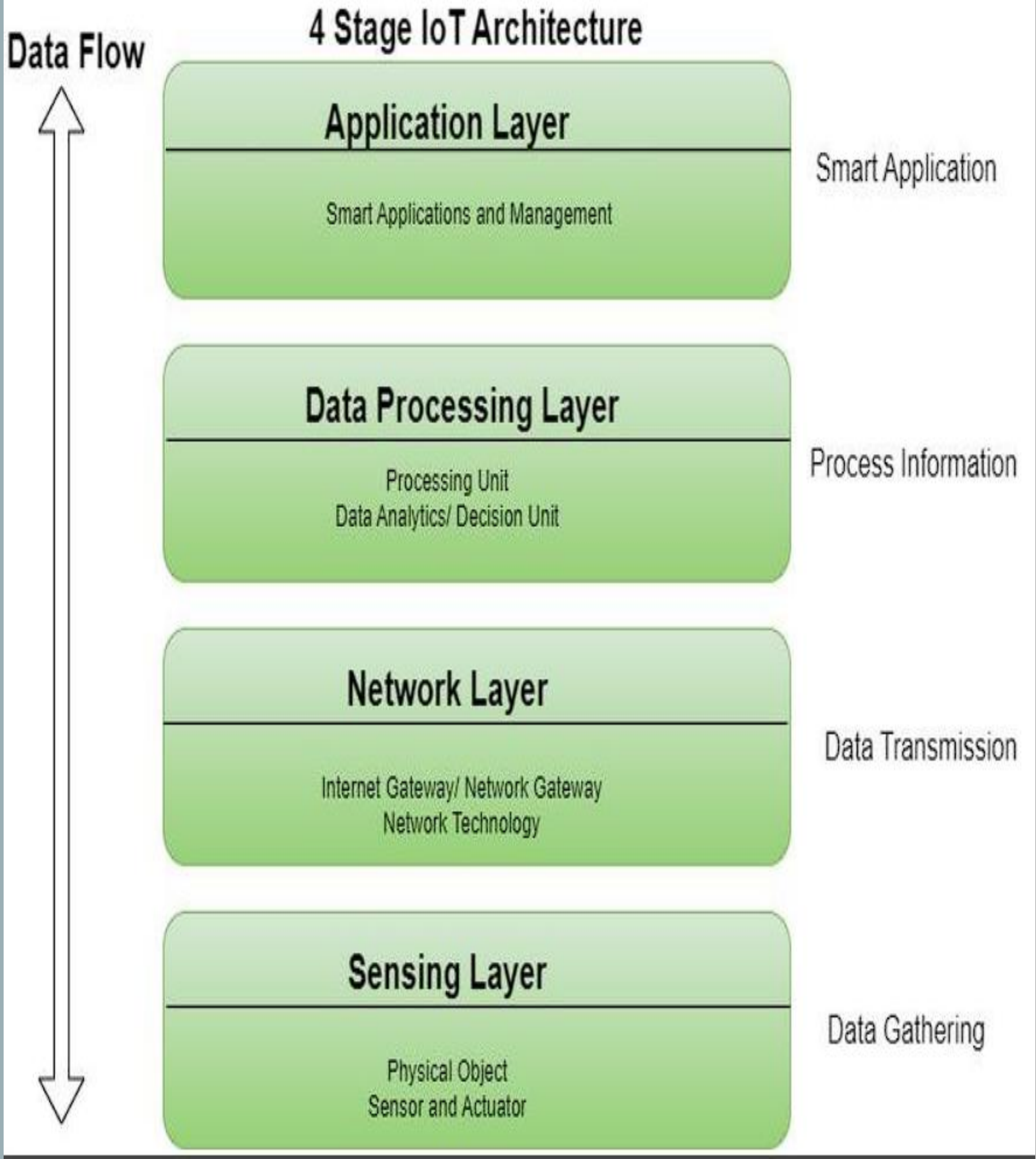
End to End Architecture of IOT

Sensing Layer: The sensing layer is the first layer of the Internet of Things architecture and is responsible for collecting data from different sources. This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters. Wired or wireless communication protocols connect these devices to the network layer.

Network Layer: The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system. It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet. Examples of network technologies that are commonly used in IoT include WiFi, Bluetooth,

Data processing Layer: The data processing layer of IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing, and interpreting data from IoT devices. This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action.The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms. These tools are used to extract meaningful insights from the data and make decisions based on that data. Example of a technology used in the data processing layer is a data lake, which is a centralized repository for storing raw data from IoT devices.

Application Layer: The application layer of IoT architecture is the topmost layer that interacts directly with the end-user. It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices.This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure. It also includes middleware services that allow different IoT devices and systems to communicate and share data seamlessly.The application layer also includes analytics and processing capabilities that allow data to be analyzed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities.



IoT levels and Deployment Templates

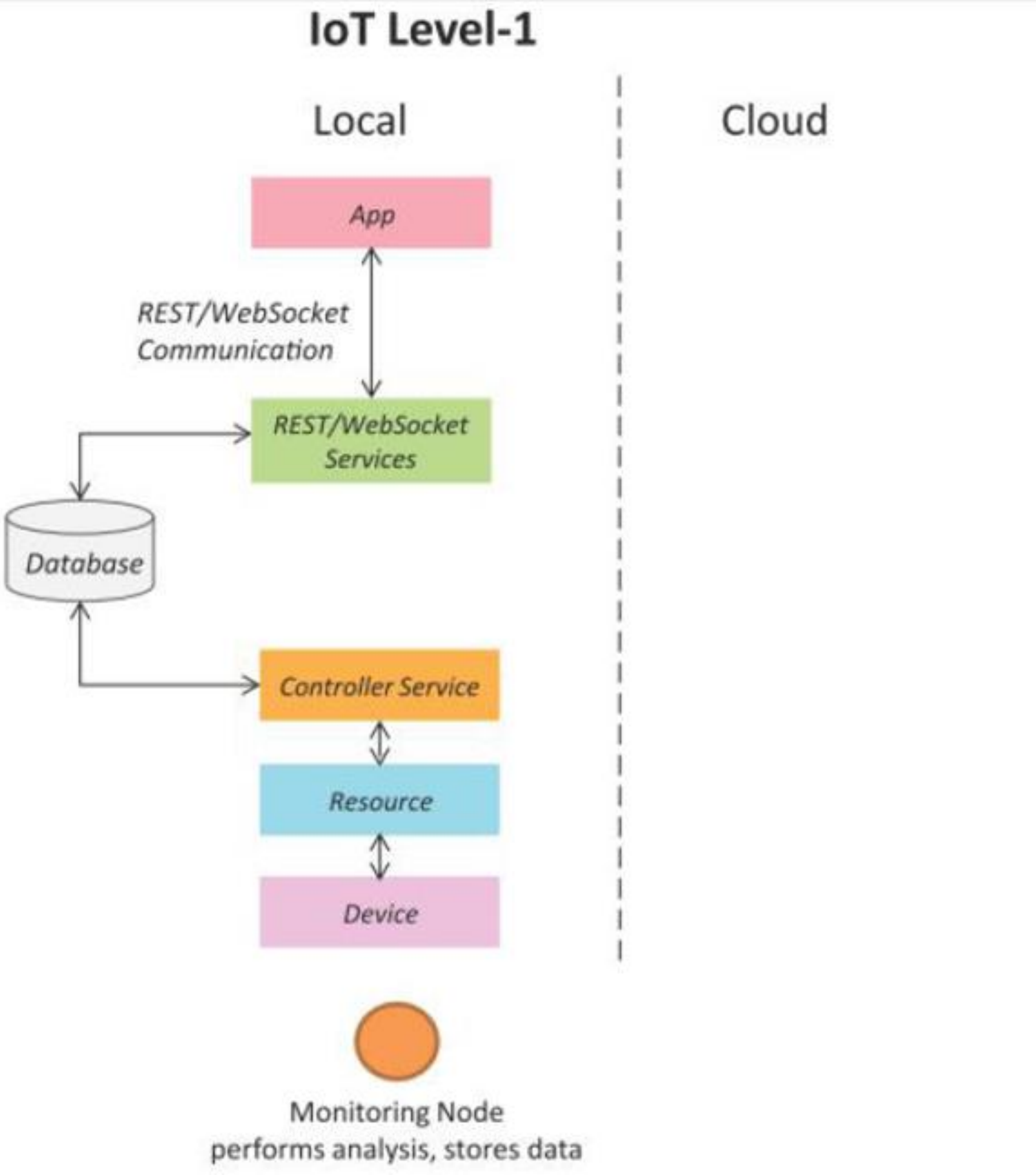
SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

Database: Database can be either local or in the cloud and stores the data generated by the IoT device.

- Web Service: Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
- Analysis Component: The Analysis Component is responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.
- Application: IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed data

IoT levels and Deployment Templates

- A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application
- Level-1 IoT systems are suitable for modeling lowcost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.

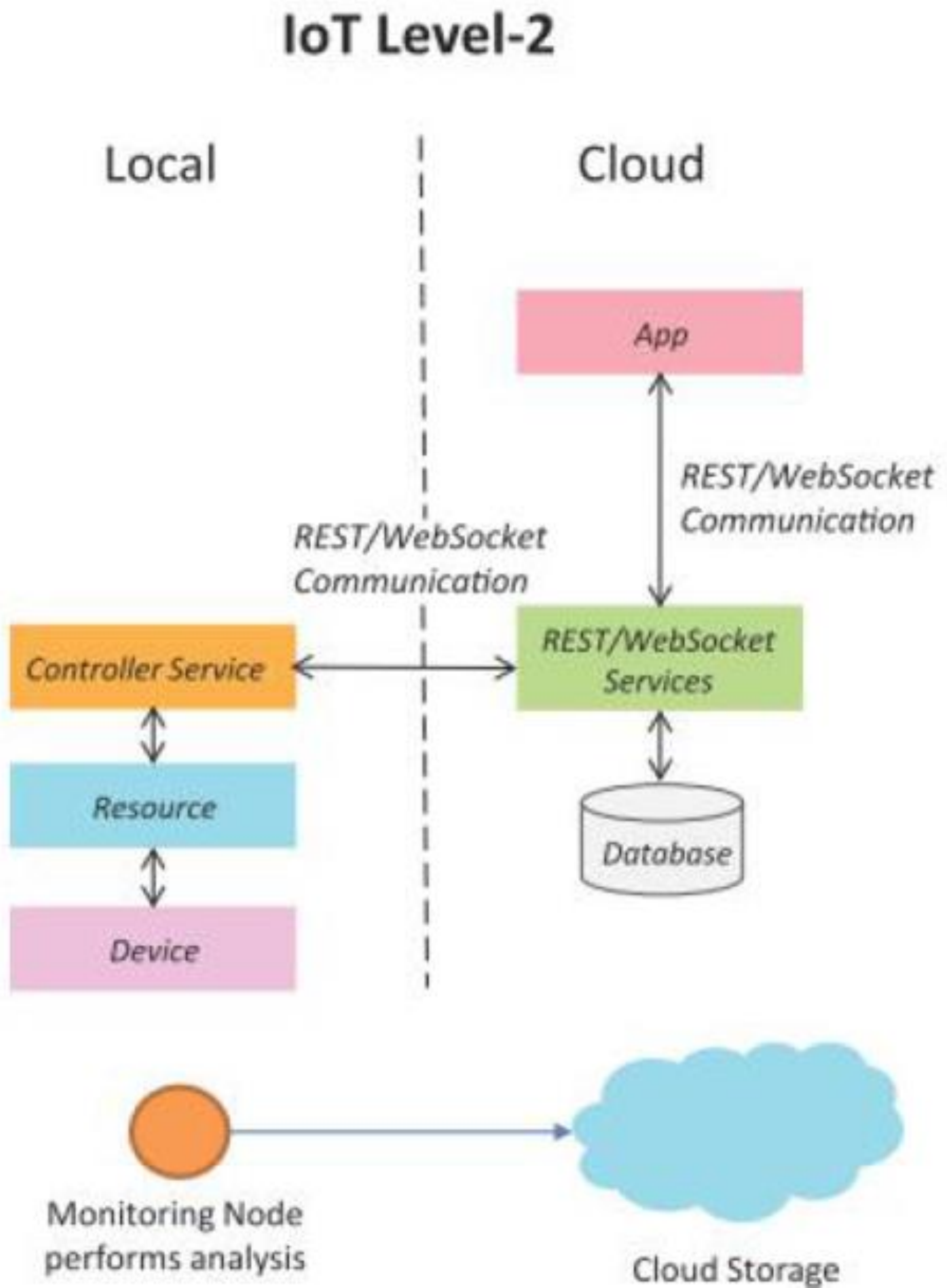


IOT LEVEL 2

A level-2 IoT system has a single node that performs sensing and/or actuation and local analysis.

• Data is stored in the cloud and application is usually cloudbased.

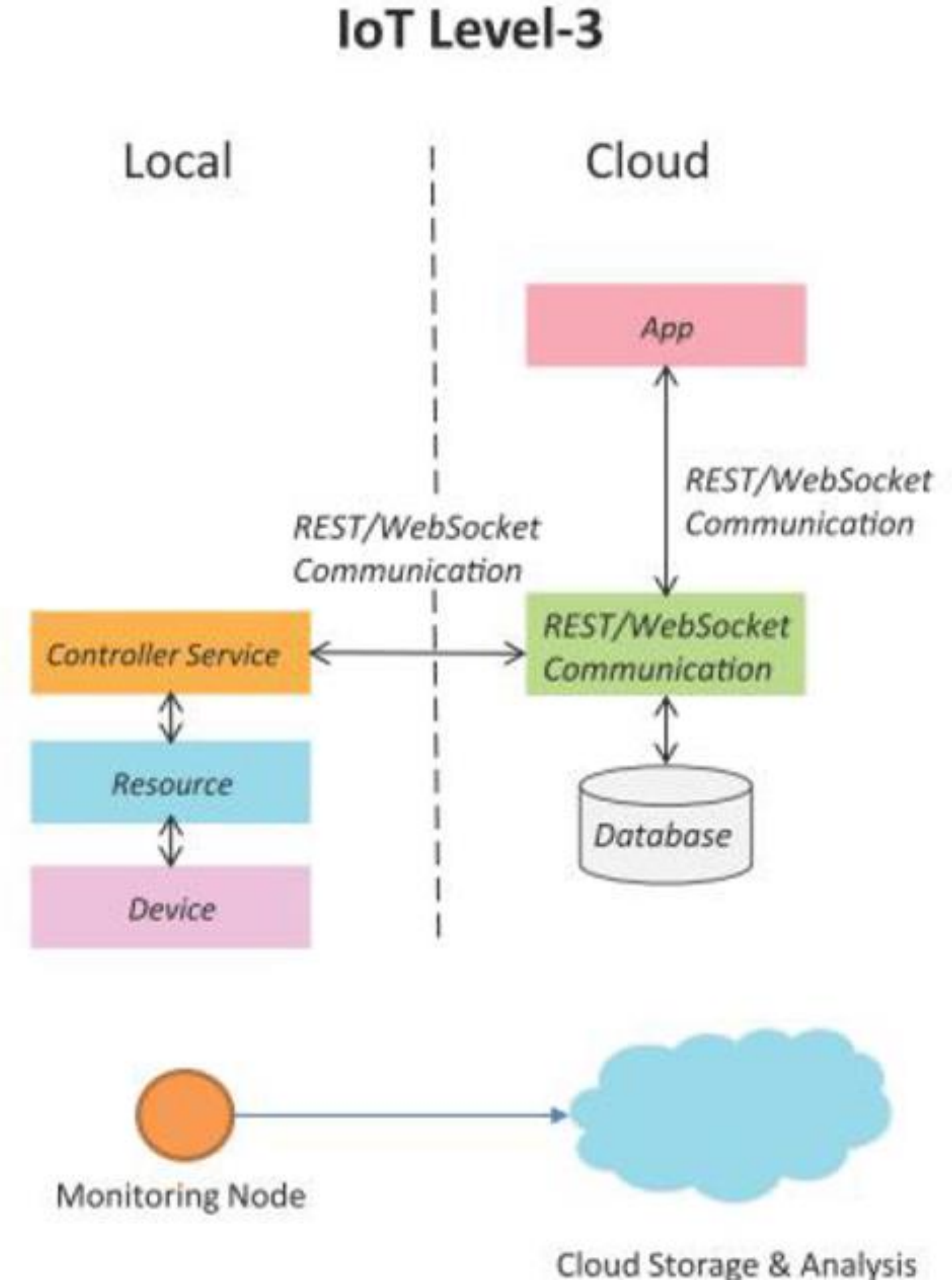
• Level-2 IoT systems are suitable for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.



IOT LEVEL 3

A level-3 IoT system has a single node. Data is stored and analyzed in the cloud and application is cloudbased.

• Level-3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive

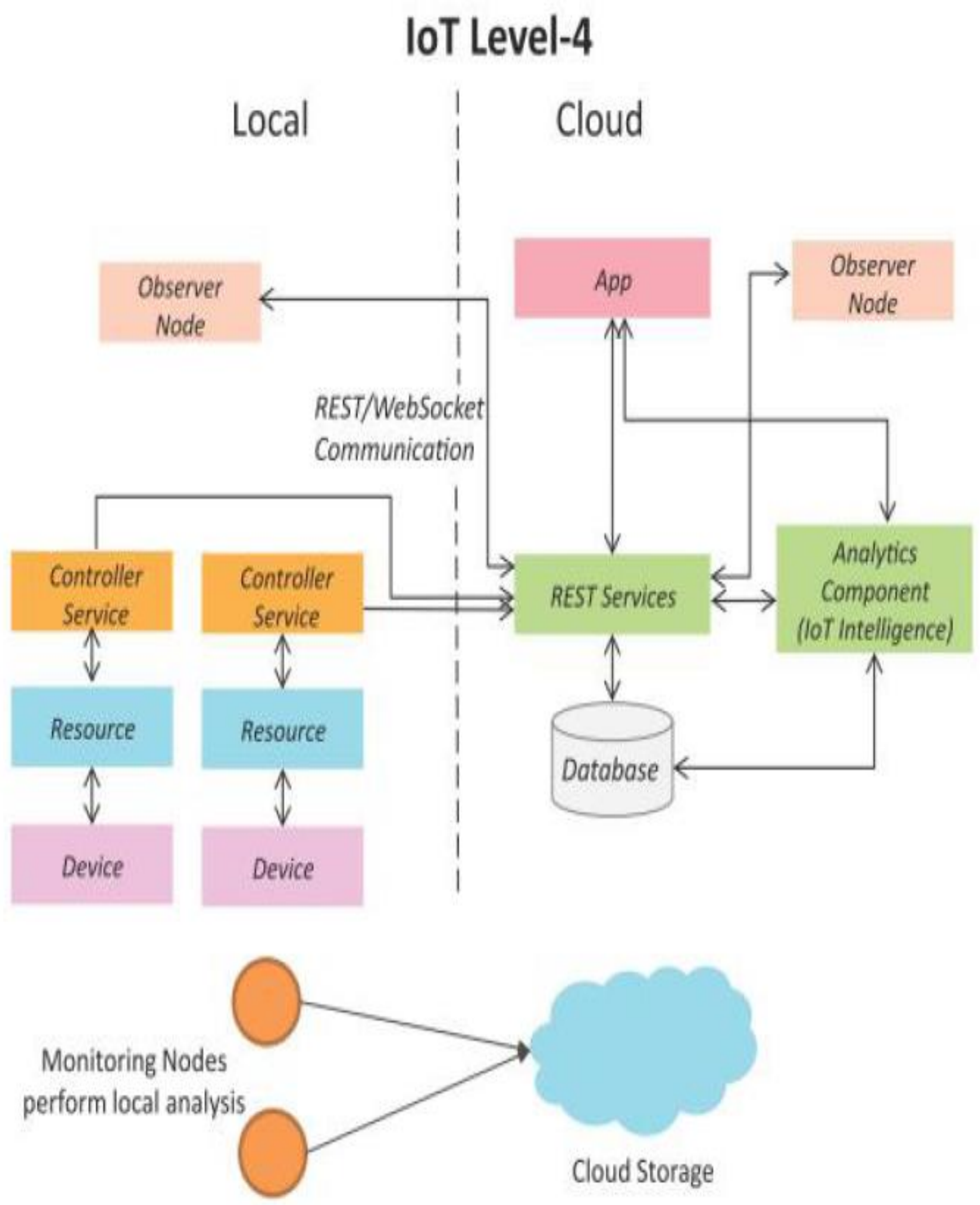


IOT LEVEL 4

A level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud-based.

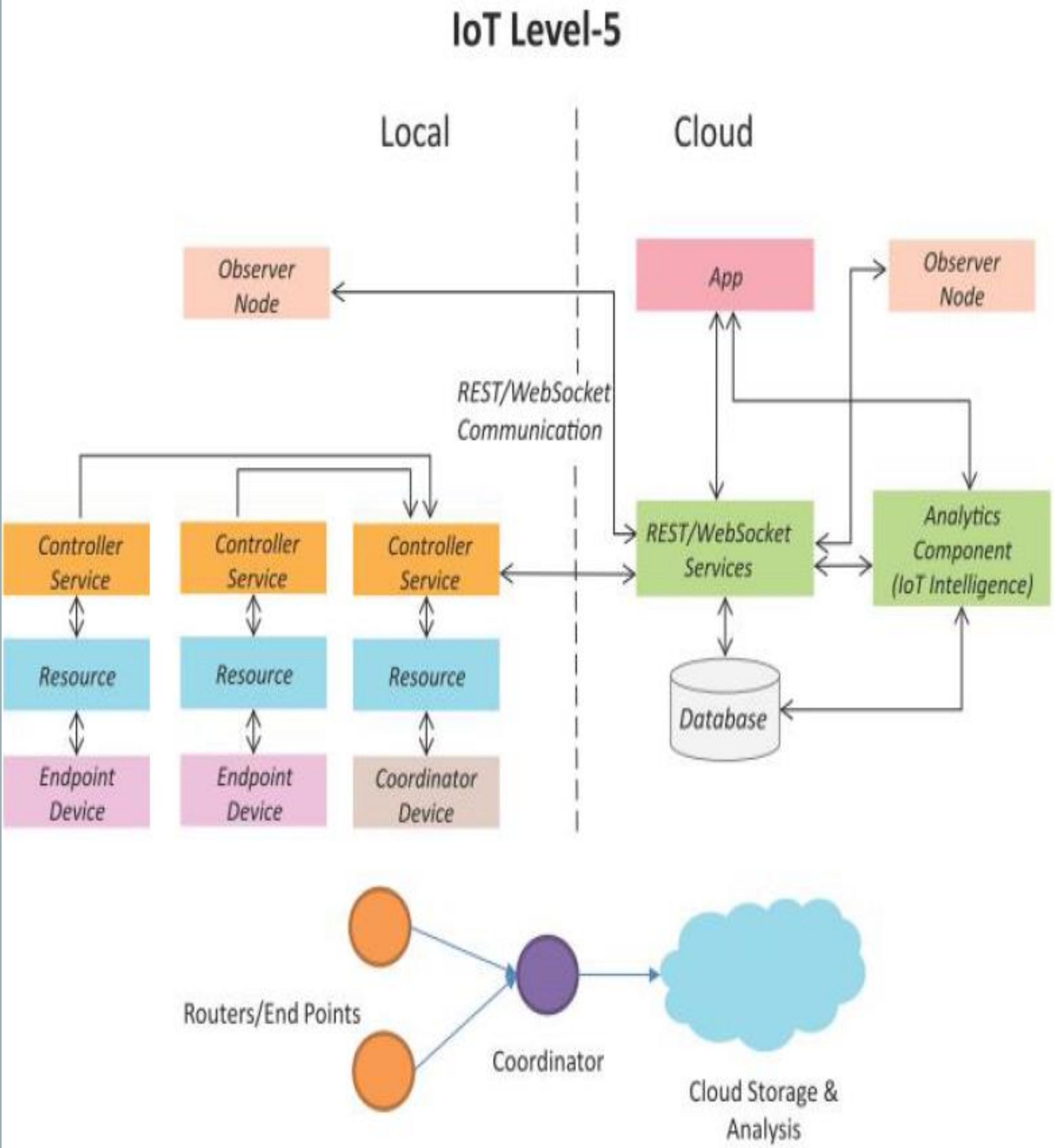
• Level-4 contains local and cloudbased observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.

• Level-4 IoT systems are suitable for solutions where multiple nodes are required, the data involved is big and the analysis requirements are computationally intensive.



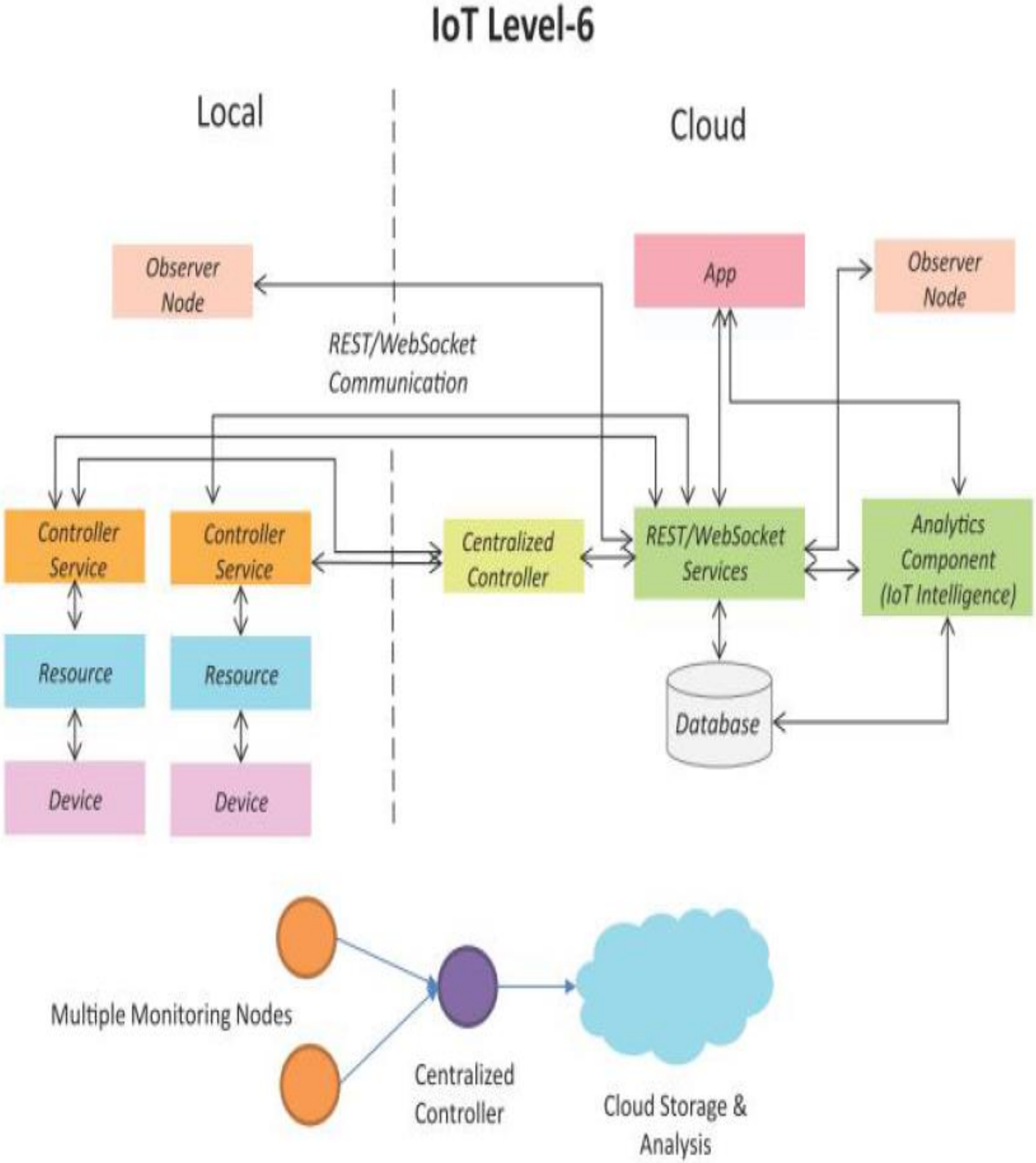
IOT LEVEL 5

- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes that perform sensing and/or actuation.
- Coordinator node collects data from the end nodes and sends to the cloud.
- Data is stored and analyzed in the cloud and application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.



IOT LEVEL 6

- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and application is cloud-based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.



ADVANTAGES OF IOT

It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.

By automating activities, it saves us a lot of time.

Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real time.

Electric Devices are directly connected and communicate with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.

Personal assistance can be provided by IoT apps, which can alert you to your regular plans.

It is useful for safety because it senses any potential danger and warns users. For example, GM OnStar, is a integrated device that system which identifies a car crash or accident on road. It immediately makes a call if an accident or crash is found.

It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.

Patient care can be performed more effectively in real time without the need for a doctor's visit. It gives them the ability to make choices as well as provide evidence-based care.

Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system.

DISADVANTAGES OF IOT

Hackers may gain access to the system and steal personal information. Since we add so many devices to the internet, there is a risk that our information as it can be misused.

They rely heavily on the internet and are unable to function effectively without it.

With the complexity of systems, there are many ways for them to fail.

We lose control of our lives—our lives will be fully controlled and reliant on technology.

Overuse of the Internet and technology makes people unintelligent because they rely on smart devices instead of doing physical work, causing them to become lazy.

Unskilled workers are at a high risk of losing their jobs, which could lead to unemployment. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing security guards, maids, ironmen, and dry-cleaning services etc.

It is very difficult to plan, build, manage, and enable a broad technology to IoT framework.

Deploying IoT devices is very costly and time-consuming.

CLOUD COMPUTING

SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

There are three main types of cloud computing service models that you can select based on the level of control, flexibility, and management your business needs:

Infrastructure as a service (IaaS)

Infrastructure as a service (IaaS) offers on-demand access to IT infrastructure services, including compute, storage, networking, and virtualization. It provides the highest level of control over your IT resources and most closely resembles traditional on-premises IT resources.

Platform as a service (PaaS)

Platform as a service (PaaS) offers all the hardware and software resources needed for cloud application development. With PaaS, companies can focus fully on application development without the burden of managing and maintaining the underlying infrastructure.

Software as a service (SaaS)

Software as a service (SaaS) delivers a full application stack as a service, from underlying infrastructure to maintenance and updates to the app software itself. A SaaS solution is often an end-user application, where both the service and the infrastructure is managed and maintained by the cloud service provider.

Interdependencies of IoT and Cloud computing.

One component that improves the success of the Internet of Things is Cloud Computing. Cloud computing enables users to perform computing tasks using services provided over the Internet. The use of the Internet of Things in conjunction with cloud technologies has become a kind of catalyst: the Internet of Things and cloud computing are now related to each other. These are true technologies of the future that will bring many benefits.

Due to the rapid growth of technology, the problem of storing, processing, and accessing large amounts of data has arisen. Great innovation relates to the mutual use of the Internet of Things and cloud technologies. In combination, it will be possible to use powerful processing of sensory data streams and new monitoring services. As an example, sensor data can be uploaded and saved using cloud computing for later use as intelligent monitoring and activation using other devices. The goal is to transform data into insights and thus drive cost-effective and productive action.

Benefits And Functions of IoT Cloud:IoT Cloud Computing provides many connectivity options, implying large network access. People use a wide range of devices to gain access to cloud computing resources: mobile devices, tablets, laptops. This is convenient for users but creates the problem of the need for network access points.

Developers can use IoT cloud computing on-demand. In other words, it is a web service accessed without special permission or any help. The only requirement is Internet access.

Based on the request, users can scale the service according to their needs. Fast and flexible means you can expand storage space, edit software settings, and work with the number of users. Due to this characteristic, it is possible to provide deep computing power and storage.

Cloud Computing implies the pooling of resources. It influences increased collaboration and builds close connections between users.

As the number of IoT devices and automation in use grows, security concerns emerge. Cloud solutions provide companies with reliable authentication and encryption protocols.

Finally, IoT cloud computing is convenient because you get exactly as much from the service as you pay. This means that costs vary depending on use: the provider measures your usage statistics. A growing network of objects with IP addresses is needed to connect to the Internet and exchange data between the components of the network.

It is important to note that cloud architecture must be well-designed since reliability, security, economy, and performance optimization depends upon it. Using well-designed CI/CD pipelines, structured services, and sandboxed environments results in a secure environment and agile development.

THANK YOU