Course Code : MCS-227

Course Title : Cloud Computing and IoT

Assignment Number : MCA_NEW(III)/227/Assign/2023

Last Dates for Submission : 30th April, 2023 (for January session)

31st October, 2023 (for July session)

This assignment has four questions of 20 Marks each, amounting to 80 marks.
Answer all questions. Rest 20 marks are for viva voce. You may use illustrations and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of presentation.

Q1: What is Cloud Computing ? How Cloud Computing differs from Cluster Computing , Grid Computing ? Explain the characteristics of Cloud Computing. Also, give benefits & applications of Cloud Computing.
Ans.

Cloud computing is a computing model that enables the delivery of on-demand computing resources over the internet, such as storage, processing power, and software applications, without the need for local infrastructure or management of resources.
Cluster computing is a type of computing that uses multiple interconnected computers to work together to perform high-performance computing tasks. In contrast, grid computing is a type of computing that uses multiple computers that are distributed over a wide geographic area and work together to perform complex computational tasks.
Cloud computing differs from both cluster and grid computing in that it provides a more user-friendly and scalable way of accessing computing resources. Cloud computing is designed to offer a wide range of computing resources that can be quickly and easily accessed over the internet, with the ability to scale up or down depending on the needs of the user.

The characteristics of cloud computing include:

1. **On-demand self-service: Users can access computing resources on-demand without requiring human intervention.**
2. **Broad network access: Cloud services can be accessed from any device with internet access.**
3. **Resource pooling: Resources are shared among multiple users to maximize efficiency.**
4. **Rapid elasticity: Resources can be quickly scaled up or down depending on user demand.**
5. **Measured service: Usage is monitored, and users are only charged for the resources they consume.**

Benefits of cloud computing include:

1. **Cost savings: Cloud computing eliminates the need for expensive hardware and infrastructure, reducing overall costs.**
2. **Scalability: Resources can be easily scaled up or down to meet changing needs.**
3. **Accessibility: Cloud services can be accessed from anywhere with an internet connection.**
4. **Reliability: Cloud providers often offer high availability and redundancy to ensure uptime.**
5. **Security: Cloud providers typically offer strong security measures to protect data and infrastructure.**

Applications of cloud computing include:

1. **Data storage and backup: Cloud storage services offer a convenient and cost-effective way to store and backup data.**
2. **Software development: Cloud-based development environments enable developers to collaborate and work on projects from anywhere.**
3. **Big data analytics: Cloud computing provides the resources needed to process and analyze large amounts of data.**
4. **Web and mobile app hosting: Cloud providers offer scalable and reliable hosting solutions for web and mobile apps.**
5. **Virtual desktops and remote work: Cloud-based desktops and remote work solutions enable employees to work from anywhere, on any device.**

Q2: Explain the following types of network connectivity in cloud computing:

1. Public Inter cloud Networking

Ans.

Public intercloud networking is the connection of multiple public clouds to enable data exchange and resource sharing across different cloud providers. It is a network connectivity model that allows organizations to access and use services and applications from multiple cloud providers in a seamless manner.

Public intercloud networking is facilitated by a set of standardized protocols and APIs that enable different cloud platforms to communicate with each other. This allows organizations to leverage the benefits of multiple cloud providers, such as scalability, cost-effectiveness, and flexibility, without being locked into a single vendor or platform.

Public intercloud networking provides several benefits, including:

1. **Flexibility: Public intercloud networking allows organizations to choose the best cloud provider for each workload, based on cost, performance, and other factors.**
2. **Scalability: With public intercloud networking, organizations can easily scale their resources up or down as needed, without being constrained by the limitations of a single cloud provider.**
3. **Cost-effectiveness: Public intercloud networking enables organizations to use multiple cloud providers, which can help to reduce costs and improve ROI.**
4. **Resilience: Public intercloud networking can improve the resilience and reliability of cloud-based applications, by providing redundancy and failover capabilities across different cloud providers.**
5. **Innovation: Public intercloud networking can promote innovation by enabling organizations to experiment with different cloud providers and services, and to quickly adopt new technologies and approaches.**

2. Private Inter cloud Networking

Ans.

Private intercloud networking is a type of network connectivity in cloud computing that allows different private cloud environments within an organization to connect and share resources. It provides a way for organizations to create a unified cloud environment by connecting their private clouds together, which can help to improve resource utilization and reduce costs.

Private intercloud networking typically involves the use of virtual private networks (VPNs), software-defined networking (SDN), and other network technologies to create a secure and reliable network infrastructure that enables data and resource sharing between different private cloud environments.

Private intercloud networking offers several benefits, including:

1. **Resource sharing: Private intercloud networking enables organizations to share resources such as storage, processing power, and applications across different private cloud environments, which can help to improve resource utilization and reduce costs.**
2. **Scalability: Private intercloud networking allows organizations to scale their private cloud environments up or down as needed, based on changing demand.**
3. **Flexibility: Private intercloud networking enables organizations to choose the best private cloud environment for each workload, based on factors such as performance, security, and compliance requirements.**
4. **Security: Private intercloud networking provides a secure and reliable network infrastructure that enables organizations to control and manage access to their private cloud environments.**
5. **Control: Private intercloud networking provides organizations with greater control over their cloud infrastructure and resources, which can help to improve management and governance.**

3. Public Intra cloud Networking

Ans.

Public intracloud networking is a type of network connectivity in cloud computing that enables different resources and services within a single public cloud environment to connect and communicate with each other. It allows for the creation of a unified and interconnected cloud infrastructure within a single cloud provider, enabling efficient resource utilization and service delivery.

Public intracloud networking typically involves the use of various networking technologies, such as virtual private networks (VPNs), software-defined networking (SDN), and other network connectivity solutions, to create a secure and reliable network infrastructure that facilitates data and resource sharing between different resources and services within a public cloud environment.

Public intracloud networking offers several benefits, including:

1. **Resource sharing: Public intracloud networking enables different resources and services within a public cloud environment to share resources such as storage, processing power, and applications, which can help to improve resource utilization and reduce costs.**
2. **Scalability: Public intracloud networking allows organizations to scale their cloud resources up or down as needed, based on changing demand.**
3. **Flexibility: Public intracloud networking enables organizations to choose the best resources and services for each workload, based on factors such as performance, security, and compliance requirements.**
4. **Accessibility: Public intracloud networking provides easy access to different cloud services and resources within a single cloud provider, which can help to improve service delivery and efficiency.**
5. **Cost-effectiveness: Public intracloud networking enables organizations to optimize their cloud resource utilization, which can help to reduce costs and improve cost-effectiveness.**

4. Private Intra cloud Networking

Ans.

Private intra cloud networking is a method of network connectivity in cloud computing that enables secure communication and data transfer between different virtual machines (VMs) or services within the same private cloud network. It provides a dedicated, isolated network that is only accessible to authorized users, ensuring that sensitive data remains secure and protected from external threats.

In a private intra cloud network, VMs and services are typically assigned private IP addresses within the same subnet. This allows them to communicate with each other using local network traffic, while also ensuring that they remain isolated from the public internet. Private intra cloud networks use advanced networking technologies such as virtual LANs (VLANs) and software-defined networks (SDNs) to create secure, high-performance connections between different resources within the cloud infrastructure.

One of the main advantages of private intra cloud networking is that it provides a highly scalable and flexible way to connect different resources within a cloud infrastructure. It allows for the creation of complex multi-tiered applications that can be easily deployed and managed within the same private network. Private intra cloud networking also helps to reduce network latency and improves application performance by enabling faster and more efficient data transfers between different resources.

Private intra cloud networking is widely used by organizations that require high levels of security and compliance, such as financial institutions, healthcare providers, and government agencies. It is also used by businesses that need to run mission-critical applications that require dedicated and isolated resources.

Q3: Explain the importance of virtualization in cloud computing? How security is achieved through virtualization? Emulation and isolation are important features of virtualization. Justify the statement.

Ans.

Virtualization is a fundamental technology in cloud computing that allows multiple virtual machines (VMs) or operating systems to run on a single physical machine. It enables cloud providers to offer a range of services such as Infrastructure

as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) by partitioning the physical resources into multiple virtual environments.

The importance of virtualization in cloud computing can be summarized as follows:

1. **Resource utilization: Virtualization allows the efficient use of physical resources by enabling multiple virtual machines to share the same underlying hardware. This reduces the need for additional physical servers, which in turn leads to cost savings.**
2. **Scalability: Virtualization makes it easier to scale resources up or down based on the changing needs of an organization. With virtualization, administrators can create, configure, and delete virtual machines quickly and easily, without the need for additional hardware.**
3. **Agility: Virtualization enables cloud providers to offer a range of services quickly and easily, without the need for specialized hardware or software. This enables organizations to respond to changing market conditions and customer demands more rapidly.**

Security is a critical aspect of cloud computing, and virtualization plays an important role in achieving it. By isolating virtual machines from each other and the underlying physical hardware, virtualization helps to prevent security breaches from spreading across the cloud infrastructure. Additionally, virtualization technologies like hypervisors provide a layer of security by enforcing policies and access controls on virtual machines and their network traffic.

Emulation and isolation are two important features of virtualization that contribute to its security. Emulation allows multiple virtual machines to run different operating systems and applications on the same physical hardware, providing an additional layer of security by isolating them from each other. Isolation ensures that virtual machines are isolated from the underlying physical hardware, as well as from each other, preventing them from accessing or interfering with each other's resources.

In conclusion, virtualization is an important technology in cloud computing that provides numerous benefits such as resource utilization, scalability, and agility. It also plays a critical role in achieving security in the cloud infrastructure, thanks to its features of emulation and isolation.

Q4: What is an Hypervisor? Compare the functionality of Type-1 and Type-2 Hypervisor with the help of suitable block diagram for each, also give advantages and disadvantages of each.

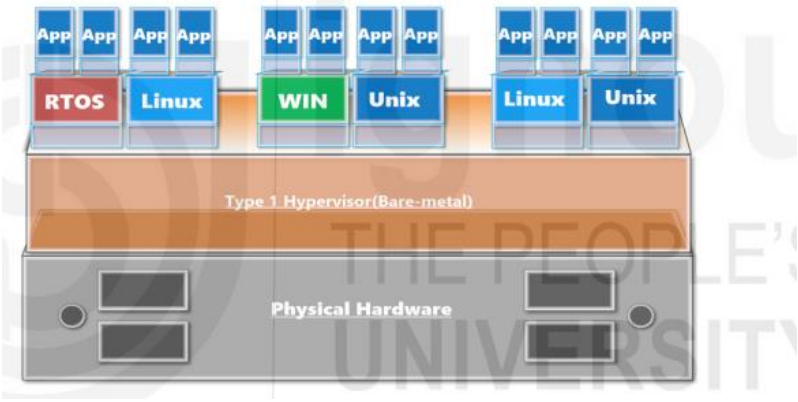
Ans.

A hypervisor, also known as a virtual machine monitor (VMM), is a software program that allows multiple virtual machines to share a single physical host machine. The hypervisor provides an abstraction layer between the physical hardware and the virtual machines, enabling them to run independently of each other.

There are two types of hypervisors:

1. **Type-1 Hypervisor (Bare-Metal Hypervisor): A Type-1 hypervisor, also known as a bare-metal hypervisor, runs directly on the host machine's hardware, without the need for an operating system. The Type-1 hypervisor controls the hardware resources and allocates them to virtual machines. The virtual machines run directly on the hypervisor and have direct access to the physical hardware.**

Here's a block diagram of a Type-1 hypervisor:



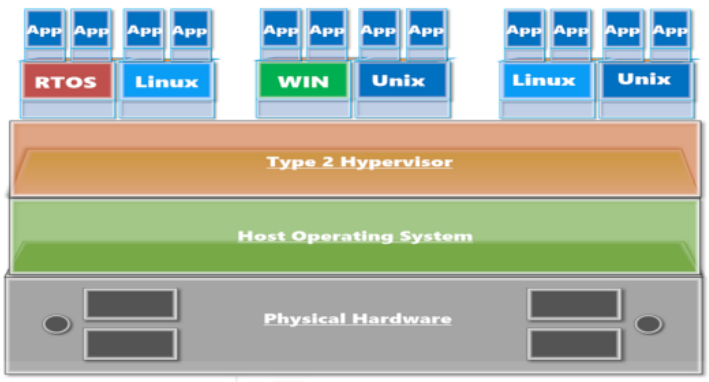
Advantages:

1. **Provides higher performance because the virtual machines run directly on the hardware.**
2. **Offers better security because the hypervisor is the only software layer between the virtual machines and the hardware.**
3. **Supports a wider range of operating systems and applications.**

Disadvantages:

1. **Requires dedicated hardware, which can be expensive.**
2. **Can be more difficult to set up and configure than Type-2 hypervisors.**
1. **Type-2 Hypervisor (Hosted Hypervisor): A Type-2 hypervisor, also known as a hosted hypervisor, runs on top of an operating system, such as Windows or Linux. The Type-2 hypervisor uses the host operating system's device drivers to control the hardware resources and allocates them to virtual machines. The virtual machines run on top of the host operating system.**

Here's a block diagram of a Type-2 hypervisor:



Advantages:

1. **Can run on any operating system that is supported by the hypervisor.**
2. **Can be easier to set up and configure than Type-1 hypervisors.**
3. **Does not require dedicated hardware.**

Disadvantages:

1. **Performance may be lower because the virtual machines have to go through the host operating system to access hardware resources.**
2. **Security may be lower because the host operating system is an additional software layer between the virtual machines and the hardware.**
3. **Supports a limited range of operating systems and applications.**

In conclusion, both Type-1 and Type-2 hypervisors have their own advantages and disadvantages, and the choice between them depends on specific requirements, such as performance, security, and compatibility with different operating systems and applications.

Q5: What is Tenancy in context of cloud computing ? Compare Multi-Tenancy model and Single Tenancy model of resource sharing. Explain the various ways through which Multi-Tenancy can be implemented.

Ans.

In cloud computing, tenancy refers to the way resources are shared among multiple users or tenants. It is a critical aspect of cloud computing as it affects the way resources are allocated, managed, and secured.

Single tenancy model is a traditional hosting model where a single instance of an application runs on a server dedicated to a single client. In contrast, multi-tenancy is a model where multiple users share a single instance of an application, running on a shared infrastructure.

The multi-tenancy model has several advantages over single tenancy, including cost savings, improved resource utilization, and scalability. However, it also introduces some challenges, especially in terms of security and data privacy.

To implement multi-tenancy, there are several ways, including:

1. **Virtualization: In this approach, the cloud service provider creates virtual machines that run multiple instances of an application, each dedicated to a different tenant. The virtual machines provide isolation and security for each tenant, ensuring that each tenant's data is protected.**
2. **Containerization: Containerization is similar to virtualization, but it provides more lightweight and efficient resource allocation. Instead of creating virtual machines, the cloud service provider uses containers to isolate the application instances for each tenant.**
3. **Segmentation: In this approach, the cloud service provider uses network segmentation to isolate the resources for each tenant. This is typically done using VLANs or other network partitioning techniques.**
4. **Application-level isolation: In this approach, the cloud service provider uses application-level isolation to separate the resources for each tenant. This can be achieved through application-level security mechanisms, such as firewalls, access controls, and encryption.**

In summary, multi-tenancy is a model where multiple users share a single instance of an application, running on a shared infrastructure. It provides cost savings, improved resource utilization, and scalability. However, it also introduces security and privacy challenges, which can be addressed through various implementation approaches, including virtualization, containerization, segmentation, and application-level isolation.

Q6: Explain the term Resource Provisioning in context of cloud computing. Also, explain the various approaches used for Resource Provisioning. Discuss the problems of Over-provisioning and Underprovisioning.

Ans.

Resource provisioning is the process of allocating and managing computing resources in a cloud environment to meet the dynamic demands of users. It is a critical aspect of cloud computing as it enables efficient and effective use of resources while maintaining service-level agreements (SLAs) and optimizing costs. Resource provisioning involves the allocation of resources such as virtual machines, storage, and network bandwidth, based on user demands.

There are several approaches used for resource provisioning in cloud computing:

1. **Manual provisioning: In this approach, resources are provisioned manually by administrators based on user requests. This approach is time-consuming, error-prone, and not suitable for large-scale environments.**
2. **Automated provisioning: In this approach, resources are provisioned automatically based on predefined policies and rules. This approach is more efficient and scalable than manual provisioning and enables rapid resource allocation and de-allocation.**
3. **Self-service provisioning: In this approach, users can provision and manage their resources without the intervention of administrators. This approach is highly efficient and enables rapid provisioning and de-allocation of resources, but it requires strong security controls to prevent unauthorized access.**

Over-provisioning and under-provisioning are common problems in resource provisioning. Over-provisioning occurs when resources are allocated in excess of the actual demand, resulting in wastage of resources and higher costs. Under-provisioning occurs when resources are allocated insufficiently to meet the actual demand, resulting in poor performance and user dissatisfaction.

To address the problem of over-provisioning, cloud providers can use dynamic resource allocation, where resources are provisioned based on the actual demand, and unused resources are de-allocated to reduce costs. To address the problem of under-provisioning, cloud providers can use predictive analytics and machine learning algorithms to forecast demand and provision resources proactively.

In summary, resource provisioning is the process of allocating and managing computing resources in a cloud environment to meet the dynamic demands of users. There are several approaches used for resource provisioning, including manual provisioning, automated provisioning, and self-service provisioning. Over-provisioning and under-provisioning are common problems in resource provisioning, which can be addressed using dynamic resource allocation, predictive analytics, and machine learning algorithms.

Q7: Explain the term Internet of Things (IoT).List and explain the various components used to implement IoT. Give characteristics of IoT. Briefly discuss the following types of IoT:

1. Consumer IoT (CIoT)
2. Industrial IoT(IIoT)
3. Infrastructure IoT
4. Internet of Military Things (IoMT)

Ans.

The Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances, and other items embedded with electronics, sensors, software, and network connectivity, which enables these objects to connect and exchange data. The primary goal of IoT is to make everyday objects "smart" by enabling them to interact with the environment and communicate with other devices, providing useful data that can be analyzed to improve efficiency, productivity, and quality of life.

The components used to implement IoT can be broadly categorized into the following:

1. **Sensors: IoT devices are equipped with sensors that collect data from the environment. These sensors can include temperature, humidity, pressure, motion, proximity, and light sensors.**
2. **Connectivity: IoT devices need to be connected to the internet or a network to transmit data. This can be achieved using various wireless and wired connectivity options such as Wi-Fi, Bluetooth, Zigbee, and cellular networks.**
3. **Processors: IoT devices use processors to analyze the data collected by sensors and make decisions. These processors can be low-power microcontrollers or powerful processors depending on the complexity of the device.**
4. **Data storage: IoT devices generate a vast amount of data, which needs to be stored for analysis. Cloud storage is commonly used to store data generated by IoT devices.**
5. **User interface: IoT devices need a user interface to interact with the user. This can be in the form of a mobile app, web interface, or voice-based interface.**

Characteristics of IoT:

1. **Interconnectivity: IoT devices are interconnected, enabling them to share data and work together.**
2. **Sensing and data collection: IoT devices are equipped with sensors to collect data from the environment.**
3. **Data analytics: IoT devices generate large amounts of data, which can be analyzed to provide valuable insights.**
4. **Automation: IoT devices can automate tasks based on data analysis, reducing the need for human intervention.**
5. **Real-time feedback: IoT devices provide real-time feedback on the status of objects and the environment.**

In summary, the Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances, and other items embedded with electronics, sensors, software, and network connectivity. The components used to implement IoT

include sensors, connectivity, processors, data storage, and user interfaces. IoT has several characteristics, including interconnectivity, sensing and data collection, data analytics, automation, and real-time feedback.

1. Consumer IoT (CIoT)

Consumer IoT (CIoT) refers to the growing network of physical devices, vehicles, home appliances, and other electronics that are embedded with sensors, software, and network connectivity, allowing them to collect and exchange data with other devices and systems over the internet.

CIoT devices are designed to enhance the quality of life and streamline daily tasks for consumers, often by automating household routines and providing real-time insights into the environment around them. Some popular examples of CIoT devices include smart thermostats, fitness trackers, home security systems, and voice assistants.

However, there are also concerns around the security and privacy of CIoT devices. As these devices often collect sensitive data about consumers, there is a risk that this information could be compromised or misused if proper security measures are not taken. Additionally, as CIoT devices become more widespread, there is a risk that they could be used as part of large-scale cyber attacks, posing a threat to critical infrastructure and public safety.

2. Industrial IoT(IIoT)

Industrial IoT (IIoT) refers to the use of internet-connected sensors, devices, and systems in industrial settings to improve efficiency, productivity, and safety. IIoT involves the use of sensors and other monitoring devices to collect data about the performance of machines, equipment, and other assets in real-time. This data is then used to optimize industrial processes, predict maintenance needs, and reduce downtime.

IIoT is commonly used in manufacturing, transportation, energy, and other industries. Some examples of IIoT applications include predictive maintenance of machines, inventory optimization, and remote monitoring of equipment. In addition, IIoT can enable more efficient supply chain management and improve workplace safety by detecting potential hazards and alerting workers in real-time.

However, there are also concerns around the security and privacy implications of IIoT. As industrial systems are often critical infrastructure, any disruption or compromise of IIoT devices could have serious consequences for public safety and national security. Therefore, it is essential to implement strong security measures and protocols to protect IIoT systems from cyber threats.

3. Infrastructure IoT

Infrastructure IoT (IIoT) refers to the use of internet-connected sensors, devices, and systems to monitor and manage critical infrastructure such as roads, bridges, water systems, and energy grids. By leveraging real-time data collection and analysis, IIoT aims to improve the efficiency and safety of public services and utilities, as well as reduce operational costs and resource consumption.

IIoT can enable a range of applications, such as real-time traffic management, predictive maintenance of bridges and roads, and smart energy grid management. For example, sensors can be installed on roads to monitor traffic flow and adjust traffic signals in real-time, reducing congestion and improving safety. Similarly, sensors can be used to monitor the structural integrity of bridges and alert authorities to potential maintenance needs before a catastrophic failure occurs.

However, there are also challenges to implementing IIoT. These include the high cost of deploying and maintaining sensor networks, as well as concerns around data security and privacy. Additionally, as IIoT becomes more widespread, it is important to ensure that the benefits of these technologies are equitably distributed across communities, and that vulnerable populations are not left behind.

4. Internet of Military Things (IoMT)

The Internet of Military Things (IoMT) refers to the use of connected devices, sensors, and other technologies to improve military operations and decision-making. IoMT applications can range from logistics and supply chain management to combat operations and situational awareness.

One example of an IoMT application is the use of drones or unmanned aerial vehicles (UAVs) to conduct reconnaissance or surveillance missions. These UAVs can be equipped with various sensors, such as cameras, thermal imaging devices, and even weapons systems, and can be controlled remotely or operate autonomously. IoMT can also improve military logistics by using connected sensors to track and monitor the location and condition of supplies and equipment, and by using predictive analytics to optimize supply chain operations.

However, the use of IoMT in military applications also raises concerns around data security, privacy, and autonomy. The data generated by IoMT devices can be highly sensitive and must be protected from cyberattacks and unauthorized access. Additionally, there are ethical and legal questions around the use of autonomous weapons systems and the role of humans in decision-making processes. These challenges highlight the need for responsible and ethical development and deployment of IoMT technologies in military contexts.

Q8: What is Edge computing? Discuss the working of Edge computing. Also, describe the relation between Edge computing, Fog computing and Cloud Computing, with the help of a suitable block diagram ?

Ans :-

Edge computing is a distributed computing paradigm where data processing and storage are performed closer to the devices generating the data, rather than in a centralized cloud or data center. It involves placing computing resources at the edge of a network, closer to the sources of data, in order to reduce latency, increase bandwidth, and improve efficiency.

In Edge computing, data is processed and analyzed on devices that are located at the network edge, such as routers, switches, gateways, and other IoT devices. This allows for faster response times, better data privacy and security, and reduced network congestion. By processing data locally, Edge computing reduces the need for large amounts of data to be transferred to a centralized cloud or data center for processing, thus reducing network bandwidth and cost.

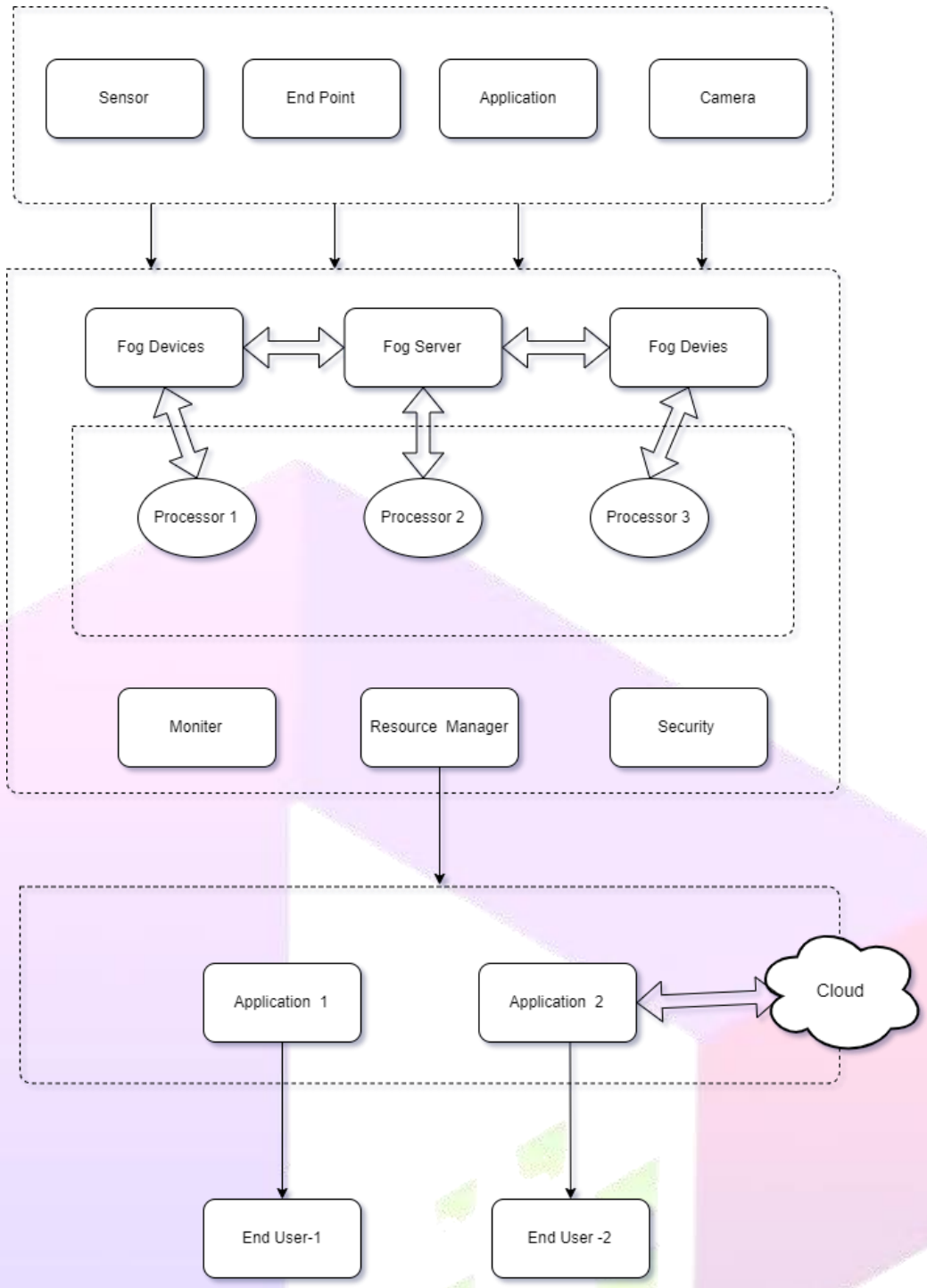
The working of Edge computing involves a number of interconnected devices and systems working together to process and analyze data at the network edge. The process starts with data being generated by devices such as sensors or cameras. This data is then transmitted to Edge devices, such as gateways or edge servers, which process and analyze the data locally. The processed data is then transmitted to the cloud or data center for further processing, analysis, and storage.

Edge computing is related to Fog computing and Cloud computing. Fog computing is a distributed computing paradigm that extends the capabilities of cloud computing to the edge of the network. It involves placing computing resources between the cloud and the edge devices, allowing for data processing and analysis closer to the edge.

Cloud computing, on the other hand, involves the centralized storage and processing of data in remote data centers, with data being accessed over the internet. It is a centralized computing paradigm that is suitable for large-scale data processing and storage.

A suitable block diagram to illustrate the relation between Edge computing, Fog computing, and Cloud computing is shown below:

Block Diagram



In this diagram, Edge devices are located at the edge of the network, such as sensors or cameras. These devices send data to Edge devices, such as gateways or edge servers, for local processing and analysis. The processed data is then transmitted to Fog devices, which act as an intermediary layer between the Edge devices and the Cloud. The Fog devices can perform further processing and analysis before sending the data to the Cloud for final processing and storage. The Cloud provides the centralized computing resources for data storage and processing, and can be accessed over the internet.

Overall, the combination of Edge, Fog, and Cloud computing allows for efficient, scalable, and distributed computing architectures that can handle large amounts of data with low latency and high security.