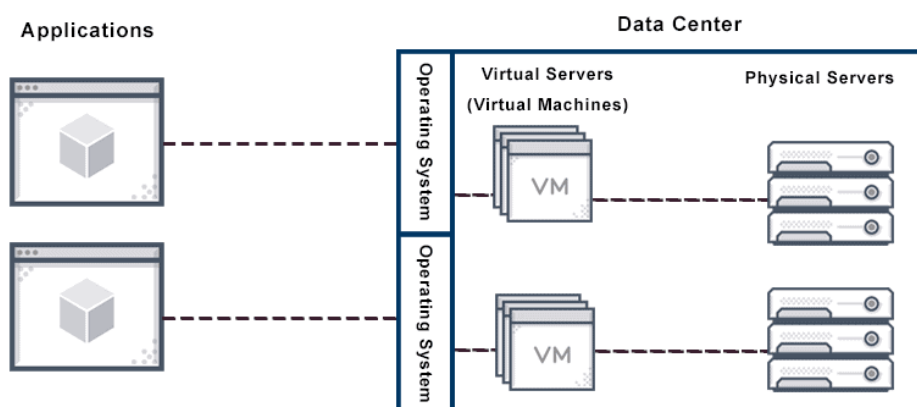


**Subject : Edge and Fog Computing**  
**Experiment No. 2**

**Aim:** To create and deploy a virtual server on AWS

**Theory:**

A virtual server mimics the functionality of a physical dedicated server. Multiple virtual servers may be implemented on a single bare metal server, each with its own OS, independent provisioning, and software. A virtual machine server uses virtual infrastructure, virtualization software and abstracts the physical server's computer resources to create virtual environments. Benefits of virtual servers include faster provisioning of applications and resources, improved disaster recovery and business continuity, and minimized or eliminated downtime. Virtualization also increases IT productivity, agility, efficiency, and responsiveness. Additional benefits of virtual servers include reduced operating costs and capital, and simplified data center



management. Virtual server environments also mimic dedicated server environments in terms of how they maintain passwords and security systems. Virtual server hosting is less expensive than data center maintenance, and server software installation provisioning may further reduce web hosting costs. To achieve efficiency, administrators use special server virtualization software to divide one physical dedicated server into multiple virtual servers. Converting one physical server into multiple virtual servers makes better use of power and resources. This in turn enables each physical server to efficiently run multiple OS and applications. Technically, a virtual server exists only as a partitioned space inside a physical server. For users, there is little difference.

**Virtual server :**

Server virtualization is using virtualization software to partition or divide up the server so that it looks and functions like multiple virtual servers. Each virtual server can then run their own OS, and be used as needed. This way, the server as a whole can be used in many ways and optimized rather than being dedicated to just one application or task.

**Subject : Edge and Fog Computing**  
**Experiment No. 2**

Benefits of server virtualization include:

- Cost-effective. By partitioning servers the supply of servers increases dramatically at almost zero cost.
- Resource isolation. Independent user environments ensure that things like software testing don't affect all users.
- Save energy and space. Fewer servers mean less power consumed and less space storing them. Resource hogging is the most common server virtualization challenge. Too many virtual servers will crowd a physical server and hurt performance. A virtual private server (VPS) is a virtual server that is a dedicated/private server from the user's perspective, although a shared physical computer running multiple operating systems is running each virtual server. A VPS is also sometimes called a virtual dedicated server (VDS). Both a VPS and a VDS are types of virtual servers.

**•Difference Between Virtual Server vs Cloud Hosting:**

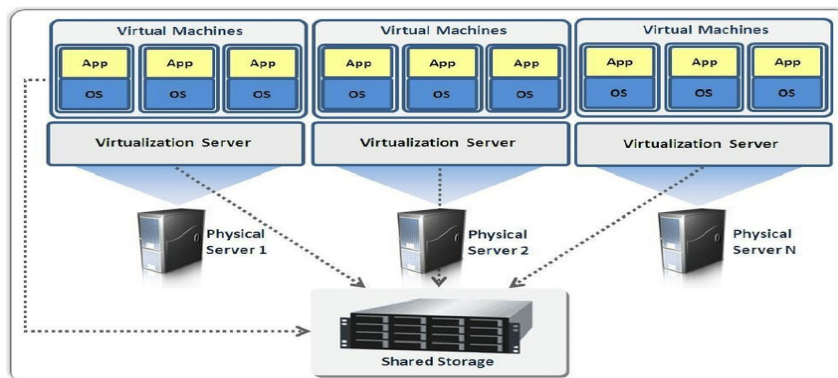
- The primary difference between virtual servers and cloud hosting environments is that a virtual server is created for one user, while cloud hosting is designed for many users.

**Difference Between Virtual Desktop and Virtual Server:**

Virtual servers and virtual desktops can achieve some of the same server virtualization goals for your computer network in practice, although they are not the same thing. A virtual desktop is technology that allows different users to run different operating systems on one computer, work apart from the physical machine, or sever connected devices should one be lost or stolen. A virtual server may still allow remote users to work and run different OSs, but it also has additional capabilities. For example, a virtual server can be used to test new software or applications without bringing down an entire server, and this is not the role of the virtual desktop. A virtual desktop server is a form of virtual desktop infrastructure. This kind of virtual server is used to create a virtual desktop environment to host multiple virtual desktops on a virtual server designed for this purpose. virtual servers used for any server, virtual servers are used to store data from different projects such as: Informational platforms and online stores (most of them have to have a database that also needs a server). Databases with private information to be used inside a company making it possible to share some data and keep it hidden from the outside. Platforms created to test software within the team or in person (when the local machine is not powerful enough). Setups that are made to work with complex systems like Odoo. Gaming servers (like ones used to host Minecraft personal playable worlds) and mail servers (to obtain full control on sent and received email). Systems to implement CCTV (to store a lot of GB's of recorded videos). And of course personal cloud storages. You can use a virtual server as a remote hard disk to store images, videos, audio files, etc.

**AWS Vs Azure Vs Google Comparison**

**Subject : Edge and Fog Computing**  
**Experiment No. 2**



The Public Cloud market is governed by top three public clouds – AWS, Google, and Azure. There is a strong competition between these three that can't be recouped by any additional public cloud provider in nearest future.

Amazon Web Services is dominating the public cloud over MS Azure and Google since 2006 when it started offering services. Microsoft Azure and Google are far from the race but growing continuously to be at the top.

On the basis of features and solutions, AWS vs Azure vs Google Features comparison is:

**Difference between AWS, Azure, and Google Cloud Platform :** However, each platform has its strengths and areas of focus. AWS is known for its wide range of services, Azure has a strong focus on building and deploying applications, and GCP is known for its machine learning and data analytics offerings

### **Amazon Web Services (AWS)**

Amazon Web Services (AWS) is a cloud computing platform which was introduced in 2002. It offers a wide range of cloud services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). AWS provides the largest community with millions of active customers as well as thousands of partners globally. Most of the organizations use AWS to expand their business by moving their IT management to the AWS. Flexibility, security, scalability, and better performance are some important features of AWS.

### **Microsoft Azure**

Microsoft Azure is also called as Windows Azure. It is a worldwide cloud platform which is used for building, deploying, and managing services. It supports multiple programming languages such as Java, Nodejs, C, and C#. The advantage of using Microsoft Azure is that it allows us to a wide variety of services without arranging and purchasing additional hardware components. Microsoft Azure provides several computing services, including servers, storage, databases, software, networking, and analytics over the Internet.

### **Google Cloud Platform (GCP)**

Google Cloud Platform (GCP) is introduced by Google in 2011. It allows us to use Google's products such as Google search engine, Gmail, YouTube, etc. Most of the companies use this platform to easily build, move, and deploy applications on the cloud. It allows us to access these applications using a high-speed internet connection. The advantage of GCP is that it supports various databases such as SQL, MYSQL, Oracle, Sam,

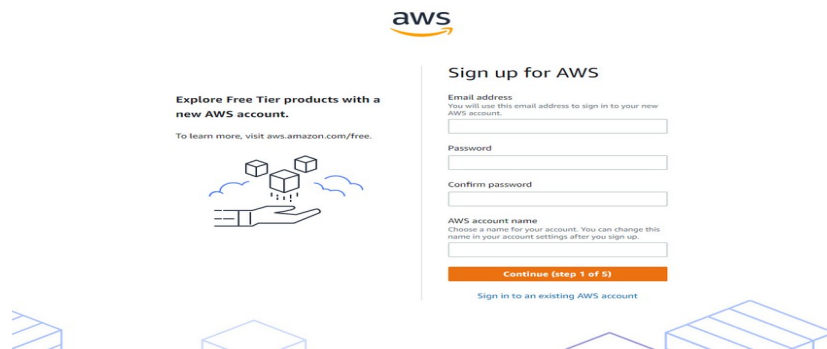
## Subject : Edge and Fog Computing Experiment No. 2

and more. Google Cloud Platform (GCP) provides various cloud computing services, including computing, data analytics, data storage, and machine learning. An Amazon Web Services (AWS) Virtual Machine (EC2) is a type of service offered by AWS that allows users to rent virtualized computing resources, such as virtual CPUs and memory, by the hour. These resources can be used to run a wide range of applications, including web servers, databases, and big data processing jobs. Users have the ability to configure and customize the operating system, storage, and networking resources of their EC2 instances to meet the specific requirements of their applications. EC2 is one of the core services of AWS and is a part of the Elastic Compute Cloud (EC2) service.

### Installation Steps:

#### 1. Create an AWS account

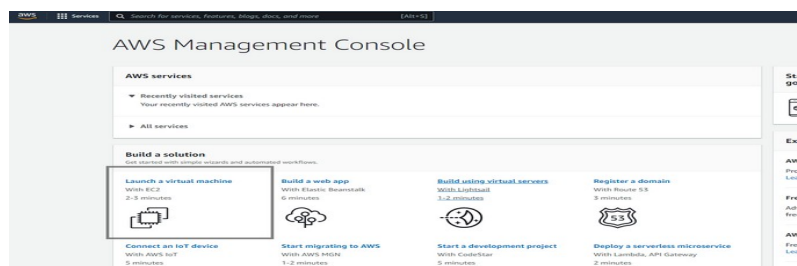
You can easily create an AWS account on the AWS Console. All new sign-ups get a free-tier offer.



The image shows the AWS sign-up page. On the left, there's a section titled "Explore Free Tier products with a new AWS account." with a link to [aws.amazon.com/free](https://aws.amazon.com/free). Below this is an illustration of a hand holding a cube. On the right, the "Sign up for AWS" form is visible. It includes fields for "Email address", "Password", and "Confirm password". Below these is the "AWS account name" field with a note: "Choose a name for your account. You can change this name in your account settings after you sign up." At the bottom of the form is an orange "Continue (step 1 of 5)" button. Below the button is a link: "Sign in to an existing AWS account".

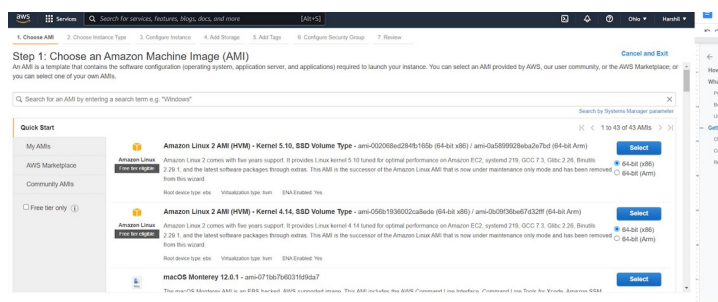
#### 2. Launch AWS virtual machine

Once you finish setting up your account, you can click on the AWS logo on the top left corner or search "console" on the search bar. You'll find a number of options in the AWS console. Select "Launch a virtual machine" to get started with VMs. If you're a new user, it can take up to 24 hours for your account to activate.



## Subject : Edge and Fog Computing

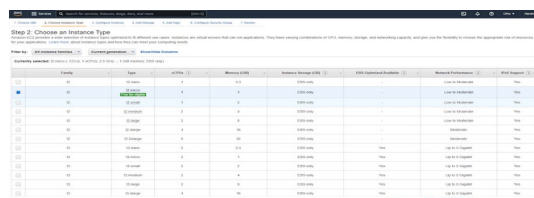
### Experiment No. 2



3. Choose AMI Amazon Machine Image (AMI) highlights the software setup (OS, application server, and apps). You can select Mac, Linux, or Windows OS. We'll look at the setup for Windows virtual machines here.

4. Choose and configure instance type.

After choosing your operating system, you need to pick an instance type. Amazon EC2 offers many instance types tailored to specific use cases. An instance is a virtual server or virtual machine. They come in a variety of CPU, memory, storage, networking, and a lot more. You can configure instance details, such as the number of instances, network, host type, and so on. Here, we'll use one instance and keep the remaining details default.



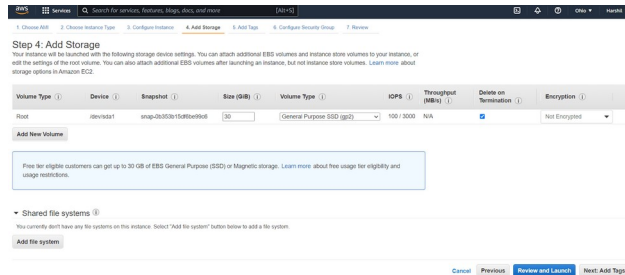
5. Add storage and tags

Once you configure an instance type, you can add or update storage info. AWS allows you to add more EBS volumes and instance store volumes, as well as change the root volume's parameters. Amazon Elastic Block Store (EBS) provides blocklevel storage volumes for use with EC2 instances. It behaves like raw, unformatted block devices. You can mount these volumes as devices on your instances.



## Subject : Edge and Fog Computing

### Experiment No. 2



**Step 4: Add Storage**  
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	devvol1	amp-0d80b1c0f0b0e0d0	30	General Purpose (SSD gp2)	100/3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage. [Learn more about free usage tier eligibility and usage restrictions.](#)

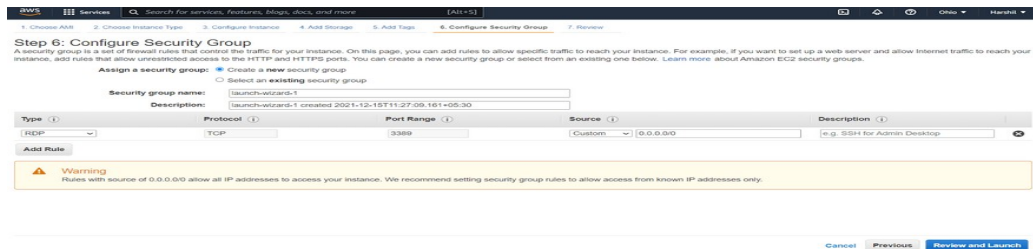
**Shared file systems**  
You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

[Add file system](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

The next step is adding tags. A tag is a label applied to an AWS resource. Each tag has a key and an optional value, which users define. 6. Configure security. A security group is a set of firewall rules that control data entering and exiting your instance. You may either recreate it or pick an existing security group.

Security is a major concern when working on public clouds like AWS and Google Cloud Platform (GCP). Attackers can launch different attacks on public cloud deployments for lack of provider security. These attacks include DOS, DDOS, website defacement, and brute-force. Public clouds have poor security, but with the right set of rules, they can be improved. Public clouds offer limited customization. Clients can choose the operating system and size of the virtual machine. Cloud data breaches are frequently caused by misconfigured cloud security settings. Many companies' cloud security posture management solutions are insufficient for safeguarding their cloud-based infrastructure.



**Step 6: Configure Security Group**  
A security group is a set of firewall rules that control traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

**Assign a security group:** ☒ Create a new security group

**Security group name:** launch-wizard-1

**Descriptions:** launch-wizard-1 created 2021-12-15T11:27:05.161+05:30

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom	0.0.0.0/0

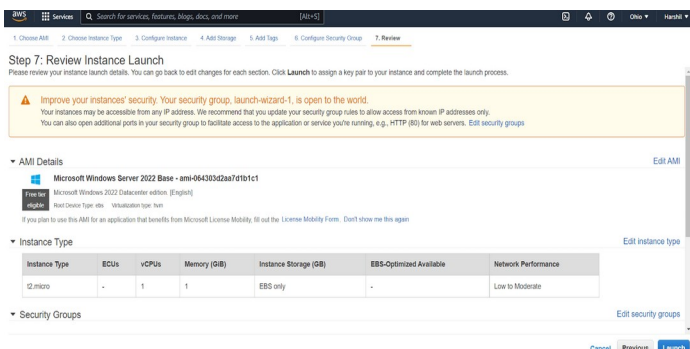
[Add Rule](#)

**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

## 7. Review and launch your AWS virtual machine

The final step in creating an AWS virtual machine is to go through your instance details. Make sure every detail is correct, then click "Launch". When you click "Launch," you need to provide a key. To create a new key, select "Create a new key pair" from the drop-down menu and set a key name, for example, key task, keytest1, and so on. Make sure you download "key pair" before launching your instance. A key pair is made up of a public key stored by AWS and your private key file. They work together to allow you to connect to your instance safely. You successfully created and launched a virtual machine on AWS. Now, check the launch status and connect to an instance.



**Step 7: Review Instance Launch**  
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Warning**  
Improve your instances' security. Your security group, launch-wizard-1, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running. (e.g., HTTP 80) for web servers. [Edit security group](#)

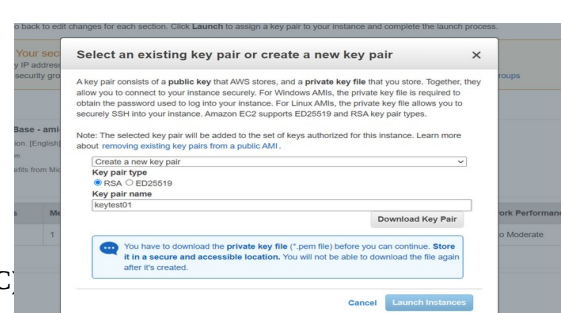
**AMI Details**  
Microsoft Windows Server 2022 Base - ami-064303d2a7d01c1

**Instance Type**

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

**Security Groups**

[Cancel](#) [Previous](#) [Launch](#)



**Select an existing key pair or create a new key pair**

A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

☒ Create a new key pair

**Key pair type**  
☒ RSA ☐ ED25519

**Key pair name**  
keytest01

[Download Key Pair](#)

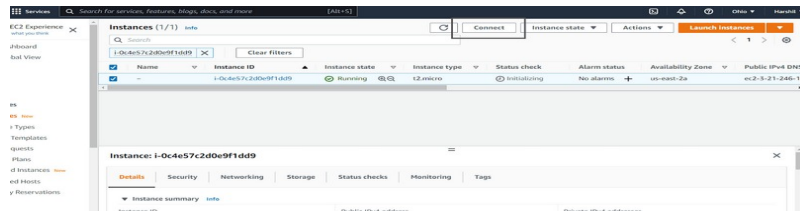
**Warning**  
You have to download the private key file (\*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)



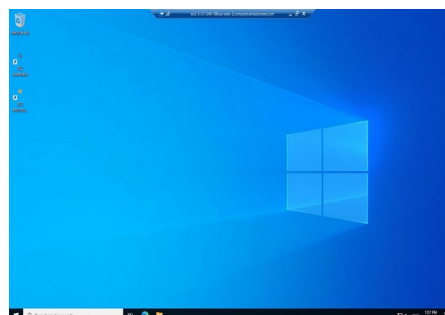
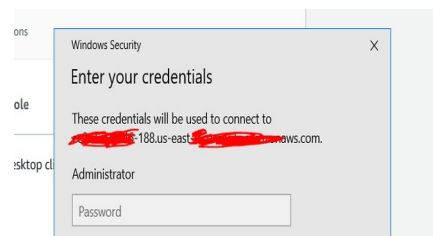
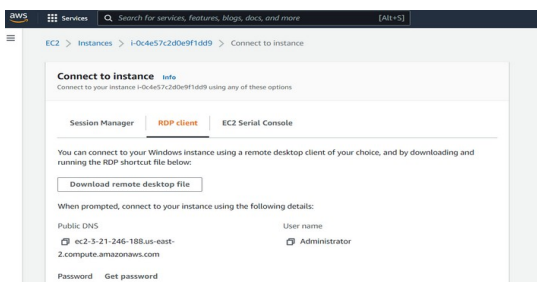
## Subject : Edge and Fog Computing Experiment No. 2

### 8. Connect to an instance



After starting the instance, you can check the status using “Dashboard>Instances”. Select your instance in the instance dashboard and click “Connect”. Select “RDP client,” click “Get password,” then upload the key pair downloaded when the instance launched (in step 7). After uploading the file, click “decrypt password” and download the remote desktop file.

You should now see a screen similar to the one below, indicating that your AWS Windows virtual machine successfully launched! In this guide, we have explained the detailed process of creating a virtual machine (VM) on Amazon Web Services (AWS). An Amazon Web Services (AWS) Virtual Machine (EC2) is a type of service offered by AWS that allows users to rent virtualized computing resources, such as virtual CPUs and memory, by the hour. These resources can be used to run a wide range of applications, including web servers, databases, and big data processing jobs. Users have the ability to configure and customize the operating system, storage, and networking resources of their EC2 instances to meet the specific requirements of their applications. EC2 is one of the core services of AWS and is a part of the Elastic Compute Cloud (EC2) service.



### Conclusion: