Practical - 1

Date:- 10-03-2023

Aim:- To study cloud architecture and cloud computing model.

Objectives: From this experiment, the student will be able to

- provide an overview of concepts of Cloud Computing.
- To encourage students to indulge into research in Cloud Computing.

Outcomes: The learner will be able to

- understand and appreciate cloud architecture.
- analyze the local and global impact of computing on individuals, organizations, and society.
- recognize the need for, and an ability to engage in life-long learning.

. Hardware / Software Required: Ubuntu operating system, Internet

Theory:

Cloud computing enables companies to consume compute resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house.Cloud computing promises several attractive benefits for businesses and end users.

Three of the main benefits of cloud computing include:

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.
- Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Type of cloud computing:

There are 3 main types of as-a-Service solutions: IaaS, PaaS, and SaaS. Each facilitates the flow of user data from front-end clients through the internet, to the cloud service provider’s systems, and back—but vary by what’s provided.

Infrastructure as a Service (IaaS):

IaaS means a cloud service provider manages the infrastructure for you—the actual servers, network, virtualization, and data storage—through an internet connection. The user has access through an API or dashboard, and essentially rents the infrastructure. The user manages things like the operating system, apps, and middleware while the provider takes care of any hardware, networking, hard drives, data storage, and servers; and has the responsibility of taking care of outages, repairs, and hardware issues. This is the typical deployment model of cloud storage providers.

Platform as a Service (PaaS):

PaaS means the hardware and an application-software platform are provided and managed by an outside cloud service provider, but the user handles the apps running on top of the platform and the data the app relies on. Primarily for developers and programmers, PaaS gives users a shared cloud platform for application development and management (an important DevOps component) without having to build and maintain the infrastructure usually associated with the process.

Software as a Service (SaaS):

SaaS is a service that delivers a software application—which the cloud service provider manages—to its users. Typically, SaaS apps are web applications or mobile apps that users can access via a web browser. Software updates, bug fixes, and other general software maintenance are taken care of for the user, and they connect to the cloud applications via a dashboard or API. SaaS also eliminates the need to have an app installed locally on each individual user’s computer, allowing greater methods of group or team access to the software.

Conclusion:
Cloud computing enables a convenient and on-demand network access to a wide range of resources. The different services and also the deployment models allow flexible service provider interaction with minimal human intervention. It saves costs but also can lead to risk issues and suspension of resources when in huge quantities.

Practical - 2

Date :- 11-02-2023

Aim :- Installation and Configuration of virtualization using KVM

Objective :- From this experiment, the student will be able to,

- Understand the concepts of virtualization.
- Understand KVM architecture and its configuration.

Outcomes:- The learner will be able,

- To analyze user models and develop user centric interfaces
- To analyze the local and global impact of computing on individuals, organizations, and society.
- To engage in lifelong learning development and higher studies.
- To understand, identify, analyze and design the problem, implement and validate the solution including both hardware and software.

Hardware / Software Required:- Ubuntu operating system, open source software KVM, Internet.

Theory:-

- Virtualization is software that separates physical infrastructures to create various dedicated resources. It is the fundamental technology that powers cloud computing.
- The technology behind virtualization is known as a virtual machine monitor (VMM) or virtual manager, which separates compute environments from the actual physical infrastructure

Procedure:-

Installation Steps :

1. sudo grep -c "svm\|vmx" /proc/cpuinfo
2. cat /proc/cpuinfo
3. sudo apt-get install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virt-manager

Run following command you should see an empty list of virtual machines. This indicates that everything is working correctly.

1. virsh -c qemu:///system list

Open Virtual Machine Manager application and Create Virtual Machine

1. virt-manager

Conclusion:-

- Installation and configuration of KVM have been done successfully onto Ubuntu and users added. Like this we can create as many virtual machines as possible on OS and can install any windows onto it

Practical - 3

Date:- 24-02-2023

Aim:- Study and implementation of Infrastructure as a Service

Objectives: From this experiment, the student will be able to,

- Understand concepts of virtualization and to use cloud as Infrastructure as a services.
- Learn the technique and its complexity Understand the importance of this technique from application point of view

Outcomes: The learner will be able,

- To match the industry requirements in the domains of Database management, Programming and Networking with limited infrastructure.
- To analyze the local and global impact of computing on individuals, organizations, and society.
- To use current techniques, skills, and tools necessary for computing practice.

Hardware / Software Required:

Ubuntu operating system, Virtual machine, WAMP/ZAMP server, Any tool or technology can be used for implementation of web application e.g., JAVA, PHP, etc.

Installation:
https://docs.openstack.org/devstack/latest/guides/single-machine.html

- sudo useradd -s /bin/bash -d /opt/stack -m stack
- sudo chmod +x /opt/stack
- apt-get install sudo -y || yum install -y sudo
- echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
- sudo su stack && cd ~

Download DevStack

- sudo apt-get install git -y || sudo yum install -y git

- git clone https://github.com/openstack/devstack.git
- cd devstack

Now to configure **stack.sh**. DevStack includes a sample in **devstack/samples/local.conf**. Create **local.conf** as shown below to do the following:

- Set **FLOATING_RANGE** to a range not used on the local network, i.e. 192.168.1.224/27. This configures IP addresses ending in 225-254 to be used as floating IPs.
- Set **FIXED_RANGE** to configure the internal address space used by the instances.
- Set the administrative password. This password is used for the **admin** and **demo** accounts set up as OpenStack users.
- Set the MySQL administrative password. The default here is a random hex string which is inconvenient if you need to look at the database directly for anything.
- Set the RabbitMQ password.
- Set the service password. This is used by the OpenStack services (Nova, Glance, etc) to authenticate with Keystone.

Run DevStack:

- ./stack.sh

A seemingly endless stream of activity ensues. When complete you will see a summary of **stack.sh**'s work, including the relevant URLs, accounts and passwords to poke at your shiny new OpenStack.

Using Openstack

At this point you should be able to access the dashboard from other computers on the local network. In this example that would be http://192.168.1.201/ for the dashboard (aka Horizon). Launch VMs and if you give them floating IPs and security group access those VMs will be accessible from other machines on your network.

Conclusion:

We have installed Ubuntu/Xen as bare metal hypervisor and implemented it. It provides access to computing resources in a virtual environment. With the help of Infrastructure as a service we can build our own IT platform. We can install Windows Operating System on Ubuntu and vice versa

Practical - 4

Date:- 11-02-2023

Aim:- To study and implementation of Storage as a Service

Objectives: From this experiment, the student will be able to

- To make the students understand the use of cloud as Platform, Storage as a service.
- To learn the efficient tools to implement the technique

Outcomes: The learner will be able to understand how Storage as a Service is provided.

Conclusion:-

- Google Docs provide an efficient way for storage of data. It fits well in Storage as a service (SaaS). It has varied options to create documents, presentations and also spreadsheets. It saves documents automatically after a few seconds and can be shared anywhere on the Internet at the click of a button.

Practical - 5

Date:- 10-03-2023

Aim:- Study and implementation of identity management

Objectives: From this experiment, the student will be able to,

- Understand concepts of virtualization and to use cloud as Infrastructure as a service.
- Learn the technique and its complexity.
- Understand the importance of this technique from an application point of view.

Outcomes: The learner will be able to

- To create and use online identity.
- To analyze the local and global impact of computing on individuals, organizations, and society and users of the company how to share and connect with each other.

Hardware / Software Required: Windows operating system, Gmail account, owncloud credentials

Theory:

- The primary goal of identity management in cloud computing is dealing with personal identity information so that a user's access to data, computer resources, applications, and services is controlled accurately.
- Identity management in cloud computing is the subsequent step of identity and access management (IAM) solutions. However, it is a lot more than merely a straightforward web app single sign-on (SSO) solution. This next generation of IAM solution is a holistic move of the identity provider right to the cloud. Known as Directory-as-a-Service (DaaS), this particular service is the advanced version of the conventional and on-premises solutions, including Lightweight Directory Access Protocol (LDAP) as well as Microsoft Active Directory (AD).
- ownCloud is an open source file sync and share software for everyone from individuals operating the free ownCloud Server

edition, to large enterprises and service providers operating the ownCloud Enterprise Subscription. ownCloud provides a safe, secure, and compliant file synchronization and sharing solution on servers that you control.

Result:

Steps:

- By default, the ownCloud Web interface opens to your Files page. You can add,remove, and share files, and make changes based on the access privileges set by you (if you are administering the server) or by your server administrator. You can access your ownCloud files with the ownCloud web interface and create, preview, edit, delete, share, and re-share files. Your ownCloud administrator has the option to disable these features, so if any of them are missing on your system ask your server administrator.
- Apps Selection Menu: Located in the upper left corner, click the arrow to open a dropdown menu to navigate to your various available apps. Apps Information field: Located in the left sidebar, this provides filters and tasks associated with your selected app. Application View: The main central field in the ownCloud user interface. This field displays the contents or user features of your selected app.
- Share the file or folder with a group or other users, and create public shares with hyperlinks. You can also see who you have shared with already, and revoke shares by clicking the trash can icon. If username autocomplete is enabled, when you start typing the user or group name ownCloud will automatically complete it for you. If your administrator has enabled email notifications, you can send an email notification of the new share from the sharing screen.
- Five Share permissions are : Can share; allows the users you share with to re-share.

  Can edit; allows the users you share with to edit your shared files, and to collaborate using the Documents app.

  Create; allows the users you share with to create new files and add them to the share.

  Change; allows uploading a new version of a shared file and replacing it.

Delete; allows the users you share with to delete shared files.

Procedure:

1. Visit https://demo.owncloud.org
2. Login using the admin credentials. (admin/admin)
3. Open the personal settings menu on the right corner and Go to ‘Users’ page.
4. Add a new user ’<your name>’ and create a new group named ’tycs’.
5. set a new password for the newly created user.
6. also select the group for the user.
7. Go to settings and click on sharing menu item.
8. check all options for sharing and exclude the admin group from sharing.
9. logout of the admin account and again login using the new user’s account.
10. Go to the files section and add a new file and share it.

Conclusion:

We have studied how to use ownCloud for ensuring identity management of the users. We can create multiple groups and provide privileges to view or modify data as per defined permissions. It also enables simplified look and feel to be used by anyone.

Practical - 6

Date

Aim: To Study Cloud Security management

Objectives: From this experiment, the student will be able,

- To understand the security features of Cloud
- To learn the technique of application security management and its complexity.
- To understand the importance of cloud security management from an application point of view.

Outcomes: The learner will be able to

- Students can study and implement single-sign-on.
- To use current techniques, skills, and tools necessary for computing practice.
- To match the industry requirements in the domains of Database management,

Programming and Networking with the required management skills.

Theory:

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider. Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data backup plan in the case of a cloud security breach.

Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security.

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

Application security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

Procedure:

- Visit https://auth0.com
- Create a new account
- Select ‘Company’ Account type, fill company name and company size
- tick the advanced settings option.
- Enter tenant domain name. Ex. ‘<your name><current year>
- select region as ‘USA’ & click on create account
- Navigate to ’Security > Multi-factor Auth’
- click on the ‘Phone Message’ section and enable it.

- Go back and enable the ‘One-Time Password’ option.
- Now, Navigate to ’Security > Attack Protection’ and enable ‘Enforce CAPTCHA’ by selecting the 'Always’ option and save it.

Conclusion:

We have studied how to secure the cloud and its data. Amazon EWS provides the best security with its extended facilities and services like MFA devices. It also gives you the ability to add your own permissions and policies for securing data more encrypted.

Practical - 7

Date: 21-03-2023
Aim: Write a program for web feed

Objective: This lab is to understand the concept of form and control validation

Scope: Write a program for web feed

Technology: XML / PHP, HTML

Theory:

RSS technology is used by millions of users around the world to get the latest information from their favorite websites. RSS (RDF Site Summary or Really Simple Syndication) is a web feed that allows users and applications to access updates to websites in a standardized, computer-readable format. Fundamentally, RSS is simply an XML text file. It's created by a website publisher and contains a running list of articles or other content published by the site, with the newest entry always at the top of the list. Each entry contains details like the article's title, description, and link to the content. RSS feeds are published and updated in real time, so if you subscribe to a site's RSS feed, you'll always have access to the newest published content. That can be handy for news sites and podcasts that are frequently updated.

Procedure:

- Visit https://gadgets360.com
- Click on the ‘RSS’ list item in the footer section.
- Select a random feed out of the given. Ex. ‘Opinion’.
- Copy the xml code.
- Create a new directory named ‘RSS’ in the 'XAMPP/htdocs’ folder and create a new xml file and paste the copied xml code. Ex. ‘itvoyage.xml’
- Start the ‘Apache' server from XAMPP.
- Open the served xml file in chrome. Ex. ‘http://localhost/RSS/itvoyage.xml'
- Go to the Chrome Store and search for the Extension 'RSS Subscription Extension’.

- Add the extension to chrome.
- Now refresh the page opened on step 7.
- You will get feed previews.

Conclusion:

RSS web feed can be used to open any xml feed webpage without having to see the code and direct content.

Practical - 8

Date

Aim: Study and implementation of Single-Sign-On

Concept: Single Sign On (SSO),openID

Objective: is to understand the concept of access control in cloud and single sign-on (SSO), Use SSO and advantages of it, and also students should able to implementation of it

Scope: installing and using auth0

Technology: auth0

Theory:

Single sign-on (SSO) is a technology which combines several different application login screens into one. With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.SSO is often used in a business context, when user applications are assigned and managed by an internal IT team. Remote workers who use SaaS applications also benefit from using SSO.SSO is an important aspect of many identity and access management (IAM) or access control solutions. User identity verification is crucial for knowing which permissions each user should \have. Cloudflare Zero Trust is one example of an access control solution that integrates with SSO solutions for managing users' identities.

Procedure:

1. Visit https://auth0.com
2. Create a new account
3. Select ‘Company’ Account type, fill company name and company size.
4. tick the advanced settings option.
5. Enter tenant domain name. Ex. ‘<your name><current year>’
6. select region as ‘USA’ & click on create account
7. Navigate to ‘Applications > SSO Integrations’ on the side navigation bar.
8. Click on Create 'New SSO Integration’
9. select the ‘Dropbox integration’ and click on continue

10. Save the integration.
11. Now again perform step 7 and you will find a new integration created.
12. Navigate to ’Security > Multi-factor Auth’
13. click on ‘Phone Message’ section

Conclusion:

Single Sign-On is all about preventing unneeded user interaction while keeping security to the highest level necessary. There doesn't have to be a trade-off between security and usability: If done properly, SSO improves both.

Practical - 9

Date

Aim: User Management in Cloud.

Concept: Administrative features of Cloud Management ,User Management

Objective: is to understand how to create, manage user and group of users accounts.

Scope: Installing and using Administrative features of ownCloud

Technology: ownCloud

Theory:

ownCloud is a suite of client–server software for creating and using file hosting services. ownCloud functionally has similarities to the widely used Dropbox. The primary functional difference between ownCloud and Dropbox is that ownCloud is primarily server software.

ownCloud supports extensions that allow it to work like Google Drive, with online office suite document editing, calendar and contact synchronization, and more. Its openness avoids enforced quotas on storage space or the number of connected clients, instead of having hard limits (for example on storage space or number of users) limits are determined by the physical capabilities of the server.

Procedure:

1. Visit https://demo.owncloud.org
2. Login using the admin credentials. (admin/admin)
3. Open the personal settings menu on the right corner and Go to ‘Users’ page.
4. Add a new user ’<your name>’ and create a new group named ’tycs’.
5. set a new password for the newly created user.
6. also select the group for the user.
7. Go to settings and click on sharing menu item.
8. check all options for sharing and exclude the admin group from sharing.
9. logout of the admin account and again login using the new user’s account.

10. Go to the files section and add a new file and share it

Conclusion:

ownCloud is open by nature and designed to integrate with existing infrastructure, management and security tools. A comprehensive set of APIs and native integrations enable anytime, anywhere access to all your data, wherever it resides.

Practical - 10

Case study on Amazon EC2/Microsoft Azure/Google Cloud Platform