ITA6009 – Cloud Computing

Assignment – II

Reg No – 22MCA0179

Name – Shubham Kumar Gupta

Question 1

Develope a successful Google Application and write the steps involved in deployment it in Google App Engine along with Google's G Cloud data storage facility for App Engine Developers.

Answer → Developing a successful Google Application and deploying it in Google App Engine with Google Cloud data storage involves several steps. Here's a step-by-step guide to help you:-

Step 1 – Design and Develope your Application

Determine requirement and functionality of your application and then develope an application, using your preffered programming language and framework.

Step 2 – Set up a Google Cloud Project

Create a Google Cloud Project. Enable necessary API's for your application. Set up billing for your application.

Step 3 – Configure App Engine

Install necessary tools such as Google Cloud SDK.

Initialize your project with the cloud SDK. Select your projects and configure default settings.

Step 4 — Prepare Your Application for Deployment :

Create a 'yaml' file in the root directory of your application as this file specifies the runtime environment settings, Include any libraries or dependencies required in your project's configuration.

Step 5 — Deploy your Application

Use the cloud SDK to deploy your application, Review the deployment prompts and confirm the deployment.

Step 6 — Set up google cloud datastore

Setup the necessary indexes and configure your DataStore setting based on your application's requirements.

Step 7 — Integrate Data Storage in your Application

Use the google cloud & datastore to store and retrieve data.

Step 8 — Test your Application

Verify that your application is running correctly by accessing the deployed url. Perform through testing.

Step 9 — Monitor and Optimize

Track your application's performance and identify any issues.

Question 2

Elucidate on Cloud Storage Model with a suitable example. List few cloud storage providers and explain any two commonly used cloud platform.

Answer-> Cloud storage is a model that allows individuals and organizations to store, manage and access data remotely over the internet. Instead of relying on a local storage device like hardrives or servers, cloud storage enables users to store their data in distributed storage systems maintained by cloud service providers. This model offers numerous benifits, including scalability, accessibility, data redundancy and cost effectiveness.

Let's consider an example of a small business that needs to store and share files among its employees. Instead of using traditional local storage options, the business decides to leverage cloud storage. They subscribe to a cloud storage service and upload their files such as documents, presentations or spreadsheets, to the cloud. Employees can access these files from any location and any device with an internet connection, enabling seamless collaboration and remote work.

Two commonly used Cloud Platforms which provides cloud storage are :-

ii) Amazon Web Service (AWS)

It is one of the leading cloud service providers, offering a wide range of services and solutions for various cloud computing needs. It provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It provides scalable and flexible cloud solutions used by startups, enterprizes and goverment organizations.

iii) Microsoft Azure

It is another prominent Cloud Computing Platform that provides a comprehensive set of cloud services for building, deploying and managing applications and services. It offers a wide range of services, including virtual machines, storage, databases, AI, analytical, networking and more.

Question 3

Write detailed steps to set the google app engine environment for executing any program of your choice.

Answer→ To set up a google app engine environment for executing any program, the following steps should be followed:

Step 1 – Setup a Google Cloud Project

Create a new Google Cloud Project and Open the google cloud console.

Step 2 – Enable the App Engine API

In the Google Cloud Console, navigate to API section and enable the App Engine Admin API to enable the API of your project.

Step 3 – Install the Google Cloud SDK.

Install the Google Cloud SDK which provide the tool for managing App Engine applications. Download the appropriate SDK for your OS.

Step 4 – ~~Authentricat~~ Authenticate with Google Cloud

Open ~~the~~ the terminal window and run the 'gcloud auth login' command to authenticate ~~wit~~ with Google Cloud.

Step 5 – Initialize the App Enviroment

Initialize the app environment by using the 'gcloud app create' command.

Step 6 – Configure Your App Engine Application

In the root directory create an 'app.yaml' file and specify the runtime, enviroment variables and other settings.

Step 7- Deploy your Application

Run the command 'gcloud app deploy' to deploy your application to App Engine. Wait for the deployment process to complete.

Step 8 - Test Your Application

Once the deployment completes visit your application by running the command 'gcloud app browse' and ~~very~~ verify it's working properly.

Question 4.

Evaluate the security governance and virtual machine security.

Answer → Security Governance

It refers to the framework and processes in a place to manage and oversee an organizations' security stategies, policies and procedures. It envolves establishing a structure to define, implement, monitor and continuously improve security controls and practices.

Key Aspects of security Governance

* Risk Management — Identifying and assessing potential risks to the organizations data and systems and implementing proper contingency measures.

* Security Policies — Developing and documenting policies and procedures that outline the security requirements.

* Compliance and Regulatory Requirements — Ensuring that the organization adheres to applicable laws, regulations and industry standards.

Virtual Machine Security

These are software emulations of physical computer, enabling multiple operating systems and applications to run on a single physical system. Ensuring the security of VMs is crucial to prevent unauthorized access, data breaches and other malicious activities.

Key Aspects of VM Security

* Hypervisor Security — It is the software or firmware layer that enables the creation and management of VMs.

* VM Isolation — VMs should be isolated from each other to prevent unauthorized access and data leakage.

* Access Control — Implementing strong authentication mechanisms, role-based access controls and privileged access management to restrict access to VMs.