**Student Assessment Submission and Declaration**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student name:  **Shahed Mushaileh** | | Assessor name:  **Ghena Barakat** | |
| Issue date (1St Submission):  **12/12/2022** | Submission date (1St Submission):  **17/1/2023** | | Submitted on:  **17/1/2023** |
| In case of resubmission | | | |
| Issue date (2nd Submission): | Submission date (2nd Submission): | | Submitted on: |
| Programme: Higher National Diploma in Cloud Computing | | | |
|  | | | |
| Assignment number and title: 1: Cloud Fundamentals-Basics and Design | | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  Student signature: Date:17/1/2023 |

QUESTION NUMBER ONE:

Cloud computing can be defined as the act of storing and using data, software, or other types of information on distant computers. Online services are offered for cloud computing. An internet connection, enables users to access their work from any location. Private clouds, public clouds, and hybrid clouds are the three main categories of cloud technology. Understanding how these technologies differ is crucial since each has particular advantages and disadvantages that you should take into account before deciding which one to adopt for your company's needs.

There are the following three types of cloud service models -

1. IaaS is an online-managed computing infrastructure. The primary benefit of using IaaS is that it saves users the money and hassle of having to buy and maintain physical servers.

IaaS characteristics

The following are some features of IaaS:

The resources are offered as a service.

Service scalability is very high.

Access via a dynamic and adaptable GUI and API

administrative duties that are automated

Examples: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud

2. For the purpose of developing, testing, running, and managing applications, the PaaS cloud computing platform was developed.

PaaS characteristics

The following describes the traits of PaaS:

1. accessible using the same development application to a variety of users.

2. connects to databases and web services.

3. based on virtualization technology, allowing resources to be readily scaled up or down to meet the needs of the enterprise.

4. support a variety of frameworks and languages.

Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

3. Another name for SaaS is "on-demand software." It is software where a cloud service provider hosts the apps. Internet access and a web browser are required for users to access these applications.

SaaS Characteristics

SaaS services have the following features:

1. controlled from a single location

2. located on a distant server

3. available over the internet

4. Hardware and software updates are not the responsibility of users. Updates are automatically implemented.

5. Pay-per-use is the method used to pay for the services.

The way one is deployed, the infrastructure that supports it, and the degree of automation of the system are frequently differences between deployment models and cloud architecture. The deployment of physical servers, virtual machines (VMs), application delivery networks (ADNs), and containerized systems are a few examples of several deployment techniques. The workings of cloud architecture, however, are very simple to comprehend: when adopting a cloud architecture model, resources are distributed from a centralized place.

Scalability and performance can be automated using cloud architectures.

To facilitate quick loading, the majority of cloud hubs include tens of thousands of servers and storage units. It is frequently feasible to select a region to bring the data "closer" to users. As a result, different cloud computing deployment strategies are grouped according to where they are used.

Types of cloud computing deployment models:

PUBLIC CLOUD:

Public access to it is available. Public cloud deployment strategies are ideal for businesses with varying and growing demands. Additionally, it's a fantastic option for businesses with few security worries. Thus, you pay a cloud service provider for internet-based storage, virtualized computing, and networking services. Additionally, it is an excellent delivery mechanism for teams that work on development and testing. It is the best option for test environments because of its rapid and simple configuration and deployment.

Private Cloud

Naturally, now that you are aware of the potential benefits of the public cloud, you are curious about what a private cloud can accomplish. The private cloud will be a better option for businesses looking for cost-effectiveness and increased control over data and resources.

It implies that it will be administered by your IT staff and integrated with your data center. Alternatively, you could decide to host it elsewhere. The private cloud provides greater opportunities that support the customization needs of certain enterprises. Additionally, it's a smart decision for processes that are mission-critical and may have requirements that change regularly.

Community Cloud

Similar to how the public cloud functions, so do the community cloud. There is only one difference: it only permits access to a particular group of users who have similar goals and use cases. Internally or through a third-party provider, this form of cloud computing deployment architecture is managed and hosted.

Hybrid Cloud:

An amalgam of two or more cloud architectures is referred to as a hybrid cloud. Even though each hybrid cloud model has a unique way of working, they are all connected by the same architecture. Additionally, internal or external providers may contribute resources as part of this cloud computing paradigm implementation.

Less sensitive data can be stored on a public cloud, but a corporation with essential data will prefer to put it there. The practice of "cloud bursting" is another popular usage of the hybrid cloud. It means that even while a company might run an application locally if there is a lot of demand, it may move to the public cloud.

CLOUD ARCHITECTURE:

The architecture of cloud computing combines event-driven architecture and service-oriented design.

The two sections of cloud computing architecture are as follows:

-The front end:

The customer use the front end. It includes programs and client-side interfaces needed to access cloud computing platforms. Web servers (such as Chrome, Firefox, Internet Explorer, etc.), thin & fat clients, tablets, and mobile devices make up the front end.

-The back end:

The service provider makes use of the back end. It oversees the management of all the resources needed to offer cloud computing services. It consists of an enormous amount of data storage, security measures, virtual machines, servers, traffic control systems, etc.

The customer use the front end. Client-side interfaces are included, as well as The components of cloud computing architecture are as follows:

-Client Infrastructure:

A part of the front end is the client infrastructure. It offers a GUI (Graphical User Interface) for cloud communication.

-Application :

Any software or platform that a client wishes to access may be the application.

-Service:

According to the needs of the client, a cloud service handles the services you can access.

QUESTION NUMBER TWO:

Despite the fact that cloud administrations enjoy many benefits for the two clients and associations, how the two utilize the changes. Since undertakings have more command over their information when it is facilitated on a cloud server instead of some other type of framework, the benefits open to them are essentially more noteworthy than those proposed to end buyers. As well as decreasing costs, end clients can profit from security, portability, and access from any place.

Cloud administrations give various advantages that are given to clients. The way that they are faster, more affordable, and less complex to use than regular strategies for information capacity is perhaps their most vital benefit. Clients can keep working without interference and offer information to collaborators or clients with the assistance of cloud administrations, which offer fast information moves. Furthermore, they empower organizations to diminish their IT costs while safeguarding the protection and security of their delicate information.

Since they can be dealt with from any area utilizing remote access instruments like intranet programs or portable applications, cloud administrations are amazing for organizations. They deal with a significant number of the normal tasks required by organizations for their regular activities, for example, programming establishments, reinforcements, document sharing, and inconvenience detailing.

THE BENEFITS OF USING CLOUD SERVICES FOR USERS:

-Flexibility and scalability:

Your company will have more freedom thanks to cloud computing. Without spending money on physical infrastructure, you may easily expand resources and storage up to match business demands. The infrastructure required to handle users' greatest load levels doesn't need to be purchased or built by users. In the same way, if resources aren't being used, they might cut back quickly.

-cost saving:

Pay-as-you-go.

-improved cooperation:

You can make data accessible whenever you need it, wherever you are, thanks to cloud storage. People can access data from anywhere in the world using any device as long as they have an internet connection, thus they are not restricted to a particular place or device.

-advanced protection

Contrary to what many people believe, the depth and breadth of security features, automatic maintenance, and centralized management of cloud computing can actually increase your security posture. Reputable cloud providers also work with the best security professionals and use cutting-edge techniques to ensure stronger security.

-prevention of data loss:

Backup and disaster recovery tools are available from cloud providers. Data loss can be avoided in the event of an emergency, such as hardware failure, malicious attacks, or even a straightforward user error, by storing data in the cloud rather than locally.

THE BENEFITS OF USING CLOUD SERVICES FOR ORGANIZATIONS:

-more rapid time to market:

Developers can speed up work with quick deployments because you can spin up new instances or shut them down in a matter of seconds. In order to test new concepts and create new applications without being constrained by hardware or having to wait through lengthy procurement procedures, cloud computing promotes fresh developments.

-money saved:

You only pay for the resources you really utilize, regardless of the cloud service model you select. This saves you from overspending on your data center's construction and equipment, and it frees up your IT teams' important time to concentrate on more critical tasks.

-advanced protection:

Contrary to what many people believe, the depth and breadth of security features, automatic maintenance, and centralized management of cloud computing can actually increase your security posture. Reputable cloud providers also work with the best security professionals and use cutting-edge techniques to ensure stronger security.

-prevention of data loss:

Backup and disaster recovery tools are available from cloud providers. Data loss can be avoided in the event of an emergency, such as hardware failure, malicious attacks, or even a straightforward user error, by storing data in the cloud rather than locally.

QUESTION NUMBER THREE:

The course of to some degree or totally moving an organization's computerized resources, administrations, information bases, IT assets, and applications to the cloud is known as cloud relocation (cloud migration). Moving to start with one cloud and then onto the next is one more part of cloud movement. The importance of migrating to the cloud is a shorter time to delivery, a lower total cost of ownership (TCO), and more potential for innovation.

Benefits of cloud migration:

1-reduced costs

In addition to the potential to optimize workloads such that they are less expensive to run, there are considerable reductions in resource, maintenance, and real estate expenditures.

2- Scalability and flexibility

-Organizations don't have to pay for and maintain IT assets that they may only use infrequently because they only pay for the cloud resources that they really utilize.

-Organizations are able to change their resources instantaneously and on demand in response to demand fluctuations or when the firm needs more powerful compute resources.

-Many businesses choose a hybrid cloud strategy, where some workloads are moved to the cloud while others remain in their current on-premises environment, to continue to reap the benefits of their existing IT expenditures. (Hybrid clouds may also provide benefits for industry compliance.)

-The majority of cloud platforms keep a presence throughout the world so that businesses can boost performance by executing workloads closer to where their users or clients reside.

3- improved security

To help ensure that an organization's resources are safeguarded, many public clouds come with built-in security features and specialized cloud security solutions. In many instances, security patches are applied automatically by the cloud provider.

4- Compliance

For highly regulated businesses like finance, healthcare, and government, certain cloud platforms have specialist offerings to effortlessly meet compliance needs.

5- Protection, restoration, and failover

The majority of cloud service providers offer built-in, one-click backup and recovery options, which enhance business continuity. Additionally, some service providers let you store backups in various locations.

6- streamlined administration and oversight

If the cloud provider provides a central management tool, organizations can manage and monitor both their on-premises data center and cloud resources from a single screen.

Cloud migration challenges:

-Planning

More so than the relatively simple process of migrating individual workloads to the cloud, a large-scale migration necessitates substantial planning throughout the business. Having a clear strategy in place and enlisting the help of important business, technical, and leadership stakeholders are the first steps in successful migration preparation.

-Cost

Although moving to the cloud can increase ROI in the short- and long-term, doing so will cost money, time, and resources. Cost estimates are crucial for both planning and carrying out a move.

-Safety and adherence

Although cloud providers provide a range of security and compliance options, it is the responsibility of migration customers to deploy the best solutions for their requirements. Organizations can plan their migrations with potential security and compliance considerations in mind.

-Business pauses

Even though migrating enormous volumes of data to the cloud can be done fast, it still necessitates careful preparation to reduce business downtime. Iteratively moving manageable chunks of data over time can help organizations migrate in waves.

-training and adoption within organizations

While IT specialists and developers will discover that the majority of their current talents translate to the cloud, some skill development is still required. Organizations may be successful both during and after migration with the help of upfront cloud skill-building and training.

-selecting a vendor or migration partner

Partners are crucial resources for businesses that lack the internal knowledge or capacity to plan and carry out their move. The ideal migration partner offers expertise and services that are in line with the requirements and commercial concerns of the migrating enterprise.

QUESTION NUMBER FOUR:

\* Private SaaS is a kind of SaaS in which the provider manages and secures the program while it is running on the client's network. availability, upgrades, and dependability are handled by the provider's Private-SaaS architecture. The control plane and data plane are divided in the private SaaS mode, allowing customer data to stay on their network.

While SaaS is very appealing for a wide range of application categories, it is less than suitable in several categories and uses cases. ML Ops tools, DataOps tools, and developer tools are a few examples of these categories. This is especially true for sectors dealing with sensitive customer data, such as FinTech, healthcare, government, and several others. In certain circumstances, businesses use open-source tool variations and self-host them within their network perimeter.

\*Private PaaS makes it easier for IT to design, install, and run on a private network or behind a firewall.

Private PaaS enables you to manage and deploy business apps while still adhering to stringent security and privacy standards. The private PaaS software can be installed on any kind of infrastructure and is compatible with the private cloud, which is run by the IT department of a firm. Developers might see commonalities between private and public PaaS, but the IT department most likely wouldn't in this crucial area.

\* Private IaaS is similar to building a customer a virtual private data center. The user has exclusive access to all of the available resources.

IaaS is not a suitable cloud computing solution and neither is it a replacement for nor comparable to a private cloud. a private cloud is far more reliable and has the capacity to supply computing resources well beyond an IaaS cloud computing platform's infrastructure emphasis.

To begin with, a private cloud can be created separately from other computer resources and work much like an on-site data center. In this situation, it is still possible to administer a private cloud environment remotely while providing a number of other services that are not offered by IaaS-only solutions. Private clouds can be bundled with other cloud computing services offered by cloud suppliers. In the latter scenario, a hosted cloud would include both the conventional infrastructure resources of an IaaS system and provide users with access, security, and IT management capabilities around-the-clock.

\* Clients have less control because public SaaS companies use a multi-tenant infrastructure where customers share networking and computing resources. Because of this, SaaS solutions offer few customization choices, and the majority of users receive the same software regardless of their particular business requirements.

Public SaaS companies provide organizations with cloud-based solutions. They operate out of a central hub where they create, build, update, and rendering software that is remotely accessible to businesses (their clients) over a network of servers provided by SaaS companies.

\* PaaS was initially introduced as a category of public PaaS. Others who had some early success in the public PaaS market include Microsoft's Azure, Engine Yard, and Heroku (now purchased by Salesforce).

The middleware provided by these public PaaS vendors allows developers to install, configure, and administer servers and databases without ever having to deal with the infrastructure side of things. But, public PaaS utilizes the public cloud and is built on top of Infrastructure as a Service (IaaS) from a vendor.

\*Public IaaS: To build or use applications, your company rents infrastructure from the cloud provider and connects to that infrastructure over the Internet.

The public cloud provider provides on-demand access to basic computing, networking, and storage services over the open Internet or dedicated connections.

\* The classic Hybris SaaS model, the HomeBrew Hybrid SaaS model, and the Next Generation of Hybrid SaaS solutions are the three different types of hybrid SaaS models.

The customer has the option to deploy the software as an on-premises solution or as a SaaS service, with the ability to switch between the two as necessary. This is known as the conventional Hybrid SaaS approach.

Proponents believe that this paradigm, which was developed in reaction to the shortcomings of the pure SaaS model, offers the benefits of the SaaS model while minimizing any potential problems.

\* Hybrid PaaS means that a single Apprenda instance may easily combine resources from a company's own data center and those from cloud providers to produce a single operational PaaS. Policies and rules influence factors like application location and routing, enabling developers to create apps that can span providers and migrate between them \*without code changes\*.

\* You can manage your mix of virtual machine- and container-based applications distributed across data centers, public clouds, and edge platforms with hybrid cloud infrastructure as a service (IaaS). No matter where the workloads are placed, this method provides consistent infrastructure and operations. The design of fault tolerance at the application level is made possible by API-based access to hybrid IaaS, enhancing overall resilience.

QUESTION NUMBER THREE:

The course of to some degree or totally moving an organization's computerized resources, administrations, information bases, IT assets, and applications to the cloud is known as cloud relocation (cloud migration). Moving to start with one cloud and then onto the next is one more part of cloud movement. The importance of migrating to the cloud is a shorter time to delivery, a lower total cost of ownership (TCO), and more potential for innovation.

Benefits of cloud migration:

1-reduced costs

In addition to the potential to optimize workloads such that they are less expensive to run, there are considerable reductions in resource, maintenance, and real estate expenditures.

2- Scalability and flexibility

-Organizations don't have to pay for and maintain IT assets that they may only use infrequently because they only pay for the cloud resources that they really utilize.

-Organizations are able to change their resources instantaneously and on demand in response to demand fluctuations or when the firm needs more powerful compute resources.

-Many businesses choose a hybrid cloud strategy, where some workloads are moved to the cloud while others remain in their current on-premises environment, to continue to reap the benefits of their existing IT expenditures. (Hybrid clouds may also provide benefits for industry compliance.)

-The majority of cloud platforms keep a presence throughout the world so that businesses can boost performance by executing workloads closer to where their users or clients reside.

3- improved security

To help ensure that an organization's resources are safeguarded, many public clouds come with built-in security features and specialized cloud security solutions. In many instances, security patches are applied automatically by the cloud provider.

4- Compliance

For highly regulated businesses like finance, healthcare, and government, certain cloud platforms have specialist offerings to effortlessly meet compliance needs.

5- Protection, restoration, and failover

The majority of cloud service providers offer built-in, one-click backup and recovery options, which enhance business continuity. Additionally, some service providers let you store backups in various locations.

6- streamlined administration and oversight

If the cloud provider provides a central management tool, organizations can manage and monitor both their on-premises data center and cloud resources from a single screen.

Cloud migration challenges:

-Planning

More so than the relatively simple process of migrating individual workloads to the cloud, a large-scale migration necessitates substantial planning throughout the business. Having a clear strategy in place and enlisting the help of important business, technical, and leadership stakeholders are the first steps in successful migration preparation.

-Cost

Although moving to the cloud can increase ROI in the short- and long-term, doing so will cost money, time, and resources. Cost estimates are crucial for both planning and carrying out a move.

-Safety and adherence

Although cloud providers provide a range of security and compliance options, it is the responsibility of migration customers to deploy the best solutions for their requirements. Organizations can plan their migrations with potential security and compliance considerations in mind.

-Business pauses

Even though migrating enormous volumes of data to the cloud can be done fast, it still necessitates careful preparation to reduce business downtime. Iteratively moving manageable chunks of data over time can help organizations migrate in waves.

-training and adoption within organizations

While IT specialists and developers will discover that the majority of their current talents translate to the cloud, some skill development is still required. Organizations may be successful both during and after migration with the help of upfront cloud skill-building and training.

-selecting a vendor or migration partner

Partners are crucial resources for businesses that lack the internal knowledge or capacity to plan and carry out their move. The ideal migration partner offers expertise and services that are in line with the requirements and commercial concerns of the migrating enterprise.

QUESTION NUMBER FOUR:

\* Private SaaS is a kind of SaaS in which the provider manages and secures the program while it is running on the client's network. availability, upgrades, and dependability are handled by the provider's Private-SaaS architecture. The control plane and data plane are divided in the private SaaS mode, allowing customer data to stay on their network.

While SaaS is very appealing for a wide range of application categories, it is less than suitable in several categories and uses cases. ML Ops tools, DataOps tools, and developer tools are a few examples of these categories. This is especially true for sectors dealing with sensitive customer data, such as FinTech, healthcare, government, and several others. In certain circumstances, businesses use open-source tool variations and self-host them within their network perimeter.

\*Private PaaS makes it easier for IT to design, install, and run on a private network or behind a firewall.

Private PaaS enables you to manage and deploy business apps while still adhering to stringent security and privacy standards. The private PaaS software can be installed on any kind of infrastructure and is compatible with the private cloud, which is run by the IT department of a firm. Developers might see commonalities between private and public PaaS, but the IT department most likely wouldn't in this crucial area.

\* Private IaaS is similar to building a customer a virtual private data center. The user has exclusive access to all of the available resources.

IaaS is not a suitable cloud computing solution and neither is it a replacement for nor comparable to a private cloud. a private cloud is far more reliable and has the capacity to supply computing resources well beyond an IaaS cloud computing platform's infrastructure emphasis.

To begin with, a private cloud can be created separately from other computer resources and work much like an on-site data center. In this situation, it is still possible to administer a private cloud environment remotely while providing a number of other services that are not offered by IaaS-only solutions. Private clouds can be bundled with other cloud computing services offered by cloud suppliers. In the latter scenario, a hosted cloud would include both the conventional infrastructure resources of an IaaS system and provide users with access, security, and IT management capabilities around-the-clock.

\* Clients have less control because public SaaS companies use a multi-tenant infrastructure where customers share networking and computing resources. Because of this, SaaS solutions offer few customization choices, and the majority of users receive the same software regardless of their particular business requirements.

Public SaaS companies provide organizations with cloud-based solutions. They operate out of a central hub where they create, build, update, and rendering software that is remotely accessible to businesses (their clients) over a network of servers provided by SaaS companies.

\* PaaS was initially introduced as a category of public PaaS. Others who had some early success in the public PaaS market include Microsoft's Azure, Engine Yard, and Heroku (now purchased by Salesforce).

The middleware provided by these public PaaS vendors allows developers to install, configure, and administer servers and databases without ever having to deal with the infrastructure side of things. But, public PaaS utilizes the public cloud and is built on top of Infrastructure as a Service (IaaS) from a vendor.

\*Public IaaS: To build or use applications, your company rents infrastructure from the cloud provider and connects to that infrastructure over the Internet.

The public cloud provider provides on-demand access to basic computing, networking, and storage services over the open Internet or dedicated connections.

\* The classic Hybris SaaS model, the HomeBrew Hybrid SaaS model, and the Next Generation of Hybrid SaaS solutions are the three different types of hybrid SaaS models.

The customer has the option to deploy the software as an on-premises solution or as a SaaS service, with the ability to switch between the two as necessary. This is known as the conventional Hybrid SaaS approach.

Proponents believe that this paradigm, which was developed in reaction to the shortcomings of the pure SaaS model, offers the benefits of the SaaS model while minimizing any potential problems.

\* Hybrid PaaS means that a single Apprenda instance may easily combine resources from a company's own data center and those from cloud providers to produce a single operational PaaS. Policies and rules influence factors like application location and routing, enabling developers to create apps that can span providers and migrate between them \*without code changes\*.

\* You can manage your mix of virtual machine- and container-based applications distributed across data centers, public clouds, and edge platforms with hybrid cloud infrastructure as a service (IaaS). No matter where the workloads are placed, this method provides consistent infrastructure and operations. The design of fault tolerance at the application level is made possible by API-based access to hybrid IaaS, enhancing overall resilience.

QUESTION NUMBER FIVE:

SECTION A:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application | IaaS, SaaS, PaaS | Platform hosting option | Management option | Cloud Models |
| Adobe Acrobat Pro | SaaS | All operating systems | All with the provider | public |
| Data Storage | IaaS | All operating systems | User: applications, data, runtime, middleware, O/S.  Provider: virtualization, servers, storage, networking. | Private, Public |
| Outlook | SaaS | Windows | All with the provider | Public |
| HR System | SaaS | Windows//mac | All with the provider | Public |
| Oracle Database | IaaS | All operating systems | User: applications, data, runtime, middleware, O/S.  Provider: virtualization, servers, storage, networking. | Private/ public |
| Video streaming | SaaS | All operating systems | All with the provider | Public |
| Network | IaaS | All operating systems | User: applications, data, runtime, middleware, O/S.  Provider: virtualization, servers, storage, networking. | Private/ public |
| Sensitive data | IaaS | Linux | User: applications, data, runtime, middleware, O/S.  Provider: virtualization, servers, storage, networking. | private |

SECTION B:

-The sensitive data should be on a private cloud so we can protect it against unauthorized users and breaches. It should be on Linux because it is more secure than windows and mac.

-Video streaming can be on all operating systems, there is no need for high security so it can be on a -public cloud so it is accessible to more users.

-Outlook is provided by windows on a public cloud because there are a lot of users and organizations that need to use it.

-HR system is a SaaS on windows or mac and managed by the provider on a public cloud.

-data storage is an IaaS on all os on private and public clouds.

QUESTION NUMBER SIX:

Organizations considering cloud migration should think about which migration approach best meets their goals. The succinct descriptions of each are as follows:

-Rehost

In order to rehost, or "lift and shift," infrastructure-as-a-service is used (IaaS). Your current data and apps are simply redeployed on the cloud server. It is also an excellent choice if you want to move your applications without changing the code and it is challenging to do so.

The main idea of this method, which is also sometimes referred to as "Lift and shift," is to make as few changes as possible to allow for simple migration to the new infrastructure.

The approach's main risk is its inability to provide a long-term return on investment. If the migration project is sizably vast, then it will be necessary for the project to demonstrate a return on investment for such a multi-year effort, and this could be difficult - particularly if the legacy infrastructure cannot be decommissioned until the end of the program. Since this is a like-for-like transfer, the business advantages will be minimal, necessitating a cost justification based exclusively on IT cost savings.

- Refactor

Refactoring, sometimes known as "lift, tinker, and shift," is the process of fine-tuning and cloud-optimizing your applications. A platform-as-a-service (PaaS) approach is used in this situation. The programs' fundamental architecture hasn't changed, but changes have been made to make greater use of cloud-based technologies.

Any refactor faces the fundamental problem that changes are being made to the application code, making exhaustive regression testing necessary. Automated regression testing is likely to fall short, necessitating end-user testing as well as a corporate sign-off. While the degree of the code changes will vary, it is advised that comprehensive user-based testing be carried out to make sure that the refactoring process did not affect fundamental functionality.

- Revise

Revision requires more substantial modifications to the architecture and code of the systems being migrated to the cloud. This is done to give programs the best chance to utilize the cloud's capabilities, which may necessitate making significant code adjustments. This tactic necessitates considerable knowledge and advanced planning.

The "Revise" option will usually continue to use the original core underlying technical architecture. These updates may also involve some incremental changes to the underlying architecture with new technologies introduced or certain technologies modified.

The difficulties of a revision mostly revolve around the requirement for corporate communication. Revise necessitates the involvement of a full business/IT project team and, consequently, involves a significantly larger change than a pure IT change.

A revision is likely to need integration testing, system testing, and end-to-end process training. If any core data structures have changed, this may affect upstream or downstream systems. This will cost significantly more than a regression test.

-Rebuild

By replacing the current code base with a new one, rebuilding takes the Revise method a step further.

Rebuilding an application is not actually a "migration" project; rather, it is a new build with the public cloud as the destination and substantially the same business purpose as the previous application.

Rebuilding a full application involves significant risks and obstacles. then these risks and challenges are very significant indeed and may be impossible to overcome. In addition to the apparent up-skilling of people that would be necessary, new architectures may also imply considerable changes in your development organization. Upskilling to a new programming language is not a quick cure; while languages can be learned rapidly, As a result, the initial stages of any new project are quite difficult, possibly necessitating outside hiring and expert consulting.

Even harder problems can arise with new architectures. It would be exceedingly risky to start a rebuilding effort for a significant application without any prior expertise with that architecture. the cost and risk to a single project are typically prohibitive.

-Replace

This entails switching to a third-party, prebuilt application that the seller provides. The data is the only component of your existing application that you migrate, and the rest of the system is brand-new.

compared to the far higher danger of a rebuild or a redesign, these are clearly low-risk actions.

The business side of the transition to SaaS presents the most obstacles. There are several instances where a large business process change is required. In cases where an integration exists, this can include reviewing entire business processes with a consequent impact on other current systems.

There is a significant impact on users as well. To exploit the new data from the SaaS system, extensive retraining might be necessary, current contracts with business process outsourcing might need to be renegotiated, and information systems (such as data warehouses) might also require a lot of work.

-Retain:

In some circumstances, it may be conceivable to migrate development and test systems to the public cloud even if the production system stays on-premises.

The cost of system maintenance may rise over time as technology and methods gradually become outdated. Platforms for hardware, software, and technology may stop receiving updates or depreciate. There is never a free option—and sometimes there isn't even a cheap option—in a do-nothing retention policy. Retaining may be a superior choice in many situations as it allows for the modernization of the underlying hardware, software, and platform with no negative influence on business operations.-

-Replatform:

Replatforming is the process of changing the technology platform while making as few modifications to the code as possible. This makes it possible for testing to be restricted to regression testing and performance testing during a migration, resulting in a shorter overall migration period. A platform transition in a cloud environment would also involve a change from self-install software to a PaaS service. Platform changes include moving from an on-premises Oracle database to an OCI database service however, switching from a self-install on-premises database to one on OCI bare metal would only require a simple rehost.

The impact typically pertains to monitoring, patching, updating, backup and recovery, and so on. Many times, the processes will be greatly enhanced (more automation, etc.), and some operational processes might even be completely removed. While advantageous, these changes also necessitate new roles, which may call for employee retraining and organizational transformation.

-Retire:

Although turning off an application should be simple, many organizations may incur charges when they retire a program. Since there is nothing extra being supplied to the business, the cost is frequently absorbed by the IT group. This means that retirement carries some sizeable cost, and those expenses have to come from someplace in the budget. Even worse, if the hardware is only partially depreciated, the asset will continue to be recorded as a cost even after it has been deactivated.

If the hardware is shared, turning down the program can not only result in no cost but also no savings.

In actuality, it is nearly impossible to cost-justify closing a single isolated app in the short term. The best practice is to carry out a retirement project that looks for a large number of legacy software and hardware that no longer add value to the company. In this way, a group of software and hardware may be handled as a cost-saving project and justified as a project with a designated budget.

-Reimagine:

There are instances where the current application has turned out to be more of a business barrier than an enabler. There are occasions when a business legitimately wishes to do something unusual, perhaps by adopting a completely novel business strategy in a particular field.

Business structures and procedures may be drastically altered by the use of mobile devices, rising digitization, and the usage of technologies like the internet of things and artificial intelligence.

QUESTION NUMBER SEVEN:

MICROSOFT AZURE:

Microsoft Virtual Server allows you to create separate virtual machines on top of your Microsoft Windows desktop, where you can install virtually any Intel-architecture operating system. Each virtual machine emulates a complete hardware system—from processor to network card—in a self-contained, isolated software environment, enabling the simultaneous operation of otherwise incompatible systems. Microsoft Virtual Server was a virtualization solution that facilitated the creation of virtual machines on the Windows XP, Windows Vista and Windows Server operating systems. Originally developed by Connectix, it was acquired by Microsoft prior to release. Virtual PC is Microsoft's related desktop virtualization software package.

Virtual machines are created and managed through a Web-based interface that relies on Internet Information Services (IIS) or through a Windows client application tool called VMRCplus

Azure Microsoft's cloud-based object storage solution is called Blob Storage. Large-scale unstructured data storage is where blob storage excels. Unstructured data, such as text or binary data, is data that doesn't follow a certain data model or specification. Through HTTP/HTTPS, users or client programs can access objects in Blob Storage from anywhere in the world. The Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library can all be used to access objects in Blob Storage.

Large volumes of consumer information that is essential to business operations can be managed using relational databases. However, it gets harder and harder to maintain all the data in a database organized, searchable, and safe as it expands and becomes more complex. When this happens, database management systems (DBMS) can aid by providing a layer of relational table management capabilities. Different management systems offer various degrees of organization, scalability, and application, much like different database structures. Relational database management systems (dbases) assist administrators in analyzing and aggregating massive amounts of organized and unstructured data (big data) received in real time in order to discover preset relationships. Users of data may navigate much more easily thanks to RDBMSes, which employ software that offers a consistent interface between users, applications, and the database. The location of your data, the sort of architecture being used, and your scaling plans will all affect the DBMS you choose.

AMAZON:

A virtual server is an element of a physical server made up of CPUs, memory, networking interfaces, and storage that is separated from other virtual servers on the same physical server by software.

An object storage service called Amazon Simple Storage Service (Amazon S3) provides performance, security, and scalability that are unmatched in the market. Any quantity of data can be stored and protected by customers of all sizes and sectors for practically any use case, including data lakes, cloud-native applications, and mobile apps. You may reduce expenses, organize data, and set up precise access controls to satisfy unique business, organizational, and compliance requirements using cost-effective storage classes and simple administration tools.

Amazon Web Services offers the managed SQL database service known as Amazon Relational Database Service (RDS) (AWS). A variety of database engines are supported by Amazon RDS for data storage and organization. Additionally, it supports activities related to relational database maintenance, including data migration, backup, recovery, and patching.

GOOGLE:

The features of a dedicated physical server are duplicated by a virtual server. It resides as a partitioned region inside a physical server transparently to users. Reallocating resources and adjusting to changing workloads are made simple by virtualizing servers.

A computer data storage architecture called object storage commonly referred to as object-based storage, is made to manage enormous amounts of unstructured data. In contrast to previous designs, it organizes data into discrete units that are each associated with metadata and a special identifier that can be used to find and access them. These items—or units—can be kept on-site, but they are usually kept in the cloud, where they are accessible from anywhere. There aren't many scaling restrictions with object storage because of its scale-out capabilities, and it's less expensive to store big data volumes with object storage than with alternatives like block storage.

A program used to create, maintain, and administer relational databases is known as a relational database management system (RDBMS). The most well-known RDBMSs include Oracle Database, PostgreSQL, MariaDB, MySQL, and PostgreSQL.

QUESTION NUMBER EIGHT:

MICROSOFT ARCHITECTURE FRAMEWORK:

A collection of principles known as the Azure Well-Architected Framework can be utilized to raise the standard of a workload. The five pillars of superior architecture make up the framework:

-Reliability: the capacity of a system to perform after failures and recover.

-Security: defending data and apps against dangers.

-Optimization of costs: Keeping expenditures under control to increase value received.

-Excellence in Operation: procedures used in operations to maintain a system in production.

-Efficiency in performance: The ability of a system to adapt to changes in load.

Tools:

-Visual Studio:

Utilizing robust integration tools, cloud apps may be developed, bug-tested, and monitored locally before being sent into production. Create highly secure apps that are tailored for the cloud quickly and effectively by utilizing the variety of Visual Studio features and capabilities.

\*Utilize your entire development machine with a 64-bit Visual Studio that expands effortlessly to large and complicated systems.

\*With local emulators and integration tools, you can create, execute, and debug cloud apps right from the IDE.

\*Manage Azure dependencies and deploy to Azure without leaving the IDE

\*Snapshot debugging makes it simpler to locate and address unhandled errors that occur in production.

- Azure DevOps: With a collection of modern dev services, you can organize better, communicate better, and ship more quickly.

Services for DevOps:

\*Boards of Azure: Utilize tried-and-true agile tools to plan, monitor, and communicate work across your teams and deliver value to users more quickly.

\*Skyline Pipelines: With CI/CD, you can create, test, and deploy applications that run on any platform, language, or cloud. Establish a connection to GitHub or another Git service to continuously deploy.

\*Aspen Repos: Get limitless private Git repositories stored in the cloud and work together to improve your code using pull requests and cutting-edge file management.

\*Test Plans for Azure: Using manual and exploratory testing tools, you can ship and test products with confidence.

\*Artifacts of Azure: With just one click, you can add artifacts to your CI/CD pipelines and create, host, and share packages with your team.

\*The Extensions Market: Access add-ons for 1,000 other apps and services, like SonarCloud, Slack, and more.

GOOGLE ARCHITECTURE FRAMEWORK:

To assist architects, developers, administrators, and other cloud practitioners in designing and running a safe, effective, robust, high-performing, and cost-effective cloud architecture, the Google Cloud Architecture Framework offers guidelines and specifies best practices. The design guidelines and best practices that make up the Architecture Framework are validated by a cross-functional team of specialists at Google. The Architecture Framework is carefully curated by the team to take into account the ever-expanding capabilities of Google Cloud, business best practices, local knowledge, and your feedback. Applications created for the cloud as well as workloads moved from on-premises to Google Cloud, hybrid cloud deployments, and multi-cloud environments are all covered by the design recommendations in the Architecture Framework.

There are six groups into which the Google Cloud Architecture Framework is divided:

-a system's design:

The Google Cloud Architecture Framework is built on this category. Learn about the Google Cloud products and services that assist system design, as well as the architecture, components, modules, interfaces, and data required to satisfy the requirements of cloud systems.

-excellence in operations:

Deploy, run, monitor, and manage your cloud workloads effectively.

-Privacy, security, and compliance:

Optimize the security of your data and workloads in the cloud, consider privacy when designing, and comply with legal and industry standards.

-Reliability:

Create and manage highly available, robust workloads in the cloud.

-Cost reduction:

Maximize the return on your Google Cloud investment.

-performance improvement:

Design and optimize the performance of your cloud resources.

Tools:

-Cloud SDK:

Tools and libraries for connecting with Google Cloud services and products.

\* Utilize client libraries for Java, Python, Node.js, Ruby, Go,.NET, and PHP to integrate with APIs.

\*Using the Google Cloud CLI, you may script or interact with cloud resources at scale.

\*Emulators for Pub/Sub, Spanner, Bigtable, and Datastore can speed up local development.

-Cloud Deployment Manager: The construction and maintenance of Google Cloud resources are automated via the infrastructure deployment service known as Google Cloud Deployment Manager. Create deployments with a variety of Google Cloud services, such as Cloud Storage, Compute Engine, and Cloud SQL, set to cooperate by writing customizable template and configuration files.

AMAZON ARCHITECTURE FRAMEWORK:

With the aid of AWS Well-Architected, cloud architects can create infrastructure that is reliable, secure, performant, and cost-effective for a range of applications and workloads. AWS Well-Architected offers clients and partners a standardized method for assessing architectures and putting into practice scalable designs. It is built around six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. Domain-specific lenses, practical labs, and the AWS Well-Architected Tool are all parts of the AWS Well-Architected Framework. The AWS Well-Architected Tool, free to use in the AWS Management Console, offers a way to frequently assess workloads, spot high-risk problems, and track advancements. In addition, AWS offers access to a partner program with hundreds of members called AWS Well-Architected.

The six pillars:

-Pillar of Operational Excellence:

The operating and monitoring of systems as well as ongoing process and procedure improvement are the main objectives of the operational excellence pillar. Automating changes, responding to events, and establishing standards to govern everyday operations are important subjects.

- Security Measure:

The protection of data and systems is the main goal of the security pillar. Data confidentiality and integrity, user authorization management, and creating controls to identify security incidents are important subjects.

- Integrity Pillar:

The reliability pillar is concerned with workloads working as planned and with failure recovery times in order to keep up with demand. Designing distributed systems, planning for disaster recovery, and adjusting to shifting requirements are important topics.

- Efficiency Performance Pillar:

The performance efficiency pillar concentrates on the organized and efficient distribution of computing and IT resources. The selection of resource types and sizes that are optimized for workload requirements, performance monitoring, and sustaining efficiency as business demands change are important themes.

- Pillar for Cost Optimization:

The goal of the cost optimization pillar is to reduce wasteful spending. Understanding spending patterns and managing fund distribution, choosing the appropriate kind and amount of resources, and growing to meet corporate objectives without going overboard are important themes.

- Pillar of Sustainability:

The sustainability pillar is concerned with reducing the negative effects that using cloud workloads has on the environment. To limit needed resources and lessen downstream repercussions, key topics include a shared responsibility model for sustainability, assessing impact, and maximizing use.

Tools:

-AWS CodeCommit: AWS CodeCommit is a managed source control solution that is safe, scalable, and makes it simpler for teams to work together on code. You no longer have to manage your own source control system or be concerned about scaling its infrastructure thanks to AWS CodeCommit.

-CloudFormation: is a service that provides organizations and developers with a convenient method to gather linked AWS and outside resources, provision them, and manage them in a systematic and predictable way.

In a straightforward, declarative manner that abstracts away the complexities of particular resource APIs, developers may deploy and upgrade compute, databases, and a variety of other resources. With the help of automatic rollbacks, automated state management, and resource management across accounts and regions, AWS CloudFormation enables the repeatable, predictable, and safe management of resource lifecycles. Recent improvements and options enable a variety of resource creation methods, such as using the AWS CDK for programming in higher-level languages, importing preexisting resources, detecting configuration drift, and a new Registry that makes it simpler to create custom types that inherit many fundamental CloudFormation advantages.

QUESTION NUMBER NINE:

“AWS pricing:

|  |  |
| --- | --- |
| S3 Standard - General purpose storage for any type of data, typically used for frequently accessed data |  |
| First 50 TB / Month | $0.023 per GB |
| Next 450 TB / Month | $0.022 per GB |
| Over 500 TB / Month | $0.021 per GB |
| S3 Intelligent - Tiering\* - Automatic cost savings for data with unknown or changing access patterns |  |
| Monitoring and Automation, All Storage / Month (Objects > 128 KB) | $0.0025 per 1,000 objects |
| Frequent Access Tier, First 50 TB / Month | $0.023 per GB |
| Frequent Access Tier, Next 450 TB / Month | $0.022 per GB |
| Frequent Access Tier, Over 500 TB / Month | $0.021 per GB |
| Infrequent Access Tier, All Storage / Month | $0.0125 per GB |
| Archive Instant Access Tier, All Storage / Month | $0.004 per GB |
| S3 Intelligent - Tiering\* - Optional asynchronous Archive Access tiers |  |
| Archive Access Tier, All Storage / Month | $0.0036 per GB |
| Deep Archive Access Tier, All Storage / Month | $0.00099 per GB |
| S3 Standard - Infrequent Access\*\* - For long lived but infrequently accessed data that needs millisecond access |  |
| All Storage / Month | $0.0125 per GB |
| S3 One Zone - Infrequent Access\*\* - For re-createable infrequently accessed data that needs millisecond access |  |
| All Storage / Month | $0.01 per GB |
| S3 Glacier Instant Retrieval\*\*\* - For long-lived archive data accessed once a quarter with instant retrieval in milliseconds |  |
| All Storage / Month | $0.004 per GB |
| S3 Glacier Flexible Retrieval (Formerly S3 Glacier)\*\*\*- For long-term backups and archives with retrieval option from 1 minute to 12 hours |  |
| All Storage / Month | $0.0036 per GB |
| S3 Glacier Deep Archive\*\*\* - For long-term data archiving that is accessed once or twice in a year and can be restored within 12 hours |  |
| All Storage / Month | $0.00099 per GB |

REGIONS:

(North America, US West (Oregon) Region, Availability Zones: 4, Launched 2011, Local Zones: 7, Launched 2019)

(US East (Northern Virginia) Region, Availability Zones: 6, Launched 2006, Local Zones: 10, Launched 2020)

(US West (Northern California) Region, Availability Zones: 3\*, Launched 2009)

(US East (Ohio) Region, Availability Zones: 3, Launched 2016)

(Canada (Central) Region\*\*, Availability Zones: 3, Launched 2016)

(GovCloud (US-West) Region, Availability Zones: 3, Launched 2011)

(GovCloud (US-East) Region, Availability Zones: 3, Launched 2018)

(South America (São Paulo) Region, Availability Zones: 3\*, Launched 2011)

(Europe (Ireland) Region, Availability Zones: 3, Launched 2007)

(Europe (Frankfurt) Region, Availability Zones: 3, Launched 2014)

(Europe (London) Region, Availability Zones: 3, Launched 2016)

(Europe (Paris) Region, Availability Zones: 3, Launched 2017)

(Europe (Stockholm) Region, Availability Zones: 3, Launched 2018)

(Europe (Milan) Region, Availability Zones: 3, Launched 2020)

(Europe (Zurich) Region, Availability Zones: 3, Launched 2022)

(Europe (Spain) Region, Availability Zones: 3, Launched 2022)

(Middle East (Bahrain) Region, Availability Zones: 3, Launched 2019)

(Middle East (UAE) Region, Availability Zones: 3, Launched 2022)

(Africa (Cape Town) Region, Availability Zones: 3, Launched 2020)

(Asia Pacific (Singapore) Region, Availability Zones: 3, Launched 2010)

(Asia Pacific (Tokyo) Region, Availability Zones: 4, Launched 2011)

(Asia Pacific (Seoul) Region, Availability Zones: 4, Launched 2016)

(Asia Pacific (Mumbai) Region, Availability Zones: 3, Launched 2016)

(Asia Pacific (Hong Kong) Region, Availability Zones: 3, Launched 2019)

(Asia Pacific (Osaka) Region, Availability Zones: 3, Launched 2021)

(Asia Pacific (Jakarta) Region, Availability Zones: 3, Launched 2021)

(AWS Asia Pacific (Hyderabad) Region, Availability Zones: 3, Launched 2022)

(Mainland China (Beijing) Region, Availability Zones: 3)

(Mainland China (Ningxia) Region, Availability Zones: 3)

(Australia (Sydney) Region, Availability Zones: 3, Launched 2012)

Microsoft pricing:

\*Microsoft 365 Business Basic USD$6.00 Microsoft 365 Business BasicUSD$6.00user/month (Annual subscription–auto-renews)1 Web and mobile versions of Office apps only Chat, call, meet up to 300 attendees 1 TB of cloud storage per user Business-class email

Standard security Anytime phone and web support Web and mobile apps and services:3,4 (MicrosoftWord/ MicrosoftExcel/ MicrosoftPowerPoint/ MicrosoftTeams/ MicrosoftOutlook/ MicrosoftExchange/ MicrosoftOneDrive/ MicrosoftSharePoint).

\*Microsoft 365 Apps for business USD$8.25 Microsoft 365 Apps for businessUSD$8.25user/month (Annual subscription–auto renews)1 Desktop versions of Office apps with premium features 1 TB of cloud storage per user Standard security Anytime phone and web support Desktop, web, and mobile apps and services:( MicrosoftWord/ MicrosoftExcel/ MicrosoftPowerPointl/ MicrosoftOutlook/ MicrosoftOneDrive/ MicrosoftAccess (PC only)/ MicrosoftPublisher (PC only))

\*Microsoft 365 Business Standard USD$12.50 Microsoft 365 Business StandardUSD$12.50user/month (Annual subscription–auto renews)1 Everything in Business Basic, plus: Desktop versions of Office apps with premium features Easily host webinars Attendee registration and reporting tools Manage customer appointments Desktop, web, and mobile apps and services:( MicrosoftWord/ MicrosoftExcel/ MicrosoftPowerPoint/ MicrosoftTeams/ MicrosoftOutlook/ MicrosoftOneDrive/ MicrosoftSharePoint/ MicrosoftExchange/ MicrosoftAccess (PC only)/MicrosoftPublisher (PC only))

\*Microsoft 365 Business Premium USD$22.00 Microsoft 365 Business PremiumUSD$22.00user/month (Annual subscription–auto renews)1 Everything in Business Standard, plus: Advanced security Access and data control Cyberthreat protection Desktop, web, and mobile apps and services:( MicrosoftWord/ MicrosoftExcel/ MicrosoftPowerPoint/ MicrosoftTeams/ MicrosoftOutlook/ MicrosoftOneDrive/ MicrosoftSharePoint/ MicrosoftExchange/ MicrosoftIntune/ MicrosoftAzure Information Protection/ MicrosoftAccess (PC only)/ MicrosoftPublisher (PC only))

Region:

AUSTRALIA, BELGUIM, BRAZIL, CANADA, CHILE, CHINA, DENMARK, EUROPE, AFRICA, FINLAND, FRANCE, GERMANY, GREECE, INDIA, INDONESIA, PALESTINE, ITALY, MALAYSIA, MEXICO,NEW ZEALAND, NORWAY, POLAND, QATAR, SPAIN, SWEDEN, TAIWAN, UAE, UK, US.”

QUESTION NUMBER TEN:

The benefits of using CSP technologies to construct previous apps:

-cost reduction

One of the main advantages of cloud computing is cost savings. Due to the lack of investments in physical hardware, it allows you to significantly reduce your capital costs. Additionally, the hardware maintenance does not require trained staff. The cloud service provider handles equipment procurement and maintenance.

-tactical advantage

A competitive advantage over your rivals is provided by cloud computing. One of the best benefits of cloud services is that you can always access the newest programs without having to spend time or money installing them.

-High Speed

Using the cloud, you can rapidly and with fewer clicks install your service. You can obtain the resources needed for your system more quickly thanks to this speedier deployment.

-Data backup and restoration

When data is kept on the cloud, it is simpler to back it up and restore it, which is a labor-intensive procedure when done on-premises.

-Integrating software automatically

Software integration takes place automatically in the cloud. As a result, you don't have to exert additional effort to integrate and configure your programs according to your preferences.

-Reliability

One of the main advantages of cloud hosting is reliability. You can always receive an immediate update on changes.

-Mobility

Employees may simply access all available services whether they are working on-site or in remote locations. All they require is Internet access.

- Unlimited amount of storage

Storage space is virtually endless in the cloud. You may always quickly increase your storage space for very low monthly costs.

-Collaboration

The cloud computing platform makes it possible for workers with different locations to collaborate safely and conveniently.

-Quick Deployment

The last but not least benefit of cloud computing is quick deployment. Therefore, if you want to use the cloud, your entire system can be up and running in a matter of minutes. However, the length of time relies on the type of technology utilized in your company.

Drawbacks of using CSP technologies to construct previous apps:

-Performance May Differ

Your application is running on the server that is also providing resources to other organizations when you are working in a cloud environment. Any selfish actions or DDOS attacks on your tenant could have an impact on how well your shared resource performs.

-Technical Problems

Technical problems and outages are a given with cloud computing. Despite upholding strict maintenance standards, even the greatest cloud service provider businesses occasionally run into problems of this nature.

-Risk to Security in the Cloud

Security risk is another disadvantage of using cloud computing services. You should be fully informed before implementing cloud technology that you will be handing over all of your company's sensitive data to a third-party cloud computing service provider. This data might be accessed by hackers.

-Downtime

Working with cloud computing requires taking into account downtime. This is due to the possibility of power outages, poor internet access, service maintenance, etc. for your cloud provider.

-Internet Connectivity

For cloud computing to work, you need to have good Internet connectivity. Cloud access requires an active internet connection. Additionally, there is no alternative means for you to collect data from the cloud.

-Reduced Bandwidth

Many cloud storage service providers place restrictions on users' bandwidth utilization. Therefore, if your company exceeds the allotted amount, the additional fees could be very expensive.

-Absence of Support

The consumers of cloud computing companies are not given adequate support. Additionally, they encourage users to rely on FAQs or online support, which can be time-consuming for non-technical people.

QUESTION NUMBER ELEVEN:

The security features offered by amazon:

- Identification and access control:

You can securely manage identities, resources, and permissions at scale with the aid of AWS Identity Services. To get started quickly and control access to your workloads and apps, AWS offers identity services for your workforce and customer-facing applications.

- Detection:

AWS detection and response services assist you in locating potential security flaws, threats, or unanticipated actions so you may act swiftly in the event that unapproved or malicious activity is taking place within your environment.

- protection for networks and applications:

You may implement fine-grained security policy at network control points throughout your organization with the aid of network and application protection services. You can use AWS services to examine and filter traffic at the host-, network-, and application-level boundaries to stop illegal resource access.

- Data security:

AWS offers services to assist you in preventing unwanted access to your data, accounts, and workloads. To help you safeguard your data and workloads, AWS data protection services offer encryption capabilities, key management, and sensitive data discovery.

The security features offered by Microsoft:

- Protection against viruses and threats - Keep an eye on potential risks to your device, run scans, and get updates to help find the newest dangers.

- Account security - Access account settings and sign-in options, such as Windows Hello and dynamic lock.

- Manage firewall settings and keep an eye on what's happening with your networks and internet connections using the firewall and network protection feature.

- Update your Microsoft Defender SmartScreen settings for app and browser control to better safeguard your device from potentially harmful downloads, programs, files, and websites. You'll have exploit protection and be able to change the settings for your devices' protection.

- Review built-in security features for your device to help defend it from attacks by malicious software. Device security.

- Performance and health information for your device may be viewed, and the most recent Windows update can be used to maintain your device clean and up to date.

- Options for families: Monitor your children's online activity and the devices in your home.

The security features offered by google:

1- Transparency in Access: Visibility of cloud providers through almost real-time logs.

-Clarify access approval with Access approval.

-Access justifications explain why access is necessary.

- Identification of the method and resource.

2- Certain Workloads: restrictions on compliance and security for delicate workloads.

-Enforcing the location of data.

-Restrict staff access.

-Built-in security controls.

-Product deployment location enforcement.

3- Authorization in binary: On Kubernetes Engine, only deploy trusted containers.

-Creating policies based on your security requirements.

-Policy enforcement and verification.

-Integration with the Cloud Security Command Center.

-Logging audits.

4- Chronicle: To quickly identify threats, extract signals from your security telemetry.

-Elastically endless.

-Price fixed.

- Unmatched storage.

-Simple to control.

5- Asset Cloud Inventory: View, keep an eye on, and examine Anthos and Google Cloud assets across projects and services.

-Complete inventory management service.

-Export all of your assets at once.

-History of export asset changes.

-Real-time alerts for asset configuration changes.

6- Avoiding Data Loss in the Cloud: a platform for the classification, examination, and redaction of sensitive material.

-Finding and classifying data.

-To safely access more of the cloud, mask your data.

-Analyze the risk of re-identification in structured data.

7- Cloud IDS: Managed network threat detection with industry-leading protection that is cloud-native.

-Identify network-based dangers such as malware, spyware, and command-and-control attacks.

-High-performance, managed, cloud-native, and simple deployment.

-Built with industry-leading threat detection technologies from Palo Alto Networks.

8- Cloud Key Administration: Google Cloud encryption key management.

-Manage encryption keys centrally.

-HSM provides hardware key security.

-EKM should support supporting external keys.

-Be the final decider for who has access to your data.

QUESTION NUMBER TWELVE:

The most typical technical issues that occur in a Cloud Computing platform and propose acceptable solutions:

--Network latency is the delay in data transmission brought on by both network congestion and the distance between the transmitter and recipient. Delays in obtaining data and services as well as poor performance may result from this. Cloud service companies employ Content Delivery Networks (CDNs) to transfer data among several locations, hence minimizing the distance between the sender and receiver, to alleviate this problem.

-- Security flaws: Cloud environments are susceptible to security lapses like malware and hacking attempts. Cloud service providers put in place security measures like firewalls, intrusion detection and prevention systems, and antivirus software to lessen these threats. Implementing best practices like multi-factor authentication, access controls, and regular security audits is also crucial.

-- Scalability: Cloud environments need to be scalable in order to adapt to changing user needs. When dealing with abrupt surges in traffic or the requirement for data storage, this might be difficult. In order to avoid overtaxing a single server, cloud providers utilize load balancers to split traffic among several servers and autoscaling to automatically modify capacity based on demand.

-- Data Loss: Although cloud service providers employ a variety of storage methods, including object storage, block storage, and file storage, data loss can still happen as a result of hardware malfunctions, software defects, or human mistake. Utilizing data replication, data replication, backups, and disaster recovery plans are used by disaster recovery plans by cloud providers to reduce this risk. Data replication, data replication, backups, and disaster recovery plans are used by cloud providers to ensure that data can be retrieved.

-- Compliance: Cloud service providers are required to abide by a number of laws, including HIPAA, SOC 2, and PCI DSS. To comply with these laws, cloud service providers must adopt security measures and controls. They must also offer compliance certifications as proof that they do so.

QUESTION NUMBER THIRTEEN:

Because remote working is so common, and as more businesses rely on cloud-based technology, it's critical to guarantee that systems are safe and that sensitive data is kept private. Although using cloud storage is not always risky, there are some security flaws that companies should be aware of and know how to avoid.

Some of the most typical issues include the following:

-a violation of data: Data breaches caused by inadequate security procedures are a major cloud security issue. Businesses must ensure that the online storage service they choose ensures total protection against data leaks and unauthorized access. (affects the user).

- loss of data: Data loss is a problem if organizations don't save their information with a company that offers dependable backups because not all cloud service providers are prepared to handle creating backups when necessary. (affects the business).

-data theft: Cloud services frequently have publicly available URLs for uploading and downloading files; if inadequate security controls are applied, this could lead to data leakage. Businesses must use robust link encryption and limited access to reduce this risk. (affects both).

- hijacking an account: The best practice is to use strong passwords that are changed frequently because cybercriminals can gain login information to access sensitive data stored in the cloud and are known to exploit weaknesses in network architecture. (affects the user).

-Insider dangers: Administrators, developers, and other dependable staff members with access to sensitive information could accidentally compromise security. It is crucial to train your workers on how to use cloud software properly. (affects the business).

- Insecure API: Cloud services with insecure APIs put the integrity and confidentiality of data at risk, and you run the risk of having your data and systems exposed. Hackers typically employ three different sorts of attacks to try to exploit APIs: brute force, denial-of-service, and man-in-the-middle. ( affects both).

-Absence of repository management: Normally, you have little control over where your data is kept; in the event of a breach, you might not even be aware of it or where it took place. It is suggested that administrators are aware of the security precautions in place at each location and encrypt their data before uploading in order to reduce this danger. (affects both).

legal issues in cloud computing:

- Protection of Data (affects the user).

When using the cloud for your business operations, data privacy is one of the most important legal concerns you need to take into account. If your business involves processing any kind of personal data about people, it is very crucial. Data protection laws include tight guidelines on how you must manage people's personal information.

Most of these laws, including the General Data Protection Regulation, which governs how EU residents' data is handled, prohibit the automatic export of personal information about individuals to the cloud without first acquiring the requisite authorization. The regulations' requirements for data protection must also be followed by you. Strict penalties would be applied if this were not done.

- Data Security and Privacy (affects the business).

Data security and privacy are other crucial legal concerns in cloud computing that you should be aware of. The reputation of your business may suffer if a third party gains unlawful access to private information about your clients. In the event of a security breach, your company runs the danger of losing private and sensitive data. Additionally, you might have to pay your customer for breaching their data privacy, which would be very expensive for your company.

- Ownership of Data (Intellectual Property Rights) (affects the business).

It is safe to assume that you are the sole owner of whatever data your organization sends to the cloud. It is best to explicitly state in your Service Level Agreement (SLA) with the CSP that your business has complete ownership of the data kept in the cloud and can access it whenever you choose. These protections must be in place, particularly with regard to data generated in the cloud. Because the freshly generated data was produced in the cloud using a data analytics tool, the CSP might want to claim it.

- Regulatory Issues (affects both).

One of the legal concerns with cloud computing is the question of the variations in laws that apply in several jurisdictions. For instance, in some places, the government can mandate that CSPs share client information. However, in certain other jurisdictions, data kept in the cloud is expressly protected, and in those jurisdictions, governments are prohibited from accessing it without completing the proper procedures.

QUESTION NUMBER FOURTEEN:

There are various legal and security aspects to take into account when migrating a data center to the cloud, including networking, servers, storage, and virtualization.

Security monitoring: Implementing security monitoring and log management is one way to promptly identify and respond to security occurrences. Intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, and security orchestration, automation, and response (SOAR) systems can be used to accomplish this.

Data sovereignty: When storing data in the cloud, the rules and regulations of the country or region in which the data is kept are applicable.

Utilizing cloud service providers with data centers spread throughout the globe and encrypting sensitive data are two solutions.

Role-based access control and multi-factor authentication are two approaches to access control that help limit who has access to cloud services and data.

Response to incident: Environments hosted in the cloud are susceptible to data breaches and online attacks.

Setting up an incident response strategy, testing it periodically, and upgrading it as needed are some solutions.

Data encryption can be used to protect data while it is in transit and at rest because cloud-based data is vulnerable to hackers. To do this, encryption technologies like SSL/TLS and AES can be employed.

Audit and compliance: Cloud-based environments are routinely evaluated to ensure sure they are in compliance with legal and regulatory norms.

The use of regular compliance checks on cloud resources and meticulous documentation of cloud deployments and configurations are some solutions.

References:

Ping, Yang (2012) ‘A Network Storage Framework Based on SAN’, 7th International Conference on Computer Science & Education, pp. 818 – 82.

Ready (2017) IT Disaster Recovery. Available at: https://www.ready.gov/business/implementation/IT. (Accessed: 8 December 2017).

Reeve (2017), ‘Big Data and NoSQL: The Problem with Relational Databases’, DELLEMC, 7 September. Available at: https://infocus.emc.com/april\_reeve/big-data-and-nosql-the-problem-with-relational-databases/. (Accessed: 8 December 2018).

TechTarget (2017), ‘Building an effective data governance’, TechTarget.

Tsai (2016), ‘Server Virtualization and OS Trends’, Spiceworks, 30 August. Available at https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends. (Accessed: 8 December 2018).

B. Hayes, “Cloud computing,” Communications of the ACM, vol. 51, no. 7, pp. 9–11, 2008.

View at: Google Scholar

M. Armbrust, A. Fox, R. Griffith et al., “Above the clouds: a berkeley view of cloud computing,” Tech. Rep. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

View at: Google Scholar

R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

View at: Publisher Site | Google Scholar

O. Abdul-Rahman, M. Munetomo, and K. Akama, “Live migration-based resource managers for virtualized environments: a survey,” in Proceedings of the 1st International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING '10), pp. 32–40, 2010.

View at: Google Scholar

P. Patel, A. Ranabahu, and A. Sheth, “Service level agreement in cloud computing,” in Proceedings of the Cloud Workshops at OOPSLA, pp. 1–10, 2009.

View at: Google Scholar

https://docs.oracle.com/en/cloud/foundation/cloud\_strategy/modernizationpatterns/replace.html

https://cloud.google.com/learn/advantages-of-cloud-computing

https://livebook.manning.com/book/amazon-web-services-in-action/chapter-3/

"Cloud Computing Issues, Challenges and Solutions" by P. V. S. S. S. N. Murty, and S. R. K. S. Prasad (2015)

"Cloud Computing: Issues and Challenges" by R. Buyya, and R. N. Calheiros (2011)

"AWS Well-Architected Framework" by Amazon Web Services (2021)

"Azure Well-Architected Framework" by Microsoft Azure (2021)

https://csp.withgoogle.com/docs/why-csp.html

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

https://tech.hindustantimes.com/tech/news/google-chrome-s-five-security-features-that-every-user-should-know-story-sctdygOtXklU4aIVx3U30H.html

https://cloud.google.com/products/security-and-identity