Final Term Paper (Spring - 2020)
Cloud Computing

Name: Syed M. Hassan Shah	**ID #: 6853**

Semester: 8th section 'B' **Date: 25, June, 2020**
Time: 6 hours **Total Marks: 50**
Instructor: M Omer Rauf

Note: Attempt all Questions. Answers should be in your own words. Plagiarism will not be tolerated, if detected, it will lead to failure.

Question No. 1: (20)

a. Explain in detail network and cloud-based storage.

Answer:

Cloud storage is the next step in the evolution of network storage devices. Instead of storing the data locally, the data can be stored on cloud and can be accessed through web. The user can have virtually unlimited storage space available at affordable rates.

There are various modes of data access in Cloud: Using web browser interfaces to move the files to and from the cloud storage. Through a mounted disk drive that appears local to the user's computer. Through API calls to access the cloud storage. There are a number of cloud storage providers which offer file storage, sharing and synchronization. Such as:

1. Carbonite
2. pCloud
3. Dropbox
4. ElephantDrive

These providers offer a certain volume of free storage as well as paid storage at low prices. Computers attached to a local area network (LAN) may require additional storage space to support file sharing, file replication and storage for large files

Traditionally this additional space is provided through file servers which have larger disk capacity. With the evolution of computer networks, the file server was extended through the use of storage area network (SAN).The SAN enabled storage devices are attached to the network. The software running over SAN devices allows direct access to these devices throughout network

Advantages of network storage (particularly of SAN) are:

- Data reliability and reconstruction through replication.
- Better performance than file server.
- Compatibility with common file systems and operating systems.
- Best choice for backups.

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure

Cloud NAS is a popular storage choice for people looking to use cloud storage for applications, user file systems or data archive. But we still see a lot of confusion when people hear the terms “Cloud network attached storage”, “Cloud-based NAS”, or cloud NAS service

A cloud NAS works like the legacy, on-premises NAS currently in a lot of data centers. But, unlike traditional NAS or SAN infrastructures, a cloud NAS is not a physical machine. It’s a virtual appliance designed to work with and leverage cloud-based storage to give you all of the functionality you’d expect from a premises-based hardware NAS or SAN

Cloud NAS is a “NAS in the cloud” that uses cloud computing to simplify infrastructure and provide flexible deployment options while reducing costs. Most cloud NAS service solutions work in cloud environments like Amazon Web Services (AWS) and Microsoft Azure. Cloud-based NAS uses easily expandable cloud storage as a central source for storage while still providing common enterprise NAS features

Benefits of using Cloud NAS service:

- **Price/Performance Flexibility:** With the right cloud NAS, you have numerous options on what type of cloud storage to use. Low performance Cloud Object storage can be used for use cases that don’t require high performance. But for a price, you can also satisfy HPC (high performance computing) level SLAs. With the right combination of Virtual Machines running your Cloud NAS controller head with the right backend cloud storage, you can meet your storage requirements for just about any project
- **Eliminate Legacy NAS Systems Refresh:** How do you predict exactly how much storage and performance from that storage you will need over the next 12 months? Do you ever have an unexpected project come up that requires more storage possibly at a different performance level? With legacy hardware NAS solutions, you usually get locked into a long-term contract, and if something changes, you incur the overhead and costs with a “forklift” upgrade. With a Cloud NAS, you are in control. You can create the storage you need when you need it, for as long as you need it without signing long-term contracts or renewals.
- **Built-in Data Resiliency:** Most cloud storage has data resiliency built in by storing multiple copies of data on multiple disks. This resiliency does not replace the need for High Availability, SnapShots and backups, but it nice to have this level of resiliency built right into the storage used by your Cloud NAS

- **Pay as You Go and Reduce Costs:** You only pay your cloud provider for the storage you need. With cloud storage becoming cheaper, you can instantly scale your cloud instances to best suit your needs. Or, you can even use tiered storage and push legacy data to low-cost storage and store frequently-accessed data in top-tiered storage to maintain performance for your “hot” data.

Drawbacks of using NAS:

Performance: Because of the Internet based access, the cloud storage can never be as fast as SAN or NAS based local storage.

Security: Not all the users may be able to trust the cloud provider for the users’ data.

Data orphans: The user has to trust the data deletion policies of the provider. The files (on cloud storage) deleted by the user may not be immediately (or ever) be deleted from the cloud storage.

Question No. 2: (20)

a. Explain in detail web application and multitenant technology.

Answer:

A web application is application software that runs on a web server, unlike computer-based software programs that are stored locally on the Operating System of the device. Web applications are accessed by the user through a web browser with an active internet connection.

Web applications include online forms, shopping carts, word processors, spreadsheets, video and photo editing, file conversion, file scanning, and email programs such as Gmail, Yahoo and AOL. Popular applications include Google Apps and Microsoft 365.

The term "software multitenancy" refers to software architecture in which a single instance of software runs on a server and serves multiple tenants. Systems designed in such manner are often called shared (in contrast to dedicated or isolated). A tenant is a group of users who share a common access with specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance - including its data, configuration, user management, tenant individual functionality and non-functional properties. Multitenancy contrasts with multi-instance architectures, where separate software instances operate on behalf of different tenants.

Multi-tenancy is a key to successful and sustainable cloud-based systems. Creating a web application framework for multiple tenants from scratch is challenging. To create an extensible, stable and robust multi-tenant web application framework developers have to understand how a web application framework is structured and how a web request is handled for each user of a specific tenant. This knowledge often takes software architects and developers a lot of effort to obtain. It present a novel object-oriented architecture pattern for developing multi-tenant web application frameworks in which maximum reuse and modularity can be achieved and application concerns can be separated. It evaluates the modularity, the extensibility, the reusability, the

maintainability and the efficiency of our pattern by qualitative analysis based on well-known patterns used in our pattern. It also validates the applicability, the correctness, the security and the performance of our pattern by testing real world systems that were built using our pattern. This pattern would reduce time and cost when developing multi-tenancy systems as well as understanding, evaluating and modifying existing web application frameworks

As a new software service model, Software as a Service (SaaS) provider provides the entire network infrastructure and software updates in Cloud for users. Users need not buy software and hardware and hire IT professional workers. They can use the SaaS system by internet and pay for selected services according to their network flow, data store capacity and computing power. The growing number of users and elastic cloud infrastructure bring down the total costs of software provider which make it popular for medium and small enterprise to use SaaS system. So, the software providers who have a well development web application want to meet the market requirement to transforming his old application to a SaaS application. How to transform a web application to a SaaS quickly, efficiently and meet multi enterprises to use is a challenge problem. Now, many researches are focusing on SaaS for its creation, security, multi-tenant architecture, scalability and configurability, but few researches focus on how to convert a well-developed typical web application to a SaaS application

b. Explain in detail cloud security threats.

Answer:

Cloud computing is growing rapidly and transforming the way organizations use, store, and share (information, applications, and workloads). With this, it has also brought several security threats and challenges. It has now become a natural target of bad actors with data increasingly moving into the cloud.

The Cloud Security Alliance has released a report which identifies the latest threats in cloud computing and the growing need for cloud customers to understand and adopt security to manage threats and rely less on the vendors. It is necessary for the organizations to be aware of cyber threats. According to the Cloud Security Alliance report, here are the top threats to cloud computing:

1. Poor Access Management

Access management is one of the most common cloud computing security risks. The point of access is the key to everything. That's why hackers are targeting it so much.

In 2016 LinkedIn experienced a massive breach of user data, including account credentials (approximately 164 million). As a result, some of the accounts were hijacked, and this caused quite a hunt for their system admins in the coming months. "

"Here's another example of cloud security threats. A couple of months ago, the news broke that Facebook and Google stored user passwords in plaintext. While there were no leaks, this practice is almost begging to cause some

2. Data Breach and Data Leak - the main cloud security concerns

The cloud security risk of a data breach is a cause and effect thing. If the data breach happens - this means the company had neglected some of the cloud security flaws, and this caused a natural consequence.

The most prominent recent data breach is the one that happened in Equifax in 2017. It resulted in a leak of personal data of over 143 million consumers. Why? Equifax's developers hadn't updated their software to fix the reported vulnerability. Hackers took advantage of this and the breach happened

3. Data Loss

If a data breach wasn't bad enough, there is an even worse cloud security threat - it can get irreversibly lost like tears in the rain. Data loss is one of the cloud security risks that are hard to predict, and even harder to handle.

One of the most infamous examples of data loss is the recent MySpace debacle.

It resulted in 12 years of user activity and uploaded content getting lost. Here's what happened. During a cloud migration process in 2015, it turned out that a significant amount of user data, (including media uploads like images and music), got lost due to data corruption. Since MySpace wasn't doing backups - there was no way to restore it. When users started asking questions, customer support said that the company is working on the issue, and a couple of months later, the truth came out. This incident is considered to be another nail in the coffin of an already dying social network

4. Insecure API

Application User Interface (aka API) is the primary instrument used to operate the system within the cloud infrastructure. This process includes internal use by the company's employee and external use by consumers via products like mobile or web applications. The external side is critical due to all data transmission enabling the service and, in return, providing all sorts of analytics. The availability of API makes it a significant cloud security risk. In addition to that, API is involved in gathering data from edge computing devices. "

"The most prominent example of insecure API in action is the Cambridge Analytica scandal. Facebook API had deep access to user data and Cambridge Analytica used it for its own benefit.

5. Misconfigured Cloud Storage

Misconfigured Cloud Storage is a continuation of an insecure API cloud security threat. For the most part, security issues with cloud computing happen due to an oversight and subsequent superficial audits. Cloud misconfiguration is a setting for cloud servers (for storage or computing purposes) that make it vulnerable to breaches

A good example of cloud misconfiguration is the National Security Agency's recent mishap. A stash of secure documents was available to screen from an external browser.

6. DoS Attack - Denial-of-service attack

Scalability is one of the significant benefits of transitioning to the cloud. The system can carry a considerable workload. But that doesn't mean it can handle more unexpectedly. It can overload and stop working. That's a significant cloud security threat.

Sometimes, the goal is not to get into the system but to make it unusable for customers. That's called a denial-of-service attack. In essence, DoS is an old-fashioned

system overload with a rocket pack on the back. The purpose of the denial-of-service attack is to prevent users from accessing the applications or disrupting its workflow. DoS is a way of messing with the service-level agreement (SLA) between the company and the customer. This intervention results in damaging the credibility of the company. The thing is - one of the SLA requirements is the quality of the service and its availability. " Denial-of-Service puts an end to that.

2014 Sony PlayStation Network attack is one of the most prominent examples of denial-of-service attacks. It is aimed at frustrating consumers by crashing the system by both brute forces and being kept down for almost a day.

7. Malicious insider

A malicious insider can access sensitive data of the system administrator or may even get control over the cloud services at greater levels with little or no risk of detection. A malicious insider may affect an organization through brand damage, financial impact and productivity loss

8. Lack of due diligence

Most cloud providers develop a good strategy for due diligence when evaluating cloud technologies. Enterprises that choose providers without analysing the technologies and the due diligence expose of it, expose themselves to risks

9. Abuse and nefarious use of cloud services

This threat refers to attackers leveraging the resources of cloud computing to target users, enterprises, and other cloud providers. Examples include launching DDoS attacks, phishing, email spams, get access to credential databases, and more.

10. Shared technology vulnerabilities

Cloud providers deliver their services by sharing applications, or infrastructure. Sometimes, the components that make up the infrastructure for cloud technology as-a-service offering are not designed to offer strong isolation properties for a multi-tenant cloud service. This may lead to vulnerabilities in shared technology that can be attacked in almost all delivery models.

Question No. 3: (10)

Briefly describe following.

a) Advantages and disadvantages of cloud computing.

Answer:

Advantages of Cloud Computing

Here, are important benefits for using Cloud computing

Cost Savings

Cost saving is the biggest benefit of cloud computing. It helps you to save substantial capital cost as it does not need any physical hardware investments. Also, you do not need trained personnel to maintain the hardware. The buying and managing of equipment is done by the cloud service provider.

Strategic edge

Cloud computing offers a competitive edge over your competitors. It helps you to access the latest and applications any time without spending your time and money on installations.

High Speed

Cloud computing allows you to deploy your service quickly in fewer clicks. This faster deployment allows you to get the resources required for your system within fewer minutes

Back-up and restore data

Once the data is stored in a Cloud, it is easier to get the back-up and recovery of that, which is otherwise very time taking process on premise

Automatic Software Integration

In the cloud, software integration is something that occurs automatically. Therefore, you don't need to take additional efforts to customize and integrate your applications as per your preferences

Reliability

Reliability is one of the biggest pluses of cloud computing. You can always get instantly updated about the changes

Mobility

Employees who are working on the premises or at the remote locations can easily access all the cloud services. All they need is Internet connectivity.

Unlimited storage capacity

The cloud offers almost limitless storage capacity. At any time you can quickly expand your storage capacity with very nominal monthly fees

Collaboration

The cloud computing platform helps employees who are located in different geographies to collaborate in a highly convenient and secure manner.

Quick Deployment

Last but not least, cloud computing gives you the advantage of rapid deployment. So, when you decide to use the cloud, your entire system can be fully functional in very few minutes. Although, the amount of time taken depends on what kind of technologies are used in your business.

Disadvantages of Cloud Computing

Here, are significant challenges of using Cloud Computing:

Performance Can Vary

When you are working in a cloud environment, your application is running on the server which simultaneously provides resources to other businesses. Any greedy behavior or DDOS attack on your tenant could affect the performance of your shared resource.

Technical Issues

Cloud technology is always prone to an outage and other technical issues. Even, the best cloud service provider companies may face this type of trouble despite maintaining high standards of maintenance.

Security Threat in the Cloud

Another drawback while working with cloud computing services is security risk. Before adopting cloud technology, you should be well aware of the fact that you will be sharing all your company's sensitive information to a third-party cloud computing service provider. Hackers might access this information.

Downtime

Downtime should also be considered while working with cloud computing. That's because your cloud provider may face power loss, low internet connectivity, service maintenance, etc.

Internet Connectivity

Good Internet connectivity is a must in cloud computing. You can't access cloud without an internet connection. Moreover, you don't have any other way to gather data from the cloud.

Lower Bandwidth

Many cloud storage service providers limit bandwidth usage of their users. So, in case if your organization surpasses the given allowance, the additional charges could be significantly costly

Lacks of Support

Cloud Computing companies fail to provide proper support to the customers. Moreover, they want their user to depend on FAQs or online help, which can be a tedious job for non-technical persons.

b) Collaborative meeting in cloud.

Answer:

Cloud collaboration is a way of sharing and co-authoring computer files through the use of **cloud computing**, whereby documents are uploaded to a central "**cloud**" for storage, where they can then be accessed by others. Businesses in the last few years have increasingly been switching to use of **cloud collaboration**.

Strengthen business relationships with Cisco Collaboration Meeting Rooms (CMR). Enable everyone to meet using virtually any device, for a business-quality video collaboration experience that combines video, voice, and content sharing technologies. Cisco CMR brings together our industry-leading video conferencing infrastructure and proven, scalable, WebEx cloud conferencing services to deliver an exceptional meeting experience. With our technology you can host video-optimized meetings, which are available to anyone, anywhere, on any device

Cisco CMR helps enable people to meet with others in a way that suits their working day. You can Invite others to meet in your personalized, always-available virtual meeting place quickly and easily, anytime Create instant meetings whenever needed, add a third person to your conversation, or start new meetings Reserve the conference rooms and media resources required for scheduled meetings for defined audiences"

"This advancement in the way we store and share data has led to a number of benefits that allow us to connect and work collectively as a team – and in an efficient and productive manner. Here are five benefits of cloud collaboration.

1. IMPROVED ORGANIZATION

With documents kept in a central, cloud-accessible location, employees can work on a document without having to send an updated version (not to mention trying to keep track of the latest version) to all the necessary team members

2. HIGHER PARTICIPATION LEVELS

Allowing access to projects can lead to higher levels of employee participation. With cloud collaboration, all team members have an equal opportunity to provide input, and it can be done from wherever they are, at any time.

3. IMPROVED ACCESS TO LARGE FILES

Most email servers cannot handle documents larger than a few MB. When dealing with large audio or video files that email servers can't accommodate, cloud computing solutions have the answer. Because you can provide access to the cloud, where the large files are stored, there is no need to send files. Through the cloud, there is no delay in receipt or distribution dilemmas.

4. REAL-TIME UPDATES

Teams can work on projects without having to be in the same room, or even country. Edits and updates appear in real time and can be accessed by everyone. Any confusion over which version is the latest is eliminated with cloud collaboration

5. BETTER BRAINSTORMING

The cloud can become a brainstorming forum, allowing ideas to be shared and productive conversations to take place. The cloud is an ideal medium to facilitate better communication between staff and project managers, various team members and other collaborators.