BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 6

DCA3243

CLOUD COMPUTING

Unit 5

Cloud Computing Technology

Table of Contents

1. INTRODUCTION

To have the best outcome from cloud computing technology, following the critical factors involved, the proper hardware and the infrastructure in the right place. In this unit, we will discuss the equipment required from your end and how it should be configured to get a better and more efficient interaction with the cloud. The first section in this unit focuses on clients consisting of hardware or software that relies on cloud computing for its application process. The second section is a unit discussing the security issues associated with cloud computing technology and what are the different measures through which we can

Maintain our data safe since we will use the third-party service. The following section deals with different network types involved in the cloud computing technology. Finally, we are going to conclude this unit with a discussion of the different services that we have to run based on the cloud provider, and these services got disturbed based on the infrastructure that your company deployed.

1.1 Objectives

After studying this unit, you should be able to:

- *Explain the types of clients of cloud computing technology.*
- *Describe various security issues involved while utilising cloud service.*
- *Discuss the levels of network connectivity involved.*
- *List various connection methods with their description and use.*
- *Explain the different services involved in cloud providers.*

2. CLIENTS

A cloud ***client*** consists of computer hardware and/or computer software which relies on cloud computing for application delivery; it embraces the use of cloud computing architectures but adds a client technology that runs locally on a computer or device and can interact with local applications and resources.

It also acts as an interface between the cloud and the common computer user through web browsers and thin computing terminals. So, the term cloud client describes a piece of hardware, a piece of software, or both that is specifically designed for a cloud service.

2.1 Hardware clients

There are three types of hardware clients.

Thick Client

The thick clients consist of many interfaces, internal memory, I/O devices, etc.; they are also called **heavy clients**. Thick clients are functional whether they are connected to a network or not. Even though the system is fully functional, it will be considered a 'client' when it is connected to a server. The server may provide the thick client with programs and files that are not stored on the local machine's hard drive. It is not uncommon for workplaces to provide thick clients to their employees. This enables them to access files on a local server or use the computers offline. When a thick client is disconnected from the network, it is often referred to as a workstation. It is possible to use the thick client for many different tasks; a good example is the well-known standard desktop PC.

Thin Client

The thin client, on the other hand, has only the necessary components for one specific task, in the most extreme form, only input and output interfaces. Since they do not have hard drives, thin clients do not have any software installed on them. Instead, they run programs and access data from a server. For this reason, thin clients must have a network connection and are sometimes referred to as "network computers". An example is the OnLive hardware.

Smartphones

Now, we are going to discuss the third type of hardware client, which is smartphones. They let you access cloud services from everywhere; examples are the iPhone, Android-based phones, and phones with the Windows mobile operating system. Most of the cloud services available can be used with a thick client, for example, the Amazon Simple Storage Service (S3). The Amazon Simple Storage Service is “storage for the Internet”; it provides a web-service interface to store and retrieve data in and from the cloud. The Amazon Machine Image (AMI) is a virtual machine that runs on EC2; it can be created by the user and uploaded to S3.

Some cloud services can be used on smartphones; an example is Salesforce.com Mobile Lite Client. Salesforce.com is a purely cloud-based CRM system for companies.

2.2 Software clients

Now, we move on to the software side; we find that software clients, in general, can be put into one of three groups. These different types include (in order from more desktop-related to more web-related):

Rich or Fat Client

Desktop applications connected to the Internet or Fat Clients are applications that make use of network support but also run offline, sometimes with limited functionality. Examples are the e-mail client Microsoft Outlook or the media player iTunes. These applications need to be installed on the user's machine.

Smart Clients

A Smart Client application environment offers:

- delivers applications over a web HTTP connection.
- does not require installation (or provide automated installation and updates)
- automatically updates without user action.
- has the look and feel of desktop applications.

Web-applications/Thin Clients

Web applications/Thin Clients rarely have to be installed by the user. An example is the online agenda application Google Calendar. Applications of this kind often run in a web browser.

2.3 Cloud clients

In software clients for the cloud, very often, users expect a browser-based interface. If it is required, only lightweight client software will be installed. Often, there are different ways to access the cloud. Live Mesh, for example, offers a Web-based solution and a client tool. This can be different for different user groups. For example, the end-user uses a web-based frontend to work with the cloud application, but for administration and deployment, a command line tool has to be used. Sometimes, it is even possible to switch to offline mode. Google Calendar and Gmail applications are examples of the above situation. After the installation of the browser plug-in Gears, they are working without an Internet connection in read-only mode. New emails are sent after a new connection has been set up.

Web-based clients

The Web-based clients are used, for example, in the Salesforce.com Customer Relationship Management (CRM) system, Google Apps or Google Docs. Google Docs is an office suite that runs in the cloud. It provides a text writer and tools to create presentations and charts.

Client applications

Other systems use client applications, but not always exclusively. The Microsoft Live Mesh service, for example, offers a client application in addition to the web-based solution. The command-line tool available for Amazon Elastic Compute Cloud (EC2) is a set of tools written in Java that you can run from the Linux/UNIX or Windows command line that closely mimics the Amazon EC2 API functions.

Applications with cloud-extensions

Some desktop applications, such as Mathematica and MatLab, have optional extensions to the cloud. The latest versions of the mathematics software package MatLab and Mathematica provide an extension for compute-intensive tasks. They are capable of using Cloud Computing to perform expensive evaluations. To use this, one or more Amazon EC2 images have to be configured. Matlab offers two different work modes: batch and interactive. In batch workflow, a MatLab user can submit a job to the cluster scheduler, possibly shut down MatLab, and retrieve results later once the job has been executed. In an interactive workflow, a Matlab user is connected directly with the MatLab workers running in the cluster. The user sends commands that are executed immediately, and the results are available as soon as the command execution is complete. Response times may be slow depending on traffic and the amount of data exchanged.

SELF-ASSESSMENT QUESTIONS – 1

1. ____________________ clients are functional whether they are connected to a network or not.
2. Expand CRM
   a) Customer Relationship Management
   b) Customer Relation Management
   c) Customer Relationship Maintenance
   d) Customer Relation Maintenance
3. Salesforce.com is purely cloud-based ____________________ for companies.

3. SECURITY

There are a number of security issues/concerns associated with cloud computing since a third party stores your data. But these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected, whereas the customer must ensure that the provider has taken the proper security measures to protect their information.

Data Leakage

Protection involves the maintenance of data segregation between the users. Proper care is required while storing data and also during transportation. The biggest benefit is the centralisation of data. Centralisation also provides the opportunity for better monitoring. Thick clients are apt to download files and maintain them on the hard drive; using thin clients creates a better chance for centralised data storage. As such, there's less chance of data leakage.

Cloud providers should have proper systems:

- to prevent data leaks or access by third parties.
- should ensure that auditing and/or monitoring cannot be defeated.
- surety protection even from privileged users at the cloud provider.

Offloading Work

It's up to the cloud provider to provide adequate security. After all, can your organisation afford 24-hour IT security staffing? The fact of the matter is that your cloud provider might offer more security features than you had before.

The fact that there are many clients paying allows cloud providers to have beefier security simply because of the economy of scale involved. This means there are many paying clients, so the provider is able to do more because there is more money in the pot. Plus, it's to the provider's benefit to offer more because they want to get a good reputation.

Logging

Logging is something that, in-built, usually gets the short end of the stick. But in the virtualised world of cloud computing, in order to extend logging, providers can add as much memory as they need. Here is the ability to do a deeper level of logging in the cloud environment via a large database, otherwise called a “big table”, where the company is working in a computing commodity environment. Logging everything and then building logic around those logs is one of the many benefits of cloud computing that might make network forensics investigators' lives easier.

Forensics

If there is a gap, the cloud provider can respond to the incident with less downtime than if you had to investigate the breach locally. After using the server, the cost will be estimated. Construction of an online forensic server is one of the easiest jobs. The virtual machine can be cloned for easy offline analysis. Further, many companies don’t have a dedicated in-house incident response team. If there is a problem, IT staff has to quickly figure out their new job of taking the server down, quickly investigating, and getting it back online for minimal production downtime.

Development

Vendors are actively developing products that can apply to virtual machines and the cloud. They also have an exclusive opportunity in the cloud. Since it’s new ground, there are new opportunities for the vendors who are open-minded enough to imagine them. Enterprises, those who want to extend control to data in the cloud, propose a shift from protecting data from the outside to protecting data from within. We call this approach of data and information protection itself information-centric. This self-protection requires intelligence to be put into the data itself.

Auditing

Securing data in your own local network is the toughest job. But we have to face new issues when you send your data to the cloud since your data is being stored on someone else’s equipment.

IT audits in practice

- Use of partly irrelevant and insufficient controls for cloud computing
- Approach tailored for client-server/ on-premises IT.
- Emphasis on (service management) processes with paper evidence
- Recommendations are only partly aimed at mitigating cloud-specific risks.

Compliance

The same security issues that your organisation deals with are the sorts of issues that SaaS providers face—securing the network, hardware issues, applications, and data. But compliance adds another level of headache. Regulations like Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), and HIPAA, and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) make things particularly challenging.

Prior to SaaS, compliance could be managed by a few tasks:

- Identify users and access privileges.
- Identify sensitive data.
- Identify where it's located.
- Identify how it is encrypted.
- Document this for auditors and regulators

SaaS makes these steps even more complicated. If you store compliance-sensitive data with a SaaS provider, it is difficult to know where the data is being stored. It could be on the provider's equipment, or it could even be on the equipment of one of the provider's partners.

SELF-ASSESSMENT QUESTIONS – 2

4. Ability to do a deeper level of logging in the cloud environment via a large database, otherwise called as.
5. The virtual machine can be cloned for easy ________________ analysis.

4. NETWORK

There are different levels of connectivity needed in order to deliver its best resources through the cloud. The research firm Gartner identified four different levels in a June 2008 study. Gartner also notes that different organisations require different things from the cloud, and as such, they will have to connect in different ways. What works for one organisation might not necessarily be the best means of connectivity for another.

4.1 Basic Public Internet

The public Internet is the most basic choice for cloud connectivity. The first option is the pipe most of us have come into our offices or homes. It is one of the types of access that you buy from an Internet service provider (ISP) and connect via broadband or dial-up, based on your location. There are no extras like Transmission Control Protocol (TCP) acceleration, advanced compression, or application-specific optimisation.

This model has the following advantages:

- Anyone with Internet access can use this solution.
- It's highly fault tolerant.
- Many provider options are available.
- Secure Sockets Layer (SSL)–based on Hypertext Transport Protocol Over Secure Sockets Layer (HTTPS), encrypted access provides confidentiality.
- It's cost-effective.

It also has the following disadvantages:

- Lack of end-to-end quality of service (QoS), thus making end-to-end service-level agreements (SLAs) difficult to reach.
- Probability of poor response over high-latency connections. This is worsened by protocol inefficiencies in TCP, HTTP, and web services.
- Downtime that might be out of your control (cable cuts, problems at the ISP, and so forth).

Consuming this method, organisations should think through subscribing to multiple ISPs, and cloud providers should also get bandwidth from multiple sources. Ideally, the client would get bandwidth from one of the same ISPs as the vendor. This aids in speed, reliability, and a better chance of success with an SLA.

4.2 The Accelerated Internet

Like almost every other area of enterprise IT, cloud computing is far from a 'one-size-fits-all' solution. There are at least five types of cloud architecture, from the basic public Internet to an 'accelerated Internet' (where ADCs can significantly speed performance), an 'optimised Internet,' a 'private cloud' utilising VPN (virtual private network) and an 'internal cloud' based solely on an enterprise's own equipment. The accelerated Internet model is emerging as the most common model, and, as a result, both cloud providers and enterprises are embracing ADCs (Application Delivery Controllers) to speed performance and manage traffic. Even away from cloud computing, accelerated performance is a burning issue for most enterprises.

The past decade has seen a huge growth in browser-based enterprise applications, from enabling online support and booking and sales systems to delivering a back-office application to a remote site. These services create new demands on IT infrastructure because of "chatty" and complex protocols. As a result, end-user performance can be very disappointing unless issues such as bandwidth, latency, and, of course, security are suitably addressed.

4.3 Optimised Internet Overlay

An optimised Internet overlay approach allows customers to access the cloud via the public Internet, but enhancement occurs on the provider’s cloud. Enhancements at these points of presence (POP) include.

- Optimized real-time routing. This helps avoid slowdowns, helping to make SLAs easier to attain.
- An SSL session can be stopped so that protocols and payload can be optimised and re-encrypted.
- Some of the application logic can reside on the POP. This allows for better scalability, fault tolerance, and response time, usually in excess of 80 per cent.
- Content that is frequently accessed can be delivered from local caches.
- Disadvantages of this method include.

- It is costlier than public Internet connectivity, sometimes as much as four times as much.
- There is a strong vendor lock-in if the application is distributed into the carrier's network.

4.4 Site-to-site VPN

The fourth option is to connect to the service provider directly using a private wide area network (WAN) (normally an MPLS/VPN connection). This setup allows confidentiality, guaranteed bandwidth, and SLAs for availability, latency, and packet loss. MPLS can also scale to meet changing bandwidth needs, and Quality of service can also be written into the SLAs. On the downside, private WANs are not normally more reliable than Internet connections, especially redundant connections to multiple ISPs. Table 5.1 compares all four connections.

4.5 Cloud Providers

A robust connection method is necessary for the cloud providers for their service to disperse across. Private tunnels make sure that loss, bandwidth and latency are not likely to affect performance and encryption and strong authentication are the additional benefits. Since the network bandwidth charges increase, growing cloud providers might incur high costs.

This traffic is from traffic among provider sites as well as traffic both to and from clients. Big providers like Google construct their own WANs with multiple peering points, and major ISPs are able to sidestep these charges. To reduce bandwidth requirements by up to 80 per cent, smaller providers can use WAN optimisation controllers (WOCs). If providers use asymmetrical optimisation, performance can be improved, and bandwidth charges can be reduced. This requires an appliance at the provider and a client applet. This can reduce response time by up to 70 per cent and bandwidth requirements by up to 80 per cent. The benefit is that additional equipment is not needed at client sites.

Table 5.1: Features of connectivity option

Connection Method	Description	Examples of use
Basic public internet	Anyone can use it.Fault-tolerant Multiple providers Cost-effective Performance issues globally delivered applications	Consumer applications Advertising-supported services Applications where “best effort” service is sufficient
Accelerated internet	Improved end-user performanceInconsistent performance, basedon provider and ISP configuration Low cost	Best for cost-sensitive service where improved response times and bandwidth are necessary
Optimised overlay	Consistent performance Ability to have strong SLAs Expensive Limited provider options Provider risk	Business-critical applications that require SLAs to deliver promised response times and bandwidth
Site-to-site VPN	Ability to have strong SLAs Site-specific delivery Consistent performance Lowest latency Limited reach	Business-critical applications, including server-to-server traffic

4.6 Cloud consumers

Cloud computing has become a big buzzword in the IT industry, with infrastructure providers jumping over one another to provide cloud services. Large companies can build their own scalable distributed IT infrastructure in which data centres are connected with their own private fibre optic connections. This depends on distance, bandwidth requirements, and—of course – their budgets. This infrastructure starts to look like a cloud computing service.

Clients located at major sites normally access applications over the corporate WAN. For smaller offices or mobile workers, VPN connections across optimised and accelerated Internet services provide a more robust solution. VPN tunnels across the Internet are best as a primary link only when high performance is not crucial.

4.7 Pipe size

Bandwidth is, simply put, the transmission speed or throughput of your connection to the Internet. However, measuring bandwidth can be difficult since the lowest point of bandwidth between your computer and the site you're looking at is what your speed is at that moment.

There are three factors that are simply out of your control when it comes to how much bandwidth you need:

- The Internet bandwidth between your organisation and the cloud
- The round-trip time between your organisation and the cloud
- The response time of the cloud

Upstream/Downstream

Another factor to consider is whether it is okay for the transfers to be symmetric or asymmetric. If your connection with the cloud is symmetric, then that means you are sending and receiving data at the same rate. If your connection is asymmetric, and data is sent from your organisation at a slower rate than when you're receiving it.

How much do we need?

This can be a complex question based on what you'll be doing on the cloud. What you have to do is figure out how much data will be moving in and out of the cloud at any given time and then decide how big of a pipe you need to move that data. Chances are good that you have a beefy enough Internet connection to make cloud computing viable. However, realise that the more you do on the cloud, the more demand will be placed on your Internet connection. If you do not have enough capacity, then everyone will experience a slowdown.

Take the time to figure out how much capacity you'll use, and make sure you have enough resources to accommodate that need. If not, you are likely to have another expense that you hadn't planned on in the guise of a faster Internet connection. It's important to secure an SLA that meets your bandwidth requirements. This not only ensures that you are getting the speed that you need but also that if the ISP fails to meet those levels, there can be some sort of remediation for you.

4.8 Redundancy

When formulating your cloud infrastructure, be sure to consider the issue of reliability and uptime and ask your service provider to configure your computing infrastructure for redundancy and failover. In your LAN, redundancy used to mean that another server or two were added to the data centre in case there was a problem. These days, with virtualisation, redundancy might mean a virtual server being cloned onto the same device or all the virtual servers of one machine being cloned onto a second physical server.

It becomes more complex in the cloud. While you may think of your server being hosted at the data centre of your cloud provider, it's not as easy to nail down. Parts of your data may be housed in one location, and other parts scattered throughout the country (possibly even the world). And when the provider adds a redundant system, the data is again scattered throughout their cloud. So, it's not an issue of the service provider wheeling in a new server to provide redundant services. Rather, they simply reallocate resources to give you a redundant system.

SELF-ASSESSMENT QUESTIONS – 3

6. _____________________ The approach allows customers to access the cloud via the public Internet, but enhancement occurs on the provider's cloud.
7. Clients located at major sites normally access applications over the corporate WAN. (True/False).
8. To reduce bandwidth requirements by up to 80 per cent, smaller providers can use them.

5. SERVICES

There are different services you will need to run, depending on your cloud provider and what your organisation does. Also, these services will likely affect how your cloud infrastructure is deployed.

5.1 Identity

No matter where an application runs – in-house or on the cloud – it needs to know about its users. To accomplish this, the application asks for a digital identity – a set of bytes – to describe the user. Based on this information, the application can determine who the user is and what he or she is allowed to do.

In-house applications rely on services like Active Directory to provide this information. Clouds, however, have to use their own identity services. For instance, if you sign on to Amazon cloud services, you have to sign on using an Amazon-defined identity. Google's App Engine requires a Google account, and Windows uses Windows Live ID for use with Microsoft's cloud applications. Identity services need not be proprietary. OpenID is an open, decentralised, single sign-on standard that allows users to log in to many services using the same digital identity. An OpenID is in the form of a uniform resource locator (URL) and does not rely on a central authority to authenticate a user's identity. Since a specific type of authentication is not required, nonstandard forms of authentication may be used, including smart cards, biometrics, or passwords. An OpenID authentication is used by many organisations, including:

- Google
- IBM
- Microsoft
- Yahoo!

5.2 Integration

Applications talking among themselves have become highly common. Vendors come up with all sorts of on-premises infrastructure services to accomplish it. These range from technologies like message queues to complex integration servers. Integration is also on the cloud, and technologies are being developed for that use. For example, Amazon's Simple

Queue Service (SQS) provides a way for applications to exchange messages via queues in the cloud. SQS replicates messages across several queues, so an application reading from a queue may not see all messages from all queues on a given request. SQS also doesn't guarantee in-order delivery. These sound like shortcomings, but in fact, it's these simplifications that make SQS more scalable. However, it also means that developers must use SQS differently from on-premises messaging.

Another example of cloud-based integration is BizTalk Services. Instead of queuing, BizTalk Services utilises a relay service in the cloud, allowing applications to communicate through firewalls. Since cloud-based integration requires communicating through different organisations, the ability to tunnel through firewalls is an important problem to solve. BizTalk Services also utilises simplified workflow support with a way for applications to register the services they expose and then let those services be invoked by other applications. Integration services in the cloud are going to gain prominence as they become more and more important, especially given how important they are in-house.

5.3 Mapping

Maps are becoming more and more popular in web applications. For instance, hotel and restaurant websites show their locations on their websites and allow visitors to enter their addresses to get customised directions. But the guy who developed the website likely didn't have the time or money (not to mention the interest) to make his own mapping database. Enough organisations want this functionality, however, so it is offered as a cloud application. Such services as Google Maps and Microsoft's Virtual Earth provide this cloud-based function, allowing developers to embed maps in web pages. These services are really just additions to existing websites.

5.4 Payments

Another cloud service that you might want to plan for and configure your hardware appropriately for is payments. Depending on your organisation, you may or may not want to accept online payments from customers.

Luckily, there is no lack of ways to get paid online. You can simply sign up with a service to accept credit cards, or you can go the route of PayPal. With an online payment service, customers can send money directly to your organisation.

5.5 Search

The ability to embed search options in a website is certainly nothing new, but it is a rich feature that you might want to employ in your own web or application development.

Microsoft's Live Search allows on-site and cloud applications to submit searches and then get the results back. Searchability is limited only to the organisation and what it does. For instance, a company might develop an application that does both. For instance, let's say a company has a database of movie information. By typing in the name of the movie, you can search its own database as well as a search of the Internet to give you two types of results – what's stored in the company database as well as what's on the entire Web. If you were to use a single computer to access the cloud, the requirements are pretty minimal – all you need is a computer and an Internet connection. However, when you start planning cloud solutions for your organisation, you need to spend more time figuring out which hardware and infrastructure is best for you. In the next chapter, we'll talk about how you can use your newly configured network to access the cloud and how your clients are set up.

SELF-ASSESSMENT QUESTIONS – 4

9. In-house applications rely on services ____________________ to provide information.
10. Amazon's Simple Queue Service (SQS) provides a way for applications to exchange messages via queues in the cloud. (True/False)
11. ______________________ allows on-site and cloud applications to submit searches and then get the results back.

6. SUMMARY

- Cloud computing technology is one of the important factors in making the best services available through the cloud. If only one computer is involved to access the cloud, the requirements are also very minimal.
- Your requirement in this scene will be a computer and an internet connection. But when you plan cloud computing for your company, you need to get more and spend time studying and figuring out which hardware and infrastructure are best for you.
- A pilot study to launch cloud solutions for your company involves all the clients of cloud technology, the various services involved, and the levels and layers of work involved in the network to make cloud computing services available. S
- Security concerns and issues involved in the cloud service and how to protect your data from unauthorised and unauthenticated hands.

7. TERMINAL QUESTIONS

1. Discuss the different types of clients for cloud computing.
2. Explain the security issues and concerns associated with cloud computing.
   - Discuss the following.
   - Basic Public Internet
3. The accelerated Internet
4. Brief about cloud consumers and providers.
5. Discuss the different services under cloud computing technology.

8. ANSWERS

Self-Assessment Questions

1. Thick
2. a) Customer Relationship Management
3. CRM System
4. big table.
5. offline
6. Optimized Internet overlay
7. True
8. WOC
9. Active Directory
10. True
11. Microsoft’s Live Search

Terminal Questions

1. It also acts as an interface between the cloud and the common computer user through web browsers and thin computing terminals. (Refer to section 2)
2. Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client’s data and applications are protected, whereas the customer must ensure that the provider has taken the proper security measures to protect their information. (Refer Subsection 3)
3. The public Internet is the most basic choice for cloud connectivity. The first option is the pipe most of us have come into our office or homes. (Refer Subsection 4.1)

   Like almost every other area of enterprise IT, cloud computing is far from a 'one-size-fits-all' solution. (4.2)
4. Cloud computing has become a big buzzword in the IT industry, with infrastructure providers jumping over one another to provide cloud services (Refer to Subsection 4.5 and 4.6)
5. There are different services you will need to run, depending on your cloud provider and what your organisation does. Also, these services will likely affect how your cloud infrastructure is deployed. (Refer Section 5)

9. REFERENCES

- http://www.softwareresearch.net/fileadmin/src/docs/teaching/SS09/SaI/Hoefer_Howanitz_Paper.pdf
- http://www.wyse.com/cloud-client-computing