

The Internet

Learning Outcomes:

- Recount the history of the internet.
- Explain cloud computing

HISTORY OF THE INTERNET

Many stories and origins will be read about the history of the internet. In some written document it started with a series of memos in MIT in August 1962 which discusses a certain concept about networking. This concept was entitled “Galactic Network”. If we do try to search more information about the internet, we could be able to arrive on when it started. Most of the stories goes to the event of the launch of the first space satellite Sputnik 1. Sputnik 1 was a Russian made space satellite launched in October 4, 1957. The talks about the capability of the satellite was mysterious for United States since there was seemed to have a race with technology at that time. During this era of flight to outer space as we all know, the United States of America and NASA was able to create a way to land on the moon. As early as 1960's theories of packet switching emerged and both USA and some European countries involving some companies has already been studying of the possibility of a huge network connected together.

In 1962 an organization named as Defense Advanced Research Projects Agency was created to study the theory of a huge network being connected. Along with this are the European organization such as the NPL or National Physics Laboratory and RAND Corporation who has also been studying the possibility of such a network and the study for this network was called as ARPANET or Advanced Research Projects Agency Network. With this study packet switching was created. Packet switching is a protocol for computers to communicate with each other. As early as 1969 there were Universities connected to each other. The first four was Stanford University, University of Utah, University of California in Sta. Barbara and University of California in Los Angeles. This was the beginning of the Internet.

Uses of the Internet

The internet is a network infrastructure that is used globally. The internet has standard rules on how computers should be communicating with each other. We can actually connect to this network with the help of Internet Service Providers that helps maintain the networks.

There are a lot of ways we use the internet these days. Here are the top 5 uses of the internet according to thedigitalchain.com:

1. Search information

Using the Internet, everything that we want to know is almost searchable using a computer connected to the internet. It could be just a simple word, a certain document, article, or book that we are searching, it can still be found on the internet.

COMP 001 – INTRODUCTION TO COMPUTING

2. News

Digital News is what is new. It is paperless, it cannot be limited in terms of how much you can read and it is easier to access rather than doing it before where you wait on a television to deliver news to you or by receiving a daily newspaper.

3. Communication

Communication is one of the best things that made the internet famous. We can now send and receive messages to anyone in the world real time may it be through messaging or video calls.

4. Data Transfer

Sending data over the internet has been very useful to us. It provides us with an easier way of providing information when we need it. This has revolutionized the way we do business today. It has speed up some processes that would usually take days to be done.

5. Social Networking

Right now during the pandemic, the use of the Internet has never been more important. When most countries have been locked down due to the pandemic, we were able to utilize the use of internet for communication. We can socialize with other people through different portals using the internet. Making the quarantine life more bearable.

Internet of things

Internet of things or IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without the need of human-to-human interaction. Some would say that is like an automation involving different appliances. For example, you own a smart appliance such as an air-conditioner. This appliance has information on your daily schedule. It may also have a record on your schedule to work or even has an access on your calendar. The air-conditioner since having this information may function automatically for you. It can turn on and turn off itself which may rely on your schedule. The data gathered and the ability of the air-conditioner to automate its function is an example of IoT.

IoT works by collecting data. This data is transferred using the internet. IoT's goal is to make the life of humans much easier for us.

On our given example earlier, which is the air-conditioner, let's say you were going to work and forgot to turn off the air-conditioner. Most likely if this happens your bill will go up and it could be a problem if this happens a lot. Having it automated in an IoT network makes it easier for you since if this happens and the air-conditioner determines that you are not home then it would turn it off automatically.

Pros and cons of IoT

Some of the advantages of IoT include the following:

- ability to access information from anywhere at any time on any device;
- improved communication between connected electronic devices;
- transferring data packets over a connected network saving time and money; and

COMP 001 – INTRODUCTION TO COMPUTING

- automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

Some disadvantages of IoT include the following:

- As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.
- Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices, and collecting and managing the data from all those devices will be challenging.
- If there's a bug in the system, it's likely that every connected device will become corrupted.
- Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

Cloud Computing Overview

INTRODUCTION

Cloud computing is the on demand delivery of computer system resources especially servers, storage, networking, and analytics, that are managed by third party and used by others. In today's world, large cloud systems are decentralized and available at multiple regions to reduce latency and reducing overhead on a single server. You can subscribe to cloud services and you need to pay only the amount you use and you can focus on the business problem, not infrastructure.

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure and customize applications online. With Cloud Computing users can access database resources via the internet from anywhere for as long as they need without worrying about any maintenance or management of actual resources.

What is Cloud?



Figure 01. Internet cloud computing media

The term **Cloud** refers to a Network or Internet in other words, we can say that Cloud is something which is present at remote location. Cloud can provide services over network, i.e, on public networks or on private networks, i.e WAN, LAN or VPN.

Applications such as e-mail, web conferencing, customer relationship management (CRM) all run in cloud.

COMP 001 – INTRODUCTION TO COMPUTING

What is Cloud Computing?

It refers to manipulating, configuring, and accessing the application online. It offers online data storage, infrastructure and application. Cloud computing is both a combination of software and hardware based computing resources delivered as a network service.

Cloud computing allows companies to avoid or minimize infrastructure cost for IT solutions. It also provides improved management, security, economic, scalability and manageability.

Why do we need to learn Cloud Computing?



Figure 02. Cloud Computing at work

In today's world every company wants to grow faster and also reduce costs. Every company wants to have scalable, manageable and economical infrastructure. But infrastructure comes with a cost and in a fast-growing startup fund is a major issue, cloud computing can be very handy in this situation where you just need to pay for the service you use and no need to buy new infrastructure you can just pay and use for the time you want.

Even enterprise companies also use cloud services for their products and different services.



Figure 03. Cloud Computing Architecture includes its application, platform and infrastructure

COMP 001 – INTRODUCTION TO COMPUTING

Basic Concept

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

1. Deployment Models
2. Service Models

1. Deployment Model

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

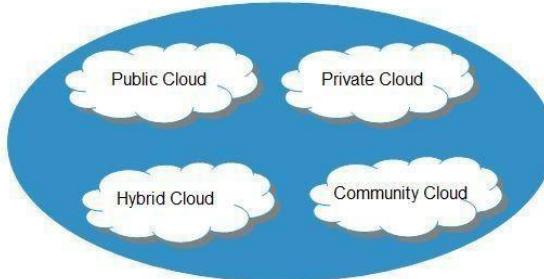


Figure 04. Deployment Model

- a. *Public Cloud* The public cloud is described as computing services provided through the public internet by third-party suppliers, making them accessible to those who want to use them or buy them. It can be free or on-demand for customers to pay for the cycles, storage or bandwidth they consume per usage. bandwidth they consume per usage.
Example: Sun Cloud, AWS, Microsoft Azure
- b. *Private Cloud* A private cloud is a cloud computing system in which IT services are supplied for the specialized use of one organization over private IT facilities. A single organization operates the cloud infrastructure only. It can be run on-site or off-site by the organization or a third party. Private cloud terms are often employed interchangeably with the virtual private cloud (VPC). Technically speaking, a VPC is a private cloud that uses the infrastructure of a third-party cloud provider, while an inner cloud is enforced.
Example: AWS, VMware
- c. *Community Cloud* A particular group of customers from organizations with shared issues can only use cloud infrastructure. It may be owned, operated, managed and run by one or more of the communal organizations, a third party or a mixture of them.
- d. *Hybrid Cloud* is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

2. Service Models

This are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

- a. Infrastructure as a Service (IaaS)
- b. Platform as a Service (PaaS)
- c. Software as a Service (SaaS)

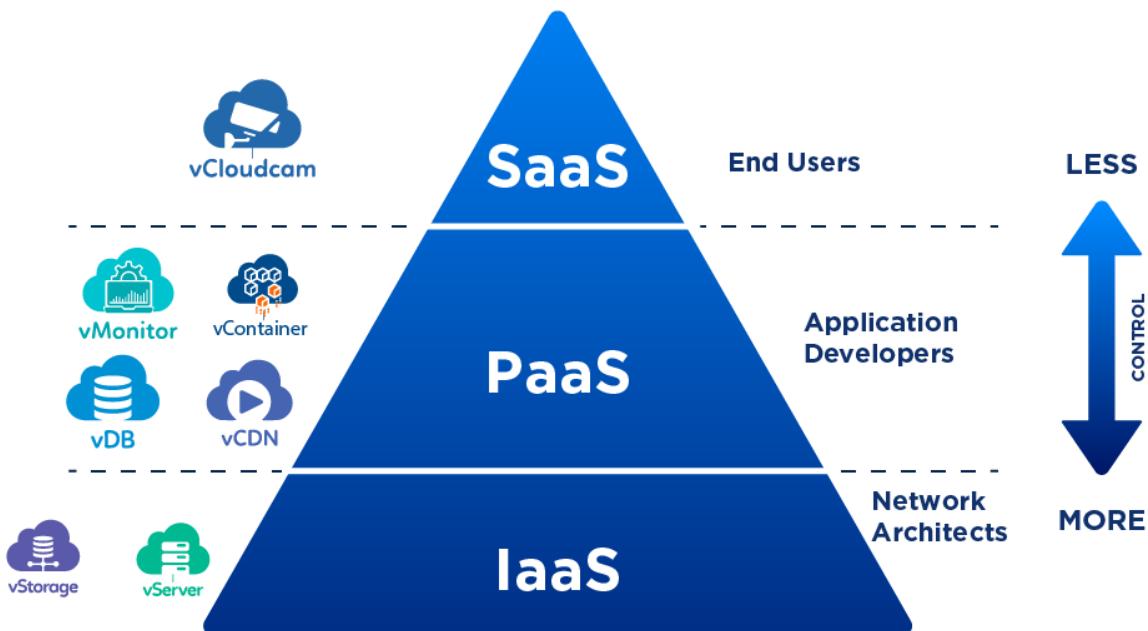


Figure 05. IaaS vs PaaS vs SaaS

Infrastructure as a Service (IaaS)

IaaS is the delivery of technology infrastructure as an on demand scalable service. It provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

- Usually billed based on usage
 - Usually multi tenant virtualized environment
 - Can be coupled with Managed Services for OS and application support
- Examples: AWS, Microsoft Azure, Google Cloud Platform (GCP)

Platform as a Service (PaaS)

PaaS provides the runtime environment for applications, development & deployment tools, etc. It provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely from the Internet.

Typically applications must be developed with a particular platform in mind

- Multi tenant environments
- Highly scalable multi tier architecture

Example: Google App Engine, AWS Elastic Beanstalk, Microsoft Azure App Service, Joyent, Salesforce.com

Software as a Service (SaaS)

SaaS model allows to use software applications as a service to end users. It is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service.

- Usually billed based on usage
- Usually multi-tenant environment
- Highly scalable architecture

Example: Google Workspace, Microsoft 365, Hubspot, Zoom, DropBox

COMP 001 – INTRODUCTION TO COMPUTING

ADVANTAGE OF CLOUD COMPUTING

1. Saves Money

You do not have to buy software and hardware. They are provided by the cloud. Hence you save costs such as office space rent, electricity, air conditioning, maintenance as well as operational expenses. Also, you pay only for the services that you use. Earlier there used to be unused hardware and software for organizations using on-premises hardware and software. Cloud eliminates that aspect of the business.

2. Scalable

You can change the resources you need from the cloud up or down. This was not possible earlier. Companies had to buy additional resources when requirements increased. When requirements reduced, they were left with unwanted resources.

3. Allows companies to focus on their core areas of business

Earlier, businesses had to allocate human resources, time, money, and effort to manage in-premises hardware. Cloud takes care of all the hardware and software aspects of businesses. This allows the business to concentrate on taking care of their domain areas.

4. Swift Deployment

Thanks to the cloud your business system can be up and running in just a few minutes. This gives an early lead over companies using the traditional or conventional approach.

5. Competitive Advantage

Businesses leveraging the cloud has a strategic edge over those that don't. This is because they can start off quickly and have the latest hardware as well as software services.

6. Compete with bigger players

Cloud creates a level playing field. Even small companies can afford it. They don't have to spend a huge amount initially to start operating. The cloud subscription cost is much less than outright purchasing the new and latest hardware as well as software.

7. Employees can work from any place at any time

Cloud services are available round the clock. Even if the office is closed work can go on. You can work at any time and from any geographical location as long as you have an Internet-enabled device.

8. Superior collaboration

Thanks to the cloud technology company staff stationed in different places can collaborate conveniently while maintaining high levels of security.

9. Superior backup

Compared to on-premise technology where backup, as well as recovery, takes a lot of time you can easily and conveniently do backup and recovery on the cloud platform. There is less downtime involving cloud-based platforms. The latter provides quicker as well as relatively more accurate retrievals of information as well as applications.

10. Convenient as well as easy implementation

Cloud technology lets companies retain the same business processes while not having to handle the backend technicalities.

COMP 001 – INTRODUCTION TO COMPUTING

11. Saves office space

Since there is minimum hardware installed at the company premises and fewer people required to manage and administer the hardware and software considerable office space is saved. This is an important benefit given the current trend of costly commercial real estate rates.

12. Superior Security

The cloud host completely handles the important responsibility of security. You don't have to worry about or handle security. The cloud host installs the latest security hardware and software. He/she also regularly update the security services, applies security patches and reviews the security level.

Although cloud is the latest technology and has many benefits, it's important not to overlook its flaws. We ought to be aware of its drawbacks.

DISADVANTAGES OF CLOUD COMPUTING

1. Loss of control

By opting for cloud services you are handing over your data as well as applications. You are dependent on the cloud provider in case any hardware or software issues manifest themselves. The speed and quality of service in such situations may not match your expectations.

2. Disruption of Cloud Services

In case of a cyber-attack, power outage or loss of Internet connectivity at the Cloud provider's end your business can suffer from unwanted downtime.

3. Cloud Vendor Shutting Shop

There is the possibility of your cloud service provider going out of business or changing its business domain. Your business will stop operating in this eventuality. You will have to quickly find another cloud service provider who is competent as well as reliable.

4. Potential Security Threat

Hackers are currently targeting high profile websites such as that of prominent cloud service providers. You have no control over the security of your data, applications, and software. Also, you can suffer losses and downtime if your cloud service provider's security is breached.

5. Vendor lock-in

In the event of migration to another cloud platform from the current platform, you may encounter major issues as the two platforms may be quite different. The challenges may include lack of support, configuration issues as well as an extra cost.

6. Wrong choice of provider

If you have not done your homework well or asked for reliable references while selecting a suitable cloud services provider then you may be in trouble. The quality of service may not be as desirable or certain features of cloud services may not be offered. This can affect the whole or part functioning of your business or operations.

COMP 001 – INTRODUCTION TO COMPUTING

7. Inadequate support

Some cloud computing providers fail to provide adequate support to their clients. Also, they ask you to refer FAQs for technical problems which are a difficult task for non-technical persons.

DIFFERENT CLOUD COMPUTING SERVICE PROVIDER

Now let us look at the Top Cloud computing Service Providers.

1. AWS

AWS is a secure cloud platform that provides a broad range of infrastructure services such as database storage, computer energy, and networking. From using AWS, we can host static websites. It is the most popular since it was the first one to enter the cloud services. AWS has an easy Sign-up Process. It provides hybrid capacity and billing per hour.

2. Kamatera

Kamatera's cloud server tool is comparable to a physical server. Kamatera offers high-performance cloud infrastructure services with very low maintenance. The cost of its cloud services is also very low as the search says that you can buy the cloud servers at 5 dollars. Try 100% for 30 days free. No covered charges or engagement Access all the features of the cloud management platform in the trial period. Across around four continents with they have 14 global data centers. They have human tech support around 24/7 and 365 days.

3. Microsoft Azure

Azure is a computer cloud platform introduced in February 2010 by Microsoft. The open-source cloud platform supports developing, storing data, managing services & hosting solutions. The most effective solution for your information requirements is provided by Windows Azure. This Computer Cloud service supports different operating systems, databases, tools, languages of programming and frames. This helps people to collect, monitor and analyze IoT data from sensors and other devices.

These services provide a number of tools to support, collect, automate, schedule and monitor the Azure deployment of a cloud manager. Microsoft Azure is one of the major global providers of public cloud services.

4. Google Cloud Platform

Google Cloud Platform is a computer resource provider for web application deployment and operations. Google Cloud Platform utilizes resources in Google Data Centers such as pcs, virtual makers, hard drives, etc. Google Cloud Storage is a cloud platform for storing large, unstructured information sets. Google Cloud provides application development services as well as integration services. Google Cloud Pub / Sub, for instance, is a managed and real-time messaging service for exchanging emails between apps. Like other public cloud services, most Google Cloud Platform services are pay-as-you-go and pay for the resources that they consume in the cloud. Google provides Google Cloud Platform training programs and certifications.

5. IBM Cloud

IBM Cloud means a collection of technology and services that have been created to assist clients in evaluating the readiness of their cloud, create adoption policies and define company points of enterprise in a cloud setting. A hybrid cloud model is used for IBM's cloud computing policy, which focuses on incorporating a company's personal cloud services into the public cloud. The IBM Cloud catalog lists more

COMP 001 – INTRODUCTION TO COMPUTING

than 170 different categories of service. IBM Cloud provides the data science tools like Spark, Hadoop and Watson Machine Learning IBM, and data streaming analytic services. Uses IBM Watson to provide machine learning, NLP and other services.

6. VMWare

VMware is a comprehensive platform for cloud management. It allows you to handle a hybrid environment from traditional workloads to containers. You can also maximize your organization's profit with these tools. VMware is a universal leader in cloud infrastructure and virtualization. VMware vCloud Air is a safe, secure public cloud platform providing Internet networking, storage, disaster recovery, and computing services. It offers extra integrations with custom apps and tools for third parties.

7. Salesforce

Multiple cloud services like the Sales Cloud, Service cloud, marketing cloud and so on are offered by Salesforce cloud computing. It allows your business to make correct and decisive decisions. Helps customer information management, business process automation, etc. Salesforce now provides a range of software and a platform for custom software developers and developers.

Customers from Salesforce usually claim it is unique for three main reasons:

- Fast: It may take more than one year for traditional CRM software to deploy; compare it with Salesforce for months or weeks.
- Easy: Salesforce wins with category hands that are simple to use. You can use it for longer and find it for less moment.
- Effective: As it is easy to use and can be tailored to meet business needs, Salesforce is very efficient for customers.

8. Alibaba Cloud

Alibaba Cloud provides extremely scalable cloud computing and data management services, with versatile, cost-effective solutions for tiny and large companies, financial institutions, governments, and other organizations to address their networking and data requirements. Alibaba Cloud operated the network that supports not only the broad online and mobile ecosystem of the Alibaba Group, but also a worldwide of cloud computing services providing support to sellers and the others involved in this ecosystem for many organizations worldwide. The Alibaba Group is one of the largest ecological ecosystem enterprises in the globe.

9. Rackspace

A range of cloud computing services is available from Rackspace Cloud, such as hosting internet apps, cloud files, cloud block storage, cloud backup, databases, and cloud servers. In order to achieve high-performance, Rackspace Cloud Storage utilizes a mixture of robust drives and hard drives. Cloud backup Rackspace utilizes methods of compression and encryption and offers file-level, low-cost backups.

10. Adobe

Adobe provides numerous cloud service goods. Few of these clubs include Adobe Creative Cloud, Adobe Experience and Adobe Document Cloud. Adobe creative cloud is a SaaS, which provides its customers with access to the tools Adobe provides, such as video editing, photography and graphic design. Adobe Experience Cloud provides its users access to a wide range of publicity, construction, and company intelligence solutions. Adobe Document Cloud is a comprehensive digital documentation solution.

COMP 001 – INTRODUCTION TO COMPUTING

11. Liquid Web

The Liquid website provides cloud websites, a managed hosting platform that allows creative internet building and launching without learning to manage cPanel or server. From the liquid web, you can rapidly and easily handle your sites. On the liquid web from a single account, we can host Unlimited sites and applications. The tool can be integrated easily with WordPress, Drupal, Joomla and so on.

12. Oracle Cloud

Innovative and integrated cloud services offered by Oracle Cloud. It can help you to build, deploy and manage cloud and local workloads. Oracle Cloud also allows businesses to transform and decrease complexity. Oracle allows you to understand the significance of contemporary technology such as artificial understanding, chatbots, machine education, and more.

13. Digital Ocean

Digitalocean's droplet is a cloud platform that provides add-on storage, security, and monitoring services to run applications efficiently. It is popular for its simplicity, the robustness of the servers. Also, it provides reliable infrastructure, and it is affordable. In DigitalOcean, we can create, automate, and manage a cloud server which is also called as DigitalOcean droplets, without worrying about technical aspects as it offers great features like Tier-1 bandwidth, support for all PHP based apps, shared private networking, floating IP addresses. It also has additional features such as SSD (solid-state drive) hard based servers, account management dashboard, backup support, etc. It provides advanced and pre-configured cache technologies for an optimized experience.

14. Dell Cloud

Dell offers a cloud platform, cloud-enabled infrastructure as well as cloud-based servers at the same time. The Dell Cloud is a highly scalable and reliable cloud platform that works with your existing operations. It helps to create and deploy applications with standard API libraries.

15. PhoenixNAP

PhoenixNAP is a global cloud service provider that offers highly secure and scalable Infrastructure. It provides private, public as well as managed cloud services along with Data Security Cloud, Virtual Private Data Center, etc., that helps to manage the business efficiently. PhoenixNAP is a great solution for advanced backup, disaster recovery as it mirrors the data globally. It is an ideal cloud platform which offers high bandwidth connectivity, compliance, security at an affordable price.

CLOUD COMPUTING IN DIFFERENT FIELDS

Now we are going to discuss the Examples of Cloud Computing which are mention below:

1. Dropbox, Facebook, Gmail

Cloud can be used for storage of files. The advantage is an easy backup. They automatically synchronize the files from the desktop. Dropbox allowing users to access files and storage up to 1 terabyte of free storage. Social Networking platform requires a powerful hosting to manage and store data in real-time. Cloud-based communication provides click-to-call capabilities from social networking sites, access to the Instant messaging system.

2. Banking, Financial Services

Consumers store financial information to cloud computing serviced providers. They store tax records as online backup services.

COMP 001 – INTRODUCTION TO COMPUTING

3. Health Care

Using cloud computing, Medical professionals host information, analytics and do diagnostics remotely. As healthcare also comes in the list of examples of cloud computing it allows other doctors around the world to immediately access this medical information for faster prescriptions and updates. Application of cloud computing in health care includes telemedicine, public and personal health care, E-health services and bioinformatics.

4. Education

This is useful in institutions of higher learning provide benefits to universities and colleges so henceforth Education comes in the examples of cloud computing. Google and Microsoft provide various services free of charge to staff and students in different learning institutions. Several Educational institutions in United States use them to improve efficiency, cut on costs. Example- Google App Education (GAE). They allow the user to use their personal workspace, teaching becomes more interactive.

5. Government

They deliver e-Governance services to citizens using cloud-based IT services. They have the technology to handle large transactions, citizens can see fewer congestion bottlenecks.

6. Big data Analytics

Big data analytics is another example of Cloud computing, As cloud computing enables data scientist in analyzing their data patterns, insights, correlations, predictions and help in good decision making. There are many open sources of big tools like Hadoop, Cassandra.

7. Communication

Cloud allows network-based access to communication tools like emails and calendars. Wats app is also a cloud-based infrastructure as it comes in communication it is also one of the examples of cloud computing. All the messages and information are stored in service providers' hardware.

8. Business Process

Business email is cloud-based. ERP, document management and CRM are based on a cloud service provider. SAAS has become an important method for the enterprise. Examples include Salesforce, HubSpot. They make many business processes more reliable because data can be copied at multiple redundant sites on the cloud providers.

The popularity of cloud computing is grooming day by day due to its numerous benefits. The ability to avoid expensive software license costs is one of the factors that enables companies to provide cloud services. They are internet based Cloud resources are available over the network anytime and are accessed through a standard mechanism that promotes use by different types of platforms (e.g.: mobile phones, laptops, and PDAs). They also help in e-learning by providing many services online for education. Cloud computing allows focusing more on business, not on data centers.

Impact of the Internet

The internet is the guiding technology of the IT Age just as the electrical engine was of the Industrial Age. The internet is a global network of inter-linked networks that mainly provide wireless interactive communication. Though the internet was first deployed in 1969, it was only in the 1990s that it became available to the public.

COMP 001 – INTRODUCTION TO COMPUTING

From there onwards, its use has diffused rapidly throughout the world with there being around 7 billion users of wireless devices currently that employ internet technology. With about 7.7 billion people in this world and with limited use among those under 5 years of age, it's almost safe to say that the entire humanity is now connected to the internet! There are however variations in the bandwidths available, the efficiency and cost of its use.

It's been postulated that about 95% of all information available has been digitized and made accessible via the internet. The internet has also led to a complete transformation in communication, availability of knowledge as well as social interaction. However, as with all major technological changes, there are positive and negative effects of the internet on society too.

The positive impacts of the internet include the following:

- It provides effective communication using emailing and instant messaging services to any part of the world.
- It improves business interactions and transactions, saving on vital time.
- Banking and shopping online have made life less complicated.
- You can access the latest news from any part of the world without depending on the TV or newspaper.
- Education has received a huge boost as uncountable books and journals are available online from libraries across the world. This has made research easier. Students can now opt for online courses using the internet.
- Application for jobs has also become easier as most vacancies are advertised online with online applications becoming the norm.
- Professionals can now exchange information and materials online, thus enhancing research.

The negative impacts of the internet on society include:

- Easy availability of illegal or inappropriate materials online that isn't age-suitable.
- Addiction to social networks can disrupt an individual's life, both personally and professionally.
- Some miscreants use the internet to hack into people's accounts for spurious activities including stealing data or banking information.
- Yet others have been known to misuse the internet for spreading hate and terrorism, two dangerously catastrophic scenarios.

Internet Security

What Does Internet Security Mean?

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.

According to Techopedia

Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments.

COMP 001 – INTRODUCTION TO COMPUTING

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

WHY WEB SECURITY IS SO IMPORTANT

As technology changes, it becomes increasingly challenging for businesses of all types to keep their personal and customer's information on the web secure.

Web security is important to keeping hackers and cyber-thieves from accessing sensitive information. Without a proactive security strategy, businesses risk the spread and escalation of malware, attacks on other websites, networks, and other IT infrastructures. If a hacker is successful, attacks can spread from computer to computer, making it difficult to find the origin.

How Do I Know if a Website Is Secure?

There are many ways to know if a website is secure, including implementing HTTPS on your website. In addition to HTTPS, you can tell if a website is trustworthy by asking yourself:

- Is the website an established authority institution?
- Does the site provide expert value?
- Does the website look spammy, broken?
- When I hover over the links does the link look spammy?

How Do I Make My Information on the Web More Secure?

The best line of defense on the web starts with user awareness. Avoid the risk of web security attacks and implement these 5 security tips:

1. Use Strong Passwords

It used to be that 3 or 4 character passwords would keep your information safe. However, as technology has advanced, so have the abilities and ways to crack passwords. Now, your passwords need at least 8 characters with a mixture of lower case letters, capitals, numbers, and a special character like an exclamation mark is highly recommended.

Don't make your password a familiar phrase. It might be easy for you to remember the phrase "I love my children" but a password cracking software will break that in no time. A great idea is to take the first letter of a phrase you will remember and use those, like this:

"I love my children, John, Mary, and Phil" would be "ILm3c-JM&P".

Never use a password twice. If someone hacks into any of your accounts then could access your bank accounts, your online purchase accounts, and any other important information.

2. Two-Factor Authorization

A two-factor authorization comes in handy when a website recognizes a different IP address is used to login to a website like your Google account. You are immediately sent a text message with a phone

COMP 001 – INTRODUCTION TO COMPUTING

number you registered with to confirm if it is you. If you didn't log in, you should immediately change the password to secure your account.

3. Always Use Secure Networks

When logging into financial and other crucial websites, look at the address bar before logging into your bank website and other sites on which you have personal information. If the address starts with HTTPS then you know it is secured (by the added "s"). If it doesn't, then you either have the wrong login page or it is possibly a spoof (fake) website.

Never click on a link in an email that seems suspicious. Better yet, never click on a link that comes from any crucial website such as your bank. Simply go to the website link you trust and have saved in your bookmarks to login, or call them. They will understand your caution.

4. Use More Than One Email Address

The email you use for your personal banking might be more secure if you use a different email for things like Facebook, Twitter, and even EBay. If someone were to hack into one then they would not automatically have access to the others.

5. Be Cautious About Posting Your Email Address Online

This is simply an invitation for spam if nothing else, but it also opens up a message of "Hey, hack me. Here's my email." Avoid posting your email address on forums, review sites, and message boards where spammers can easily pick up your address.

Types of Network Security

Cybercrime is one of the fastest-growing forms of criminal activity. The global cost of dealing with the damage caused by cybercrime is estimated to reach \$6 trillion by 2021, doubling the damage recorded in 2015. According to some reports, the average cost of a cyberattack is more than \$1 million, and is also expected to rise.

What network security types are available?

Network security refers to the various countermeasures put in place to protect the network and data stored on or passing through it. Network security works to keep the network safe from cyberattacks, hacking attempts, and employee negligence. There are three components of network security: hardware, software, and cloud services.

Hardware appliances are servers or devices that perform certain security functions within the networking environment. Hardware can be installed out of the path of network traffic, or "out-of-line," but it's more commonly installed in the path of traffic, or "in-line." The advantage of this is that in-line security appliances are able to stop data packets that have been flagged as potential threats, whereas out-of-line appliances simply monitor traffic and send alerts when they detect something malicious. Network security software, which includes antivirus applications, can be installed on devices and nodes across the network to provide added detection and threat remediation.

Cloud services refer to offloading the infrastructure to a cloud provider. The set-up is generally similar to how network traffic passes through in-line hardware appliances, but incoming network traffic is redirected

COMP 001 – INTRODUCTION TO COMPUTING

to the cloud service instead. The cloud service does the work of scanning and blocking potential threats for you before the traffic is allowed onto your network.

Every good network security system uses a combination of different types of network security tools to create a layered defense system. The theory behind this strategy is that if a threat manages to slip past one security countermeasure, the other layers will prevent it from gaining entry to the network. Each layer provides active monitoring, identification, and threat remediation capabilities in order to keep the network as secure as possible

What are the different types of network security devices and tools?

There are quite a few different networking security tools you can incorporate into your line-up of services. The following list is by no means exhaustive, but available security tools can include:

Access control.

This refers to controlling which users have access to the network or especially sensitive sections of the network. Using security policies, you can restrict network access to only recognized users and devices or grant limited access to noncompliant devices or guest users.

Antivirus and anti-malware software.

Malware, or “malicious software,” is a common form of cyberattack that comes in many different shapes and sizes. Some variations work quickly to delete files or corrupt data, while others can lie dormant for long periods of time and quietly allow hackers a back door into your systems. The best antivirus software will monitor network traffic in real time for malware, scan activity log files for signs of suspicious behavior or long-term patterns, and offer threat remediation capabilities.

Application security.

Each device and software product used within your networking environment offers a potential way in for hackers. For this reason, it is important that all programs be kept up-to-date and patched to prevent cyberattackers from exploiting vulnerabilities to access sensitive data. Application security refers to the combination of hardware, software, and best practices you use to monitor issues and close gaps in your security coverage.

Behavioral analytics.

In order to identify abnormal behavior, security support personnel need to establish a baseline of what constitutes normal behavior for a given customer’s users, applications, and network. Behavioral analytics software is designed to help identify common indicators of abnormal behavior, which can often be a sign that a security breach has occurred. By having a better sense of each customer’s baselines, MSPs can more quickly spot problems and isolate threats.

Data loss prevention.

Data loss prevention (DLP) technologies are those that prevent an organization’s employees from sharing valuable company information or sensitive data—whether unwittingly or with ill intent—outside the network. DLP technologies can prevent actions that could potentially expose data to bad actors outside the networking environment, such as uploading and downloading files, forwarding messages, or printing.

COMP 001 – INTRODUCTION TO COMPUTING

Distributed denial of service prevention.

Distributed denial of service (DDoS) attacks are becoming increasingly common. They function by overloading a network with one-sided connection requests that eventually cause the network to crash. A DDoS prevention tool scrubs incoming traffic to remove non legitimate traffic that could threaten your network, and may consist of a hardware appliance that works to filter out traffic before it reaches your firewalls.

Email security.

Email is an especially important factor to consider when implementing networking security tools. Numerous threat vectors, like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails. Because so many of these threats will often use elements of personal information in order to appear more convincing, it is important to ensure an organization's employees undergo sufficient security awareness training to detect when an email is suspicious. Email security software works to filter out incoming threats and can also be configured to prevent outgoing messages from sharing certain forms of data.

Firewalls.

Firewalls are another common element of a network security model. They essentially function as a gatekeeper between a network and the wider internet. Firewalls filter incoming and, in some cases, outgoing traffic by comparing data packets against predefined rules and policies, thereby preventing threats from accessing the network.

Mobile device security.

The vast majority of us have mobile devices that carry some form of personal or sensitive data we would like to keep protected. This is a fact that hackers are aware of and can easily take advantage of. Implementing mobile device security measures can limit device access to a network, which is a necessary step to ensuring network traffic stays private and doesn't leak out through vulnerable mobile connections.

Network segmentation.

Dividing and sorting network traffic based on certain classifications streamlines the job for security support personnel when it comes to applying policies. Segmented networks also make it easier to assign or deny authorization credentials for employees, ensuring no one is accessing information they should not be. Segmentation also helps to sequester potentially compromised devices or intrusions.

Security information and event management.

These security systems (called SIEMs) combine host-based and network-based intrusion detection systems that combine real-time network traffic monitoring with historical data log file scanning to provide administrators with a comprehensive picture of all activity across the network. SIEMs are similar to intrusion prevention systems (IPS), which scan network traffic for suspicious activity, policy violations, unauthorized access, and other signs of potentially malicious behavior in order to actively block the attempted intrusions. An IPS can also log security events and send notifications to the necessary players in the interest of keeping network administrators informed.

Web security.

Web security software serves a few purposes. First, it limits internet access for employees, with the intention of preventing them from accessing sites that could contain malware. It also blocks other web-based threats and works to protect a customer's web gateway.

COMP 001 – INTRODUCTION TO COMPUTING

What are the principles of network security?

There are three principles within the concept of network security—confidentiality, integrity, and availability—which together are sometimes referred to as the “CIA triad.” A network can only be considered secure when it has all three elements in play simultaneously.

Confidentiality works to keep sensitive data protected and sequestered away from where it can be accessed by the average user. This goes hand-in-hand with the principle of availability, which seeks to ensure that data and resources are kept accessible for those who are authorized to access them. Challenges to availability can include DDoS attacks or equipment failure. The principle of integrity seeks to protect information from intentional or accidental changes in order to keep the data reliable, accurate, and trustworthy.

Every decision made regarding network security should be working to further at least one of these principles. This means that MSPs need to ask if each decision will ensure that data is kept confidential, that its integrity will be protected, and that it will be made more easily available to those with authorization to access it.

Why are these network security concepts so important?

Cyberattacks are on the rise, with a recent report from Positive Technologies showing that government and healthcare organizations are becoming prime targets for hackers. The report also shows the goal of more than half of cybercrimes is data theft, and that financial gain was the motivation behind 42% of cyberattacks against individuals—and behind 30% of cyberattacks against organizations.

As our world becomes increasingly digitized, we rely more and more on the internet and networks to function. This in turn requires that the internet and networks provide us with reliable and secure service. However, as more of our personal and sensitive data is stored in electronic repositories and archives, hackers are turning their attention to networked systems. For this reason, it is imperative that MSPs and security support personnel offer customers robust security systems that protect data from various threat vectors.

How does Internet security work?

Internet browsers and Web servers have a secure way of talking to each other called http secure, or https. It works by combining “certificates” and encryption, a communications technique that scrambles the information as it crosses the Internet. Certificates are a type of digital security document used to prove the online identity of websites and application providers, as well as individuals and businesses. The very powerful and flexible https encryption, called SSL/TSL, overlays http, the basic standard underpinning all Internet communications.

You can tell when you have a secure connection by looking at the browser bar address window. Instead of “<http://mybank.com...>” you will see “<https://mybank.com...>” as pictured below. The “s” is for secure. You will also see the padlock. Click on the padlock to confirm the name on the site’s certificate is the same company you trust. Newer browsers color code the address bar green for safe sites with active encryption or red for potentially dangerous ones.

Other aspects of Internet security are protecting your passwords, not using hotspots to sign into your accounts and avoiding phishing or malware attacks from hackers and identity thieves.

INTERNET PROTOCOL

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since c. 2006.

Common Internet protocols

TCP/IP is a stream protocol. This means that a connection is negotiated between a client and a server. Any data transmitted between these two endpoints is guaranteed to arrive, thus it is a so-called lossless protocol. Since the TCP protocol (as it is also referred to in short form) can only connect two endpoints, it is also called a peer-to-peer protocol.

HTTP (Hypertext Transfer Protocol) is the protocol used to transmit all data present on the World Wide Web. This includes text, multimedia and graphics. It is the protocol used to transmit HTML, the language that makes all the fancy decorations in your browser. It works on TCP/IP.

FTP (File Transfer Protocol) is the protocol used to transmit files between computers connected to each other by a TCP/IP network, such as the Internet.