UNIT II

CLOUD INSIGHTS ARCHITECTURAL INFLUENCES

1. HIGH PERFORMANCE COMPUTING

- High-performance computing (HPC) is the practice of using parallel data processing to improve computing performance and perform complex calculations.
- HPC achieves these goals by aggregating computing power, so even advanced applications can run efficiently, reliably and quickly as per user needs and expectations.
- It thus delivers much higher power and better performance than traditional computers, workstations and servers.

The need for high-performance computing (HPC)

- In the modern world, groundbreaking discoveries and inventions can only happen with technology, data and advanced computing.
- As cutting-edge technologies like artificial intelligence (AI), machine learning (ML) and IoT evolve, they require huge amounts of data.
- They also need high-performance computing because HPC systems can perform quadrillions of calculations per second, compared to regular laptops or desktops that can perform at most 3 billion calculations per second (with a 3 GHz processor).
- HPC is specifically needed for these reasons:
  - It paves the way for new innovations in science, technology, business and academia.
  - It will complete a time-consuming operation in less time.
  - It will complete an operation under a light deadline and perform a high numbers of operations per second.
  - It is fast computing, we can compute in parallel over lot of computation elements CPU, GPU, etc. It sets up very fast network to connect between elements.
  - It improves processing speeds, which can be critical for many kinds of computing operations, applications and workloads.
  - It helps lay the foundation for a reliable, fast IT infrastructure that can store, process and analyze massive amounts of data for various applications.

Benefits of HPC

High speeds

- HPC is mainly about lightning-fast processing, which means HPC systems can perform massive amounts of calculations very quickly.
- In comparison, regular processors and computing systems would take longer -- days, weeks or even months -- to perform these same calculations.
- HPC systems typically use the latest CPUs and GPUs, as well as low-latency networking fabrics and block storage devices, to improve processing speeds and computing performance.

Lower cost

- Because an HPC system can process faster, applications can run faster and yield answers quickly, saving time or money.

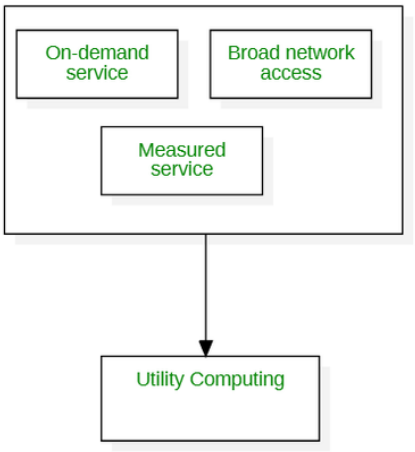
- Moreover, many such systems are available in "pay as you go" modes and can scale up or down as needed, further improving their cost-effectiveness.

Reduced need for physical testing

- Many modern-day applications require a lot of physical testing before they can be released for public or commercial use.
- Self-driven vehicles are one example.
- Application researchers, developers and testers can create powerful simulations using HPC systems, thus minimizing or even eliminating the need for expensive or repeated physical tests.

2. **UTILITY COMPUTING**

- Utility Computing is a type of computing that provide services and computing resources to customers.
- It is basically a facility that is being provided to users on their demand and charge them for specific usage.
- It is similar to cloud computing and therefore requires cloud-like infrastructure.
- It allows organization to allocate and segregate computing resources and infrastructure to various users on basis of their requirements.
- Utility computing is very similar to virtualization, so that the total amount of web storage space, along with the computing power that users receive, is much larger than a single time-sharing computer.
- Utility computing is divided into two types: Internal utility and External utility.
- Internal utility means that the computer network is shared only within a company.
- External utility is when used by many different computer companies to pool together a particular service provider.



Benefits of Utility Computing

Cost

- The cost of IT can be reduced due to Utility computing, given that existing resources can be used more effectively.
- In addition, the cost is transparent and can be assigned directly to different departments of a company.
- There will be fewer people required for operational activities in IT departments.

Flexibility

- Companies gain more flexibility, as their IT resources adapt to fluctuating demand more quickly and easily.
- Overall, the entire IT infrastructure is easier to manage, as application, which is an advantage for specific IT infrastructure.

3. GRID COMPUTING

- Grid computing is a computing infrastructure that combines computer resources spread over different geographical locations to achieve a common goal.
- All unused resources on multiple computers are pooled together and made available for a single task.
- Organizations use grid computing to perform large tasks or solve complex problems that are difficult to do on a single computer.
- All machines on that network work under the same protocol to act as a virtual supercomputer.
- The task that they work on may include analyzing huge datasets or simulating situations that require high computing power.
- Grid nodes and middleware work together to perform the grid computing task.
- In grid operations, three main types of grid nodes perform three different roles. They are:
    - User Node
    - Provider Node
    - Control Node

User node

- A user node is a computer that requests resources shared by other computers in grid computing.
- When the user node requires additional resources, the request goes through the middleware and is delivered to other nodes on the grid computing system.

Provider node

- In grid computing, nodes can often switch between the role of user and provider.
- A provider node is a computer that shares its resources for grid computing.
- When provider machines receive resource requests, they perform subtasks for the user nodes, such as forecasting stock prices for different markets.
- At the end of the process, the middleware collects and compiles all the results to obtain a global forecast.

Control node

- A control node administers the network and manages the allocation of the grid computing resources.
- The middleware runs on the control node.
- When the user node requests a resource, the middleware checks for available resources and assigns the task to a specific provider node.

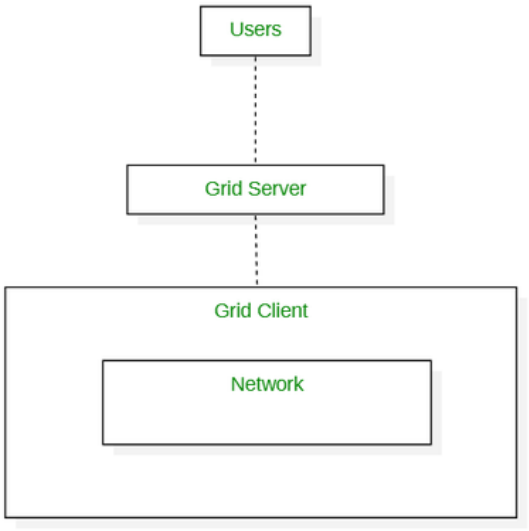


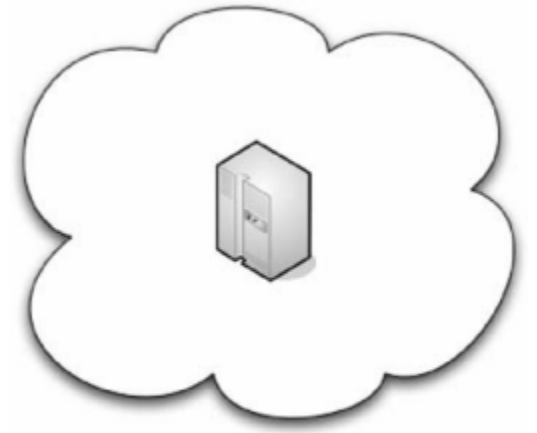
Figure 2: Grid Computing

4. CLOUD SCENARIOS

There are three different major implementations of cloud computing.

Compute Clouds

- In cloud computing, the term “compute” describes concepts and objects related to software computation.
- It is a generic term used to reference processing power, memory, networking, storage, and other resources required for the computational success of any program.
- Compute clouds allow access to highly scalable, inexpensive, on-demand computing resources that run the code that they’re given.
- Three examples of compute clouds are
    - Amazon Elastic Compute Cloud (Amazon EC2)
    - Google App Engine
    - Berkeley Open Infrastructure for Network Computing (BOINC)
- It is used by developers and businesses to run their applications in the cloud.
- These can help you build your applications on top of a server instance and pay only for the resources you need.

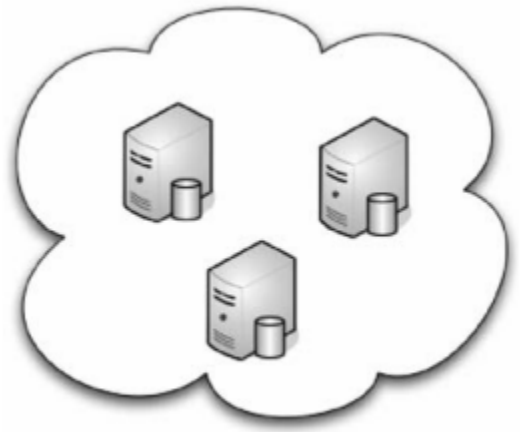


Compute clouds allow you to access applications maintained on a provider's equipment.

Figure 3: Compute Cloud

Cloud Storage

- One of the first cloud offerings was cloud storage and it remains a popular solution. There are already in excess of 100 vendors offering cloud storage.
- This is an ideal solution if you want to maintain files off-site.
- Security and cost are the top issues in this field and vary greatly, depending on the vendor you choose.
- Currently, Amazon Simple Storage Service (Amazon S3) is the widely used cloud storage.



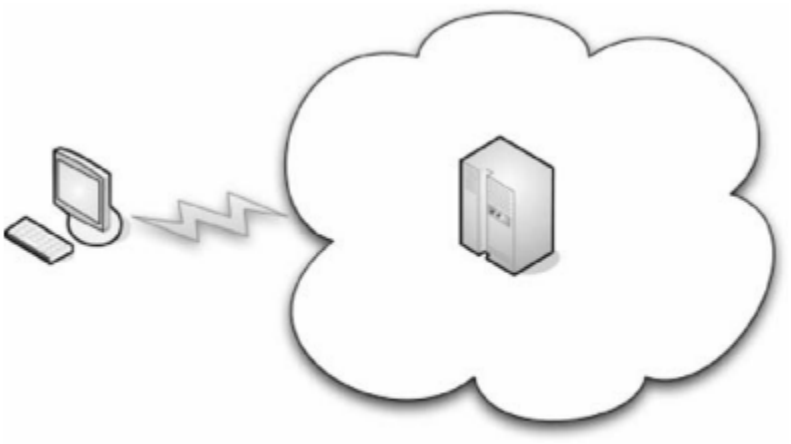
Cloud storage allows you to store your data on a vendor's equipment.

Figure 4: Cloud Storage

Cloud Applications

- Cloud applications differ from compute clouds in that they utilize software applications that rely on cloud infrastructure.
- Cloud applications are versions of Software as a Service (SaaS) and include such things as web applications that are delivered to users via a browser or application like Microsoft Online Services.

- Cloud applications often eliminate the need to install and run the application on the customer's own computer, thus alleviating the burden of software maintenance, ongoing operation, and support.
- Some cloud applications include
    - Peer-to-peer computing (like Bit Torrent and Skype)
    - Web applications (like Myspace or YouTube)
    - SaaS (like Google Apps)
    - Software plus services (like Microsoft Online Services)



Cloud applications deliver applications that depend on the infrastructure of the Internet itself.

Figure 5: Cloud Applications

5. BENEFITS OF CLOUD COMPUTING

Scalability

- The requirements of an organization change with its growth trajectory.
- The logistics, infrastructure, or human resources requirements of a start-up, for instance, can be nowhere comparable to that of a large enterprise.
- With Cloud Computing, businesses can quickly scale up or down their operation and storage-based needs on the go.
- Cloud Computing eliminates the need related to purchasing and installing manual upgrades.
- Cloud solutions can easily handle such fluctuation in traffic volumes.

Simplicity

- With no need of buying and configuring a new equipment, the cloud solution makes it possible to get the application started immediately
- It costs a fraction of what it would cost to implement an on-site solution.

Vendors

- The first comers to the cloud computing party are actually very reputable companies.
- Companies like Amazon, Google, Microsoft, IBM, and Yahoo! have been good vendors because they have offered reliable service, plenty of capacity.

Security

- Vendors have strict privacy policies and employ stringent security measures, like proven cryptographic methods to authenticate users.
- Further, one can always encrypt his data before storing it on a provider's cloud.
- In some cases, between your encryption and the vendor's security measures, your data may be more secure than if it was stored in-house.

6. LIMITATIONS OF CLOUD COMPUTING

Sensitive Information

- Cloud service providers implement the best security standards to store important information.
- But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider.
- While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.
- Encrypting the data before sending it out protects it.
- If someone gets the encrypted data, they need the proper credentials or all they get is gibberish.

Application Development

- In some cases, the applications themselves are not ready to be used on the cloud.
- They may have little quirks that prevent them from being used to their fullest abilities, or they may not work whatsoever.
- First, the application might require a lot of bandwidth to communicate with users.
- The application might also take a lot of effort to integrate with other applications.
- If you try to relocate it to a cloud, one may find that the savings are erased by the additional effort required to maintain the integration.
- Some applications may not be able to communicate securely across the Internet.
- If they cannot communicate securely or through a tunnel, then the data is at risk.
- In the event the application cannot communicate securely, you will need to host it locally where you can have other means of security to protect data as it is transported across networks.
- Also, since the application results are being displayed on an interface like a web browser, one must ensure that the application is compatible with a variety of browsers and will operate properly using encryption like SSL, for some or all of the interaction your user has within the application.

7. SECURITY LEVEL OF THIRD PARTY

- All the reputable vendors are doing all they can to protect the data.
- If word gets out that they don't protect the data they house, then no one will want to do business with them
- There are a lot of ways that their cloud and your data can be compromised. Some of them are:
    - Hackers
    - Botnets

Hackers

- There's a lot they can do if they've compromised the data.
- It ranges from selling your proprietary information to your competition to surreptitiously encrypting the storage until you pay them off.
- Or they may just erase everything to damage your business and justify the action based on their ideological beliefs.
- Hackers are a real concern for your data managed on a cloud.
- Because your data is held on someone else's equipment, you may be at the mercy of whatever security measures they support.

Bot Attackers

- In a commonly recognized worst-case scenario, attackers use botnets to perform distributed denial of service(DDOS) attacks.

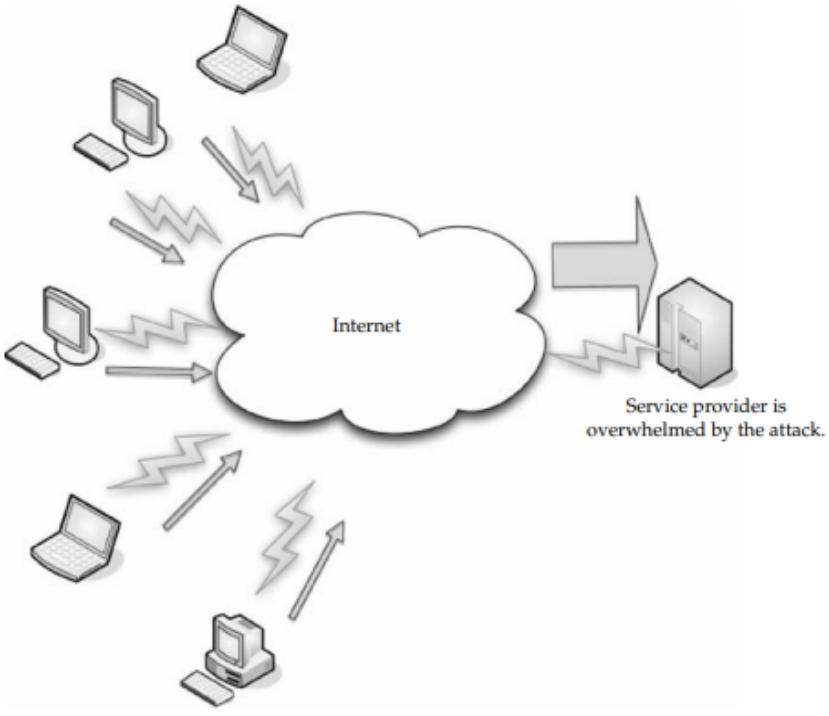


Figure 6:Security Concern

7.1. SECURITY BENEFITS

- Despite the security concerns, these third party service providers do endeavor to ensure security.
- Otherwise, word of mouth and repeat business will shrivel up.
- But the very nature of the cloud lends it to needing some very strong security practices.

Centralized Data

- There are some good security traits that come with centralizing your data.
- Just in practice, it makes the system more inherently secure

Reduced Data Loss

- By maintaining data on the cloud, employing strong access control, and limiting employee downloading to only what they need to perform a task, cloud computing can limit the amount of information that could potentially be lost.

Monitoring

- If your data is maintained on a cloud, it is easier to monitor security than having to worry about the security of numerous servers and clients.
- Of course, the chance that the cloud would be breached puts all the data at risk, but if you are mindful of security and keep up on it, you only have to worry about one location, rather than several locations.

Instant Swap over

- If the data is compromised, while one is conducting the investigation to find the culprits, you can instantly move your data to another machine.
- When one performs the swap over, it's seamless to your users. One does not have to spend hours trying to replicate the data or fix the breach.
- Abstracting the hardware allows you to do it instantly.

Logging

- In the cloud, logging is improved.
- Logging issues develop with storage space.
- On a cloud, you don't need to guess how much storage you'll need and you will likely maintain logs from the start. The only reason of concern will be the usage.
- Also, you can use more advanced logging techniques.

Secure Builds

- When you developed you own network, you had to buy third-party security software to
- get the level of protection you want.
- With a cloud solution, those tools can be bundled in and available to you and you can develop your system with whatever level of security you desire.
- Also, you can perform patches and upgrades offline.
- As you patch a server image, you can keep it safe offline, and when you are ready to put the virtual machine online, you can conveniently do that.
- Finally, the ability to test the impact of your security changes is enhanced.
- You simply perform and offline test the version of your production environment.

- This allows you to make sure the changes you make aren't detrimental to your network before you put it online.

Improved Software Security

- Vendors are likely to develop more efficient security software.
- Since you're charged for your CPU cycles, you're going to notice and squawk if the price is too high.
- As such, the vendor doesn't want to lose your business and is going to be more inclined to develop more efficient security software.
- Additionally, the vendor will be likely to look at the entire security setup and tune wherever possible for a more efficient system.
- They know that the security vendor who delivers the more efficient product will win the game.

Security Testing

- SaaS providers don't bill you for all of the security testing they do.
- It's shared among the cloud users.
- The end result is that because you are in a pool with others (you never see them, but they are there), you get to realize lower costs for security testing.
- This is also the case with PaaS where your developers create their own code, but the cloud code scanning tools check the code for security weaknesses.

8. REGULARITY ISSUES

- It's rare when we actually want the government in our business.
- In the case of cloud computing, however, regulation might be exactly what we need.
- Without some rules in place, it's too easy for service providers to be insecure or even shifty enough to make off with your data.

No existing Regulation

- Currently there is no existing regulation, but there should be.
- There isn't a third party insuring anyone's cloud data, and if a provider decides to close up shop, then that data can be lost.

Issues regarding the place of government in cloud computing

- First, if government can figure out a way to safeguard data—either from loss or theft any company facing such a loss would applaud the regulation.
- On the other hand, there are those who think the government should stay out of it and let competition and market forces guide cloud computing.

Issues regarding the ownership of the data

- A big problem is that people using cloud services don't understand the privacy and security implications of their online email accounts, their LinkedIn account, their MySpace page, and so forth.
- While these are popular sites for individuals, they are still considered cloud services and their regulation will affect other cloud services.

- Hence data's ownership can be claimed by both cloud service provider or by people using the cloud service.
- Therefore, the government will have to work out who owns the data.
- The government will also have to work out if law enforcement agencies have should have easier access to personal information on cloud data than that stored on a personal computer

Issues regarding government procurement

- There are also questions about whether government agencies will store their data on the cloud.
- Procurement regulations will have to change for government agencies to be keen on jumping on the cloud.