CLOUD COMPUTING - UNIT 2

Cloud Insights Architectural influences

Utility-Oriented Computing

1. Utility computing, or computer utility, is nothing but a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed and charges them for specific usage rather than a flat rate.
2. The term utility refers to utility services such as electricity,telephone, water and gas that are provided by a utility company. Similar to the electricity or telephone if the customer receives the utility computing, the computing power on a shared computer network, its consumption is measured and billed on that basis.
3. 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.
4. Utility computing is divided into two types: Internal utility and External utility.
5. Internal utility means that the computer network is shared only within a company.
6. Used by many different computer companies to pool together a particular service provider called an external utility.
7. Additionally, various hybrid forms are possible in this type of utility computing.

Advantages of Utility Computing

1. Cost
   - The cost of IT can be reduce 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.

2. 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.

Grid computing

1. Grid computing is a computing infrastructure that combines computer resources spread over different geographical locations to achieve a common goal.
2. All unused resources on multiple computers are pooled together and made available for a single task.
3. Organizations use grid computing to perform large tasks or solve complex problems that are difficult to do on a single computer.
4. 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.
5. Grid nodes and middleware work together to perform the grid computing task. In grid operations, the three main types of grid nodes perform three different roles.
   - **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.

Advantages of Grid Computing:

1. It is not centralized, as there are no servers required, except the control node which is just used for controlling and not for processing.
2. Multiple heterogeneous machines i.e. machines with different Operating Systems can use a single grid computing network.
3. Tasks can be performed parallelly across various physical locations and the users don't have to pay for them (with money).

Cloud scenarios

There are three different major implementations of cloud computing. How organisations are using cloud computing is quite different at a granular level, but the uses generally fall into one of these three solutions.

Compute Clouds

1. In cloud computing, the term "compute" describes concepts and objects related to software computation.
2. It is a generic term used to reference processing power, memory, networking, storage, and other resources required for the computational success of any program.

3. Compute clouds allow access to highly scalable, inexpensive, on-demand computing resources that run the code that they're given.
4. Three examples of compute clouds are
- Amazon Elastic Compute Cloud (Amazon EC2)
- Google App Engine
- Berkeley Open Infrastructure for Network Computing (BOINC)
5. 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.

Cloud Storage

1. 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.
2. This is an ideal solution if you want to maintain files off-site.
3. Security and cost are the top issues in this field and vary greatly, depending on the vendor you choose.
4. Currently, Amazon Simple Storage Service (Amazon S3) is the widely used cloud storage.

Cloud Applications

1. Cloud applications differ from compute clouds in that they utilize software applications that rely on cloud infrastructure.
2. 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.
3. 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.
4. Some cloud applications include
- Peer-to-peer computing (like BitTorrent and Skype)
- Web applications (like MySpace or YouTube)
- SaaS (like Google Apps)
- Software plus services (like Microsoft Online Services)

Benefits of cloud computing

Scalability

If you are anticipating a huge upswing in computing need (or even if you are surprised by a sudden demand), cloud computing can help you manage. Rather than having to buy, install, and configure new equipment, you can buy additional CPU cycles or storage from a third party. Since your costs are based on consumption, you likely wouldn't have to pay out as much as if you had to buy the equipment.Once you have fulfilled your need for additional equipment, you just stop using the cloud provider's services, and you don't have to deal with unneeded equipment. You simply add or subtract based on your organisation's need.

Simplicity

Again, not having to buy and configure new equipment allows you and your IT staff to get right to your business. The cloud solution makes it possible to get your application started immediately, and it costs a fraction of what it would cost to implement an on-site solution.

Knowledgeable Vendors

Typically, when new technology becomes popular, there are plenty of vendors who pop up to offer their version of that technology. This isn't always good, because a lot of those vendors tend to offer less than useful technology. By contrast, 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, and you get some brand familiarity with these well-known names.

Security

There are plenty of security risks when using a cloud vendor, but reputable companies strive to keep you safe and secure.

Security Benefits

This is not to suggest that your data is unsecure on the cloud. 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

We've talked about the specter of data loss by being in one place. However, there are some good security traits that come with centralizing your data. Just in practice, you make your system more inherently secure.

Reduced Data Loss

More than 12,000 laptops are lost in American airports every year. It's bad enough to lose your data, but it's especially bad for companies who lose proprietary data or other mission-critical information. Also, how many laptops employ really strong security measures, like whole-disk data encryption? If the laptop can be effectively compromised, the information will be in the hands of the thief. 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 have 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.

Instant Swapover

If your data is compromised, while you are conducting your investigation to find the culprits, you can instantly move your data to another machine. You also don't need to spend the time explaining to your C-level management that the system will be down due to an incident. When you perform the swapover, it's seamless to your users. You don't 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 is usually thought of late in the game, and 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 get-go, if for no other reason than to check your usage. Also, you can use more advanced logging techniques. For instance, a C2 audit trail can be employed. This is generally rarely used because of the performance hit your network would take. However, in the cloud, you can reach that level of granularity.

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.

Limitations of cloud computing

- Access to Sensitive information

1. Security, trust, and privacy issues are major obstacles for massive adoption of cloud computing.
2. The traditional cryptographic technologies are used to prevent data tampering and access to sensitive information.
3. The massive use of virtualization technologies exposes the existing system to new threats, which previously were not considered applicable.
4. The lack of control over their own data and processes also poses severe problems for the trust we give to the cloud service provider and the level of privacy we want to have for our data.
5. That doesn't mean you can't maintain your data on a cloud; you just need to be safe. The best way is to encrypt your data before you send it to a third party. Programs like PGP (www.pgp.com) or open-source TrueCrypt (www.truecrypt.org) can encrypt the file so that only those with a password can access it.
6. Encrypting your data before sending it out protects it. If someone does get your data, they need the proper credentials or all they get is gibberish.
7. In general, look for paid services, rather than those funded by advertising. Those are most likely to rummage through your data looking to assemble user profiles that can be used for marketing or other purposes. No company can provide you with free tangible goods or services and stay in business for long.

- Regularity issues
    1. 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.

2. Without some rules in place, it's too easy for service providers to be unsecure or even shifty enough to make off with your data.
3. Currently there is no existing regulation, but there should be.
4. In September 2008, the United States government took control of Washington Mutual. It was viewed as the greatest bank failure in American history to date.
5. It reminds us that no matter how huge a company is, it can still come tumbling down.
6. While banks deal in money, and cloud service providers deal in data, both are of immense value to consumers and organizations alike.
7. 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.

- Government policies
    1. Is it the government's place to regulate cloud computing? There are two schools of thought on the issue.
    2. 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.
    3. 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. e important questions that government needs to work out.
    4. First, who owns the data? Also, should law enforcement agencies have easier access to personal information on cloud data than that stored on a personal computer?

5. 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.
6. While these are popular sites for individuals, they are still considered cloud services and their regulation will affect other cloud services.