Survey on Resemblance of Cloud and Grid

Shashi Brajpuriya

Near Lok Bharti School, Ramnagar,
Supela, Bhilai, Dist. Durg – 230049, Chhattisgarh
sbrajpuriya87@gmail.com

Abstract: ***Cloud Computing is a new technique of computing that is extensively used in today's industry is as well as society. It is also a new breed of service offered overview the internet, which has completely changed the way one can use the power of computers irrespective of geographical location could computing brings the revolutionary changes in the world of Information Communication Technology .It has brought in new avenues for organization and business to offer services using hardware failure of software installs or platform of third part sources and it users to avoid locally hosting multiple servers, devices equipments, and upgrading and computability issues. For many organizations cloud computing can simplify process and save time and costs and work flows they have. This paper discuss the cloud computing definitions, types of cloud, public cloud versus private cloud, grid computing, common issues of cloud and grid computing, differences between cloud and grid computing, advantages and disadvantages Security Model.***

Keywords : Cloud Computing, Grid Computing, Model.

1. Introduction

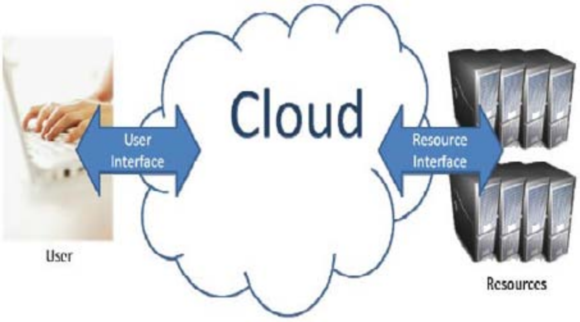
Cloud computing technology has grown very fast in the last few years in Information Technology sectors and shown its high growth rate. It has given access to its consumers and business to use applications without installation and access their personal files at any compilation with Internet access. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data centre from a capital intensive set up a variable priced environment. There are many synonyms for cloud computing such as 'on demand computing', 'grid computing', 'distributed computing', 'software as a service', 'information utilities', or ' automatic computing'. The internet as a platform and others, 1 Cloud computing is used by almost those all who have accessed and connected to the internet on a regular basis. Whether they are the internet on a regular basis. Whether they are using Google's Gmail, to ward processing or photo sharing or video sharing one can use products that live I the cloud. Which are secure, backed-up and accessible from an internet connection. The best example of this is G – mail.

1.1.1 What is Cloud Computing

"A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet". [2]

Cloud Computing offers its users services and applications, which are provided through the Internet, and thus, a large number of computers will be in the path of the data when the data is sent to the Cloud for analysis, and, also, when the data is coming back from the Cloud, once the analysis has been already carried out. For instance, a Mobile phone or PDA with low processing power and/or low storage capacity could take advantage of the Cloud and store or process data inside it, which would allow the mobile phone or the PDA to use applications which require more processing power than the processing power available in these kinds of electronic devices and, which will also require a permanent broadband connection in order to send and receive data at any moment from any place, thus allowing the user to access the services wherever you are. [1]

As another example of possible users that would be interested in Cloud Computing, there are lots of small and medium-sized companies that want to provide users with a new service which requires a lot of processing power, storage power and even networking capacity. To establish this infrastructure, the company should invest a lot of money in a large number of computers to process all the incoming requests, even if the peak load appears only once in a while and for these companies it makes it impossible to deploy the service due to the lack of resources. To solve this, one very small company which wants to provide a new service to a large number of customers could either use its own private Cloud (which can be either one or two computers, for example) and then, every time a peak demand appears, use the public Cloud to process the data (one example is Amazon EC2) or directly put its server into the Cloud and pay for the amount of processing power or storage capacity used at the end of the month: instead of contracting two servers for the full month, when required, they could contract one small server and increase the processing capacity through the Cloud processing and/or storage services. [1]



1.1.2 Types Of Cloud

1.1.2.1 Public Cloud

In a typical cloud computing scenario organizations run their applications from a data centre provided by a third-party – the cloud provider. The provider is responsible for providing the infrastructure, servers, storage and networking necessary to ensure the availability and scalability of the applications. This is what most people mean when they refer to cloud computing i.e. a public cloud.[15]

1.1.2.2 Private Cloud

A private cloud is a proprietary computing architecture, owned or leased by a single reorganization, which provides hosted services behind a firewall to "customers" within the organization. Some commentators regard the term "private cloud" as an oxymoron. They say that the word "cloud" implies an infrastructure running over the Internet, not one hidden behind a corporate firewall. [15]

1.1.2 Public Cloud Versus Private Cloud

There is, however, a larger body of opinion suggesting that private clouds will be the route chosen by many large enterprises and that there will be substantial investment in this area. Already vendors are lining up to release products that will enable enterprises to more easily offer internal cloud services. Whilst we will undoubtedly see a huge growth in private clouds we need to be careful that this is not just some re-badging of what is there already. Calling the services offered by the internal data centre a "private cloud" without changing management processes, organization/culture and the relationship with business customers is not going to hack it. If your data centre can't provision new environments, add new storage or increase computing power within minutes (or at worst within hours) then you are not operating in a cloud environment. Today there are very few companies that have the internal knowledge and the resources to create and effectively manage true cloud computing infrastructures. This will change as the market for cloud services matures and as new products emerge to help with rolling out private cloud-related services within the enterprise data centre. We will also see the adoption of hybrid cloud environments where organizations will combine the advantages of a public cloud with an internal private cloud. Some applications, or parts of applications, could run in the public cloud while others remain behind the corporate firewall. This paper examines the issues around cloud computing in its true sense of the meaning i.e. the public cloud. However, many of the points made can be applied to a private cloud. Regardless of which route you end up following (private, public or hybrid) your expectations of what you should be getting for your money remain the same. [15]

1.1.3 What Is Grid Computing?

"A Computational Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with the Intend of providing users easy access to these resources."[1]
Three point checklist to define what a Grid is. In this list he said:

- **"Coordinates resources that are not subject to centralized control" :** Which means that not only one entity manages all the system but some different system administrators could be managing different parts of the same Grid at the same time.
- **"Using standards, open, general-purpose protocols and interfaces" :** This will allow to all the companies involved in the Grid to use and access these standards.
- **"To deliver nontrivial qualities of service" :** In Grid computing not a fixed rate of load is going to be managed and this can be given small or big rates. This phenomenon causes the given quality of service to vary and not always stay constant.[8]

Grids allow the use of idle resources. Through this, companies create a Grid in order to share those idle resources and, if necessary, they can access more computational resources (shared by other companies) than they usually can, and share their own resources
while they are not carrying out any computationally demanding tasks. About the architecture, a lot of heterogeneous hardware is used in order to create the Grid and, in addition, these devices are not managed by only one person but by different system administrators in each of the companies. This situation causes the security, administration policies and network managing to become heterogeneous too, thus more difficult to manage.

1.1.2 Common Issues Of Cloud And Grid Computing

- To achieve good scalability, data must be distributed over many computers
- People can be afraid of sending sensitive data through a large number of computers.
- Data must be moved repeatedly to distant computers, which generates the bottleneck of the process, since the data is not always available everywhere and sometimes it is necessary to make this data available.

- Data can be requested regardless of its location[2]
- “Cloud and Grid computing provide service-level agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for receiving data late. ” [6]
- Both systems must be able to determine the amount of unused resources [6].

- **1.1.6 Differences Between Cloud And Grid Computing**

SNo	Cloud Computing	Grid Computing
1	Cloud computing normally runs in a set of homogeneous computers,	but Grid, on the other hand, runs on heterogeneous computers
2	Cloud Computing offers two types of Calculus's: standard and intensive	Grid computing is normally focused on an intensive calculus
3	Cloud Computing is not an open source	Grid computing is open-source
4	in Cloud Computing all users share all the resources at the same time	Most Grids use a batch-scheduled compute model
5	Cloud does relay on virtualization.	Grids do not rely on virtualization
6	High Performance computing is less supported comparatively Grid computing	High Performance computing is better supported In Grid computing [1]

1.1.3 Advantages & Disadvantages Of Cloud Computing

There is a huge amount of hype surrounding cloud computing but despite this more and more C-level executives and IT decision makers agree that it is a real technology option. It has moved rom futuristic technology to a commercially viable alternative to running applications in-house.
Vendor organisations such as Amazon, Google, Microsoft and Salesforce.com have invested many millions in setting up cloud computing platforms that they can offer out to 3rd parties. They clearly see a big future for cloud computing. Of course, no technology comes without a set of advantages and disadvantages so we’ve tried to sort to wheat from the chaff when it comes to the reality of cloud computing. In particular, one always has to be cautious in believing the claims of any specific vendor. [15]

1.1.4 Advantages And Disadvantages Of Grid Computing

- Federated yet separately administered resources, spanning multiple sites, countries and continents;
- Heterogeneous resources (e.g. hardware architectures, operating systems, storage back-ends, network setups);
- Distributed, multiple research user communities (including users accessing resources from varied administration domains) grouped in Virtual Organizations (VO).
- Mostly publicly funded (both resources and engineering, but not necessarily from the same funding source), at local, national and international levels;
- Range of data models, ranging from massive data sources, hard to replicate (e.g. medical data only accessible at hospital premises), to transient datasets composed of varied file sizes.[9]

2.6 Security Model [2.2]

Clouds mostly comprise dedicated data centers belonging to the same organization, and within each data center, hardware and software configurations and supporting platforms are in general more homogeneous as compared with those in Grid environments. Interoperability can become a serious issue for cross-data center, cross-administration domain interactions, imagine running your accounting service in Amazon EC2 while your other business operations on Google infrastructure. Grids however build on the assumption that resources are heterogeneous and dynamic, and each Grid site may have its own administration domain and operation autonomy. Thus, security has been engineered in the fundamental Grid infrastructure. The key issues considered are: single sign-on, so that users can log on only once and have access to multiple
Grid sites, this will also facilitate accounting and auditing; delegation, so that a program can be authorized to access resources on a user's behalf and it can further delegate to other
programs; privacy, integrity and segregation, resources belonging to one user cannot be accessed by unauthorized users, and cannot be tampered during transfer; coordinated resource allocation, reservation, and sharing, taking into consideration of both global and local resource usage policies. The public-key based GSI (Grid Security Infrastructure) protocols are used for authentication, communication protection, and authorization. Furthermore, CAS (Community
Authorization Service) is designed for advanced resource authorization within and across communities. Gruber (A Grid Resource Usage SLA Broker) [14] is an example that has
distributed policy enforcement points to enforce both local usage policies and global SLAs (Service Level Agreement), which allows resources at individual sites to be efficiently
shared in multi-site, multi-VO environments. Currently, the security model for Clouds seems to be relatively simpler and less secure than the security model adopted by Grids. Cloud infrastructure typically rely on Web forms (over SSL) to create and manage account information for end-users, and allows users to reset their passwords and receive new passwords via Emails in an unsafe and unencrypted communication. Note that new users could use Clouds relatively easily and almost instantly, with a credit card and/or email address. To contrast this, Grids are stricter about its security. For example, although web forms are used to manage user accounts, sensitive information about new accounts and passwords requires also a person to person conversation to verify the person, perhaps verification from a sponsoring person who already has an account, and passwords will only be faxed or mailed, but under no circumstance will they be
emailed. The Grid approach to security might be more time consuming, but it adds an extra level of security to help prevent unauthorized access. Security is one of the largest concerns for the adoption of Cloud Computing. We outline seven risks a Cloud user should raise with vendors before committing [6]:

1. Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions,"

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability,"

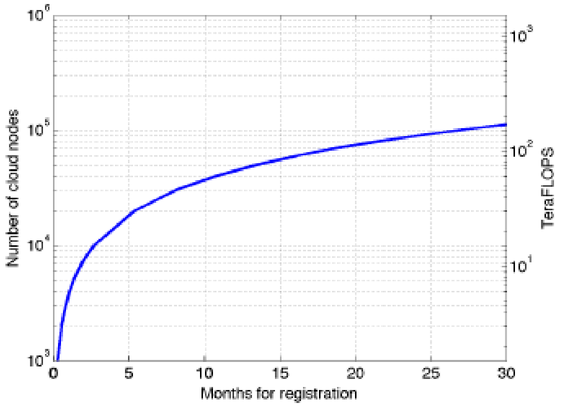
5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says.

Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,"

1) Privileged user access: All sensitive data processed outside the enterprise needs the assurance that they are only accessible and propagated to privileged users.
2) Regulatory compliance: A customer has to need verify if a Cloud vender has external audits and security certifications and if their infrastructure complies with some regulatory security requirements.
3) Data location: Since a customer will not know where her data will be stored, it is important that the Cloud provider commit to storing and processing data in specific jurisdictions and to obey local privacy requirements on behalf of the customer;
4) Data segregation: one needs to ensure that one customer's data is fully segregated from another customer's data;
5) Recovery: it is important that the Cloud provider has an efficient replication and recovery mechanism to restore data if a disaster occurs;
6) Investigative support: Cloud services are especially difficult to investigate, if this is important for a customer, then such support needs to be ensured with a contractual commitment; and
7) Long-term viability: your data should be viable even the Cloud provider is acquired by another company
Analysis



References

[1] Derrick Kondo, Bahman Javadi, Paul Malecot, Franck Cappello, David P. Anderson, Cost-Benefit Analysis of Cloud Computing versus Desktop Grids

[2] J. Brodkin. "Gartner: Seven cloud-computing security risks",

[3] http://www.networkworld.com/news/2008/070208-cloud.html, 2008.