ISSN 2250-3153

Companies in the cloud: Cloud Computing

Jyoti Rathee[*], Tamanna[**], Nitin Nara[***]

[*] M.Tech (C.S.E.) 2ndyear, S.P.G.O.I., Rohtak
[**] M.Tech (C.S.E.) 2ndyear, S.P.G.O.I., Rohtak
[***] M.Tech (C.S.E.) 2ndyear, S.P.G.O.I., Rohtak

Abstract- Cloud computing is on-demand, pay per use service which is for user's convenience and here the user has not pay for maintenance cost. It is a computing platform for the next generation. Because of it is new technology, it has both advantages and disadvantages. Cloud refers to a scalable networks of computers that work together like internet. Cloud deployment models are: SaaS, PaaS, IaaS. It helps in many ways the IT industry and also improve efficiency.

Index Terms- Cloud computing, SaaS, PaaS, IaaS

I. INTRODUCTION

Cloud computing portends a major change in how we store information and run applications. Instead of running programs and data on an individual desktop computer, everything is hosted in the "cloud"—a nebulous assemblage of computers and servers accessed via the Internet.

Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate.

With traditional desktop computing, you run copies of software programs on each computer you own. The documents you create are stored on the computer on which they were created. Although documents can be accessed from other computers on the network, they can't be accessed by computers outside the network. The whole scene is PC-centric.

With cloud computing, the software programs you use aren't run from your personal computer, but are rather stored on servers accessed via the Internet. If your computer crashes, the software is still available for others to use. Same goes for the documents you create; they're stored on a collection of servers accessed via the Internet. Anyone with permission can not only access the documents, but can also edit and collaborate on those documents in real time. it's document-centric.

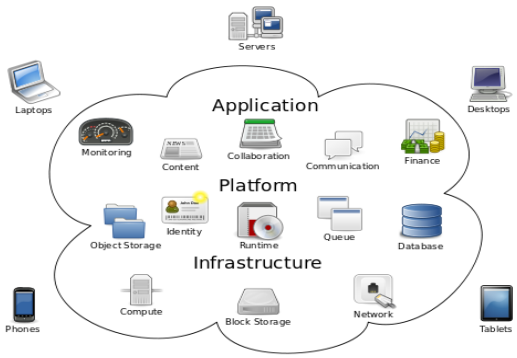

Figure1: Cloud Computing

Cloud computing isn't network computing. With network computing, applications are hosted on a single company's server and accessed over the company's network. Cloud computing is a lot bigger than that. It encompasses multiple companies, multiple servers, and multiple networks .Plus, unlike network computing, cloud services and storage are accessible from anywhere in the world over an internet connection; with network computing, access is over the company's network only. For our purposes, the cloud is a large group of interconnected computers. These computers can be personal computers or network servers; they can be public or private. For example, Google hosts a cloud that consists of both smallish PCs and larger servers. Google's cloud is a private one (that is, Google owns it) that is publicly accessible (by Google's users).

Six key properties of cloud computing:

1. Cloud computing is user-centric. Once you as a user are connected to the cloud, whatever is stored there—documents, messages, images, applications, whatever—becomes yours. In addition, not only is the data yours, but you can also share it with others. In effect, any device that accesses your data in the cloud also becomes yours.

2. Cloud computing is task-centric. Instead of focusing on the application and what it can do, the focus is on what you need done and how the application can do it for you.
3. Cloud computing is powerful. Connecting hundreds or thousands of computers together in a cloud creates a wealth of computing power impossible with a single desktop PC.

4. Cloud computing is accessible. Because data is stored in the cloud, users can instantly retrieve more information from multiple repositories. You're not limited to a single source of data, as you are with a desktop PC.

5. Cloud computing is intelligent. With all the various data stored on the computer in a cloud, data mining and analysis are necessary to access that information in an intelligent manner.

6. Cloud computing is programmable. Many of the tasks necessary with cloud computing must be automated.[1]

II. THE CLOUD FORMATION

"You can see they've gone from 50 instances of EC2 usage up to 3,500 instances of EC2 usage. It's completely impractical in your own data center over the course of three days to scale from 50 servers to 3,500 servers."

Animoto – a small startup with limited resources, created an online service that generates a unique custom video from photos and music uploaded by users. When they put the application on facebook and it went viral and demand shot up through the roof. Astoundingly, they managed to scale from 50 servers to 3500 servers in three days – all without having to buy a single piece of hardware or having to create their own compute, network and storage infrastructure. This was all accomplished by renting compute infrastructure from cloud service provider – Amazon Elastic Cloud Computing (EC2) and complementary service management capabilities from management provider right scale which enabled automated workload monitoring and Virtual Machine provisioning on Amazon's EC2 infrastructure. The above example demonstrates how existing cloud infrastructure can be used to enable massive scale and agility at a very reasonable cost using:

1. Virtualization technology to dynamically: provision virtualized software applications, load balancers and web application servers on-demand.

2. Innovative distributed computing technology that allows database distribution.

3. A managed Service Oriented Architecture for Web Service deployment.

4. A large number of commodity hardware devices (servers, storage and network elements) Impressive as it is, this current state-of-the-art in cloud computing still is just a baby step when compared to what is expected in a fully functional cloud based service creation, delivery and assurance platform.

Consider the following:

a) While the infrastructure services used by service developers are dynamically provisioned, and billed on usage, the system administration and management costs continue to increase with the number of servers used.
b) While service delivery is able to scale in the current cloud model to support spikes in demand,
c) application availability,performance optimization and security management have to be implemented separately. Today, a host of other companies are actively trying to fill this need with additional services using customized point solutions.
d) Disaster Recovery (DR) and storage management (de-duplication, tiered storage) are mostly lacking and have to be individually implemented at additional cost and effort.

The above points highlight some of the reasons why the cloud is today divided into private and public instances. The rule of thumb that seems to have evolved is that if there is a need for developing and deploying services using more than 50 to 100 servers at near full utilization, then private clouds may prove economical. It is apparent that the datacenter infrastructure required to manage virtualized computing, network and storage resources in an integrated fashion has not yet evolved to take cloud computing to the next level. One of the reasons is that datacenters today are managed using a number of legacy management systems that invariably started with a server-centric management paradigm and have since evolved incrementally over the past couple of decades to accommodate the shift towards client-server and network based computing paradigms. As a result, there is no single system today that provides truly integrated cross-domain management capabilities required for a service-oriented cloud infrastructure. At best each management offers specialized management of a particular infrastructure silo (i.e. servers, storage and networks) or partial management across more than one silo. It is also quite common for similar management functionality to be duplicated in solutions provided by multiple vendors specializing in different domains. Further, the best practices promoted by each vendor may conflict when attempting end-to-end optimization across the datacenter.[2]

III. ARCHITECTURE & TYPES OF CLOUD COMPUTING

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture:

Services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service), which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud. Infrastructure-as-a-service (IaaS) refers to computing resources as a service .This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access. Platform-as-a-Service (PaaS) is similar to IaaS, but also includes operating systems and required service for a particular application. The data-Storage-as-a-Service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

The cloud service SaaS, where the entire application is running in the cloud. A well-known example of SaaS is salesforce.com. Another type of cloud services, where the application runs on the client; An example of this type of cloud services on the desktop is Apple's iTunes. It includes cloud platform for creating applications, which is used by developers. The application developers create a new SaaS application using the cloud platform.

With Cloud Computing, the next generation of Internet will allow us to "buy" IT services from a web portal, drastic expanding the types merchandise available beyond those on e-commerce sites such as eBay and Taobao.

Cloud architecture typically involves multiple cloud components communicating with each other over application programming interfaces usually web services. The two most significant components of cloud computing architecture are known as front end and back end. They connect to each other through a network, usually the inter-net. The front end is the side the computer uses or client sees. The back end is the "CLOUD" section of the system.

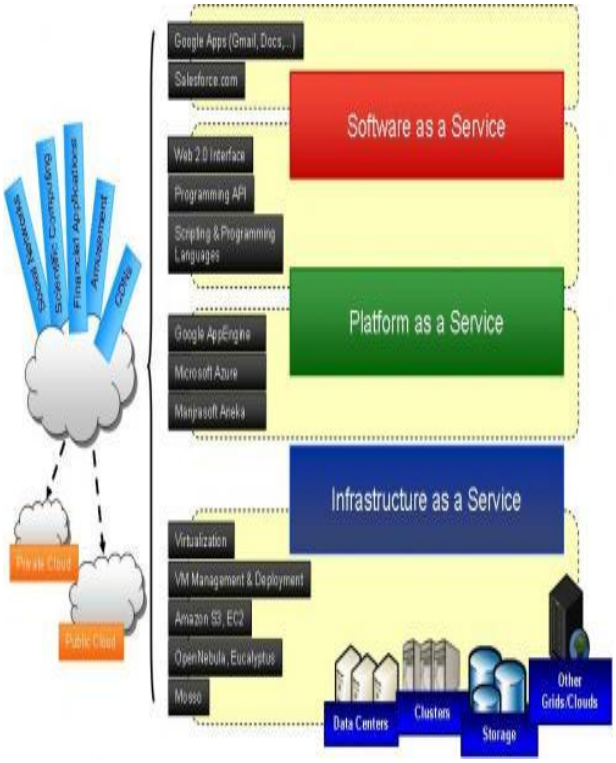

Figure 2: Cloud Computing layered architecture

If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies requires hundreds of digital storage devices. Cloud computing needs at least twice the no. of storage devices it requires to keep all its clients information stored. That's because these devices, like all computers occasionally break down. A cloud computer system must make a copy of all its clients information and store it on other devices. The copies enable the central server to access back-up machines to retrieve data that otherwise would be unreachable. Make copies of data as a back-up is called redundancy.[3]

IV. FCAPS

"Although the root cause of this particular issue was a resource contention issue between instances, things like that are going to continue to happen. There may now be a fix for this particular edge case, but there are undoubtedly others that will crop up over time. The real failure here was a failure of monitoring, and a failure of transparency."

This quotation from Oren Michels, the CEO of Mashery, regarding Amazon's EC2 outage, points out the need for application-specific Fault, Configuration, Accounting, Performance and Security (FCAPS) measurement, management and optimization.

Figure 3: Cloud Computing application

This paper restricts itself to fault, configuration, accounting, performance and security management. In short, the FCAPS capabilities. FCAPS have been adjudged to be the basic minimum management and operability capabilities necessary to offer useable services. ITIL guidelines have been gaining a lot of attention and increasing use, in particular, in the areas of IT service management. A comparison between the ITIL IT service management and FCAPS would show that FCAPS has most of the critical capabilities necessary for manageability and operability. ITIL of course has lot more in the form of guidance on processes and methods. The table below lists the various capabilities of FCAPS:

Each of these elemental capabilities may be implemented using agents that also utilize other agents such as instrumentation and monitoring agents. By separating services into fabrics and sub-fabrics and by incorporating FCAPS capabilities with in the service, a service can only affect or be affected by other services in a controlled fashion. Service security enforces its own access rights and permitted actions. At each layer of our services fabric, there are one or more management agents managing the services in their domain. All communications is by messages which themselves being first-class services have self-management capabilities and are also externally managed. The sub-fabrics also reduce the amount of "management data" (for example, various performance measures) to be managed at a manageable

level – the sub-fabric "partitions" the "total" raw data generated from all sub-fabrics into sub-fabric specific data only. Next, the different FCAPS capabilities are examined in the context of the business services fabric. Before visiting the various capabilities, let us look at a generic capability that is common to many of the FCAPS capabilities – events and performance instrumentation. For example, the alarm filtering capability in fault management can be implemented using an event filtering service agent.

a) Events and Performance Instrumentation
b) Fault Management
c) Configuration Management
d) Accounting Management (AM)
e) Security Management (SM)
f) Performance Management (PM)[4]

V. CLOUD SECURITY ISSUE:

Mobile users were more hampered by the speed limitations of dialup connections to branch or home offices. IT departments' focus was on perimeter security to ''keep the bad guys out'' of the corporate network by using stringent Network Access Control (NAC) parameters. Surveys of potential cloud-computing adopters indicate that lack of security is a primary deterrent to moving at least a part of an organizations' computing and data storage operations to the cloud. Most IT departments currently view that allowing services to be delivered by third parties means they lose control over how data is secured, audited, and maintained and they can't enforce what they can't control. In February 2009 ''Above the Clouds: A Berkeley View of Cloud Computing'' whitepaper by a team from the University of California – Berkeley's Reliable Adaptive Distributed (RAD) Systems Laboratory list the following as the first three of the ''Top 10 Obstacles for Growth of Cloud Computing''. Some of them are:

1. Availability of Service
2. Data Lock-In
3. Data Confidentiality and Audit ability[5]

Standards for Security**:**

Security standards define the processes, procedures, and practices necessary for implementing a security program. These standards also apply to cloud related IT activities and include specific steps that should be taken to ensure a secure environment is maintained that provides privacy and security of confidential information in a cloud environment. Security standards are based on a set of key principles intended to protect this type of trusted environment. Messaging standards, especially for security in the cloud, must also include nearly all the same considerations as any other IT security endeavor. A basic philosophy of security is to have layers of defense, a concept known as defense in depth. This means having overlapping systems designed to provide security even if one system fails. An example is a firewall working in conjunction with an intrusion-detection system (IDS). Defense in depth provides security because there is no single point of failure and no single entry vector at which an attack can occur. For this reason, a choice between implementing network security in the middle part of a network (i.e., in the cloud) or at the endpoints is a false dichotomy. Some protocols used for cloud security are:

SAML, O Auth, Open ID, SSL/TLS.

Security Assertion Markup Language (SAML): SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners. It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal. SAML is built on a number of existing standards, namely, SOAP, HTTP, and XML. SAML relies on HTTP as its communications protocol and specifies the use of SOAP. A SAML protocol describes how certain SAML elements. are packaged within SAML request and response elements. It provides processing rules that SAML entities must adhere to when using these elements. Generally, a SAML protocol is a simple request–response protocol. The most important type of SAML protocol request is a query.

Open Authentication (OAuth): OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications. OAuth is a method for publishing and interacting with protected data. For developers, OAuth provides users access to their data while protecting account credentials. OAuth allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity. OAuth by itself *provides no privacy at all* and depends on other protocols such as SSL to accomplish that.

OpenID:OpenID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity. It is a single-sign-on (SSO) method of access control. As such, it replaces the common log-in process by allowing users to log in once and gain access to resources across participating systems. An OpenID is in the form of a unique URL and is authenticated by the entity hosting the OpenID URL. The Open ID protocol does not rely on a central authority to authenticate a user's identity. Neither the OpenID protocol nor any web sites requiring identification can mandate that a specific type of authentication be used.

SSL/TLS:Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP. TLS and SSL encrypt the segments of network connections at the transport layer. Several versions of the protocols are in general use in web browsers, email, instant messaging, and voice-over-IP. The TLS protocol allows client/server applications to communicate across a network in a way specifically designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and data confidentiality by using cryptography.[6]

VI. CONCLUSION

The number of conclusion's are drawn:

1. It will for weather forecasting service. This web service will be helpful for weather forecasting organization.
2. Computation work will be done in very efficient manner with the help of cloud computing.
3. Cloud computing will prove boon for IT industry. Cloud computing is likely to have the same impact on software that foundries have had on the hardware industry.

The motivation factors of this study are :

a) To create an integration web service selection approach from cloud network.
b) To give details of cloud service providers.
c) To explain applications which makes it next generation computing and also challenges for cloud computing.

VII. FUTURE SCOPE

It is an interface which will work as an INTERMEDIATE CLOUD for cloud service provider selection for weather forecasting application. Further we can convert it as whole cloud which will compose of cloud web services that will collect response from other web services and return result for the development environment. We can integrate this for other approaches like

1 .Medical approach
2. Research work
3. Education field
4. Marketing sector
5. Retail sector
6. Entertainment sector

REFERENCES

[1] Michael Miller "cloud computing: web-based applications that change the way you work and collaborate online. ", que publishing,pp7-10

[2] Dr .RAO MIKKILINENI, VIJAY SARATHY "cloud computing and the lessons from the past", ieee infrastructure for collaborative enterprises, submitted for publication

[3] SPRINGER "handbook of cloud computing" editors: borko furht, armando escalante, pp 4 -7

[4] PANKAJ GOYAL SENIOR MEMBER IEEE, RAO MIKKILINENI, MURTHY GANTI "fcaps in the business services fabric model" ieee collaborative enterprises, submitted for publication

[5] ROGER JENNINGS "cloud computing with the windows azure platform" wiley publishing inc., pp 55-57

[6] JOHN W. RITTING HOUSE, JAMES F. RANSOME, "cloud computing implimentation, management and security" crc press, pp205-211

AUTHORS

First Author – Jyoti Rathee, B.Tech, Pursuing M.Tech, S.P.G.O.I, Email:ronellarathee@gmail.com
Second Author – Tamanna, B.Tech, Pursuing M.Tech, S.P.G.O.I, Email:tamanna2912@gmail.com
Third Author – Nitin Nara, B.Tech, Pursuing M.Tech, S.P.G.O.I, Email:raje.dhankher@gmail.com

Correspondence Author – Jyoti Rathee, B.Tech, Pursuing M.Tech, S.P.G.O.I, Email:ronellarathee@gmail.com, tamanna2912@gmail.com ,8059121221