A Review of Cloud Computing

[1]Dr. Kalpana Sharma
[1]Assistant Professor
[1]Computer Science & Engineering
[1]Bhagwant University, Ajmer, India

Abstract : In this paper we are presenting a review of cloud Computing. Cloud computing is growing rapidly, with applications in almost any area, including education. The cloud computing term was derived from the way the Internet is often represented in network diagrams. The term cloud as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of It, as schematic clouds. Cloud computing was coined for what happens when applications and services are moved into the internet cloud. Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. They are running applications as services over the Internet on a scalable infrastructure. Now, Cloud computing that introduces efficient scale mechanism can let construction of cloud system be entrusted to suppliers and provide a new mode for clouds.

IndexTerms **– Cloud Computing, IT, Resource, Service, Application.**

I. INTRODUCTION

Cloud computing becomes very popular because it moves the processing efforts from the local devices to the data center facilities. Therefore, any device, like an Internet connected phone, could be able to solve complex equations by simply passing the specific arguments to a service running at the data center level that will be capable to give back the results in a very short time. Many education institutions do not have the resources and infrastructure needed to run top e-learning solution. This is why Blackboard and Module, the biggest players in the field of e-learning software, have now versions of the base applications that are cloud oriented. E-learning is widely used today on different educational levels: continuous education, company trainings, academic courses, etc.

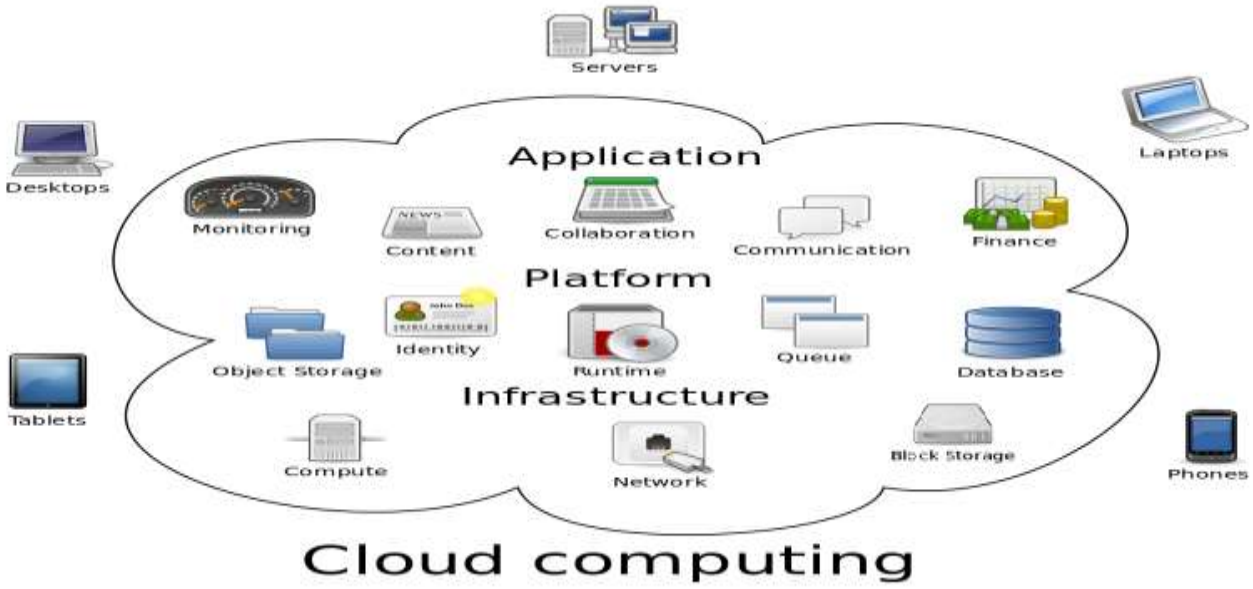
One of the biggest promoters of the cloud computing is Google that already owns a massive computer infrastructure (the cloud) where millions of people are connecting to. Today, the Google cloud can be accessed by Google Apps [6] intended to be software as a service suite dedicated to information sharing and security. Google Apps covers the following three main areas: messaging (Gmail, Calendar and Google Talk), collaboration (Google Docs, Video and Sites) and security (email security, encryption and archiving). There are many benefits from using the cloud computing for e-learning systems. Also, there are some disadvantages that have to be taken into account. Using cloud computing for e-learning solutions influences the way the e-learning software. There are specific tasks that deal with finding providers for cloud computing, depending on the requirements (infrastructure, platform or services). Also, the cost and risk management influences the way the e-learning solutions based on cloud computing are managed.

In Computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is usually Internet-based computing. The cloud is a metaphor for the Internet based on how the internet is described in computer network diagrams; which means it is an abstraction hiding the complex infrastructure of the internet.[1] It is a style of computing in which IT-related capabilities are provided “as a service”,[2] allowing users to access technology-enabled services from the Internet ("in the cloud")[3] without knowledge of, or control over the technologies behind these servers.[4]

Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.[1] Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand.[1][2][3] Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.[4]

Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing has led to growth in cloud computing.[5][6][7]

The cloud symbol was used to represent networks of computing equipment in the original ARPANET by as early as 1977,[10] and the CSNET by 1981[11] — both predecessors to the Internet itself. The word cloud was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics. With this simplification, the implication is that the specifics of how the end points of a network are connected are not relevant for the purposes of understanding the diagram.



II. CHARACTERISTICS

Cloud computing exhibits the following key characteristics:

- Performance is monitored by IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web services as the system interface.[40][45][46]
- Resource pooling is the provider's computing resources are commingle to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the consumer generally have no control or knowledge over the exact location of the provided resource.[1]
- Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.
- Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers[49]), without users having to engineer for peak loads. This gives the ability to scale up when the usage need increases or down if resources are not being used.
- Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because service providers are able to devote resources to solving security issues that many customers cannot afford to tackle or which they lack the technical skills to address. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
- Agility for organizations may be improved, as cloud computing may increase users' flexibility with re-provisioning, adding, or expanding technological infrastructure resources.

III. SECURITY AND PRIVACY

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. According to the Cloud Security Alliance, the top three threats in the cloud are Insecure Interfaces and API's, Data Loss & Leakage, and Hardware Failure—which accounted for 29%, 25% and 10% of all cloud security outages respectively. Together, these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There

are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process he called "hyperjacking". Some examples of this include the Dropbox security breach, and I Cloud 2014 leak. Dropbox had been breached in October 2014, having over 7 million of its users passwords stolen by hackers in an effort to get monetary value from it by Bitcoins (BTC). By having these passwords, they are able to read private data as well as have this data be indexed by search engines (making the information public). There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership. Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud. There is the risk that end users do not understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is becoming popular and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or Google Now). Fundamentally, private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.

IV. LIMITATIONS AND DISADVANTAGES

Privacy and confidentiality are big concerns in some activities. For instance, sworn translators working under the stipulations of an NDA, might face problems regarding sensitive data that are not encrypted. Cloud computing is beneficial to many enterprises; it lowers costs and allows them to focus on competence instead of on matters of IT and infrastructure. Nevertheless, cloud computing has proven to have some limitations and disadvantages, especially for smaller business operations, particularly regarding security and downtime. Technical outages are inevitable and occur sometimes when cloud service providers become overwhelmed in the process of serving their clients. This may result to temporary business suspension. Since this technology's systems rely on the internet, an individual cannot be able to access their applications, server or data from the cloud during an outage. According to Bruce Schneier, "The downside is that you will have limited customization options. Cloud computing is cheaper because of economics of scale, and — like any outsourced task — you tend to get what you get. A restaurant with a limited menu is cheaper than a personal chef who can cook anything you want. Fewer options at a much cheaper price: it's a feature, not a bug." He also suggests that "the cloud provider might not meet your legal needs" and that businesses need to weigh the benefits of cloud computing against the risks. In cloud computing, the control of the back end infrastructure is limited to the cloud vendor only. Cloud providers often decide on the management policies, which moderates what the cloud users are able to do with their deployment. Cloud users are also limited to the control and management of their applications, data and services. This includes data caps, which are placed on cloud users by the cloud vendor allocating certain amount of bandwidth for each customer and are often shared among other cloud users.

V. COMPARISONS

Cloud computing is often confused with other ideas:

- grid computing: a form of distributed computing whereby a "super and virtual computer" is composed of a cluster of networked, loosely-coupled computers, working together to perform very large tasks
- utility computing: the packaging of computing resources, such as computation and storage are provided as a measured service that have to be paid similar to a traditional public utility such as electricity[6]
- autonomic computing: computer systems capable of self-management.[7]

Cloud computing often uses grid computing, has autonomic characteristics and is billed like utilities, but cloud computing can be seen as a natural next step from the grid-utility model.[8] Some successful cloud architectures have little or no centralized infrastructure or billing systems including peer-to-peer networks like BitTorrent and Skype.[9]

VI. CLOUD SECURITY CONTROLS

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management.[8] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[8]

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[8] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

IV. CONCLUSION

The Academy of Economic Studies from Bucharest uses a cloud solution based on Module and it has its own datacenter that can be in the future a platform for cloud computing. A metrics system needs to be developed in order to measure the efficiency of cloud computing based cloud solutions. Cloud computing is not something that suddenly appeared overnight; in some form, it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Cloud computing has a variety of characteristics. In Computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is usually Internet-based computing.

REFERENCES

[1] What is Cloud Computing? 2013. Amazon Web Services. 2013-03-19. Retrieved 2013-03-20.

[2] Baburajan, Rajani 2011. The Rising Cloud Storage Market Opportunity Strengthens Vendors. It.tmcnet.com. Retrieved 2011-12-02.

[3] Oestreich, Ken, 2010. Converged Infrastructure. CTO Forum. Thectoforum.com. Archived from the original on 2012-01-13. Retrieved 2011-12-02.

[4] Where's The Rub 2014: Cloud Computing's Hidden Costs. 2014-02-27. Retrieved 2014-07-14.

[5] Cloud Computing: Clash of the clouds 2009. The Economist. 2009-10-15. Retrieved 2009-11-03.

[6] Gartner Says Cloud Computing Will Be As Influential As E-business. Gartner. Retrieved 2010-08-22.

[7] Gruman, Galen 2008. What cloud computing really means. InfoWorld. Retrieved 2009-06-02.

[8] Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta 2014. Amazon.com. 24 August 2006. Retrieved 31 May 2014.

[9] Antonio Regalado 2011. Who Coined Cloud Computing ? . Technology Review. MIT. Retrieved.

[10] Internet History 1977.

[11] Cloud Computing: Small Companies Take Flight

[12] Google Apps Admins Jittery About Gmail, Hopeful About Future

[13] A New Resource, Born of a Cloud Feud

[14] Google to go carbon neutral by 2008

[15] Nimbus Cloud Guide

[16] Google's Open Source Android OS Will Free the Wireless Web

[17] In Sync to Pierce the Cloud

[18] Microsoft demos mobile cloud sync client

[19] CherryPal brings cloud computing to the masses

[20] Zonbu has alluring features, price

[21] GOS cloud computing