

EVALUATION AND PERFORMANCE ANALYSIS ON CLOUD COMPUTING

^{*1}Ayushi Srivastava

Department of Computer Science & Engineering
Madan Mohan Malaviya University of technology,
Gorakhpur, India
e-mail: ayushiagra@gmail.com

²Ashish Kumar Singh

Department of Computer Science & Engineering
Madan Mohan Malaviya University of technology,
Gorakhpur, India
e-mail: ashi001.ipecc@gmail.com

ABSTRACT- Despite increasing usage of cloud computing. It is a modern era technique used almost all over the world. Cloud Computing has emerged as a popular computing model to support processing large volumetric data using clusters of commodity computers. It is a technology used in medical, enterprises, entertainment and gaming. This paper contains the details of cloud computing along with its challenges, advantages and security threats. The evolution of cloud computing can handle such massive data as per on demand service. This paper will help the researchers to get familiar with Cloud Computing. This paper includes different sections which are as follows- Section I presents the Introduction to the paper, Section II provides the brief description of Literature review and Section III concludes the paper in Conclusion section.

Keywords- Cloud Computing, virtual machine, models, security challenges.

I. INTRODUCTION

Cloud computing is a model for enabling omnipresent, convenient and on- demand network access to a shared pool of resources [1]. Resources in cloud computing are network, server, service, space and storage. Cloud is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things. Cloud computing is a pool of virtualized computing resources that allows users to gain access to applications and data in a web-based environment on demand.

Cloud computing is the collection of computing as a utility and software as a service where the applications are delivered as services over the Internet and the resources in data centers provide those services [1]. Various computing services can be accessed from any computer in any part of the world through Internet. All together it give the features that support high scalability and multi-tenancy, offer enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources vigorously with an ability to always monitor their performance.

Security, resources availability and resources allocation are the main challenges of Cloud Computing. In this paper Section II describes the detailed survey on cloud computing.

II. LITERATURE REVIEW

Cloud Computing can be compared with a banking system, where bank is similar to the environment provided to the users and bank locker can be compared

as the space provided to the user to keep their separate and individual documents/ data. For security issues the user had a password and their credentials to secure their data similarly as we have keys to the locker. The resources used in cloud computing include server, storage, network, application, service and so on [2]. The management of resources with reliability and frequent availability is a problem which is meant to be dealt with. Frequent availability is required when a user is moving from one place to another [3]. The issues of cloud computing are restricted bandwidth, network access management, quality of services, security and service convergence.

Lot of work has been done on these basics security issues which are discussed in [2]. But still many other security challenges and threats are there that needs to be resolved. They are data loss/ leakage, SQL injection attack, browser security, sniffer attack.

CHARACTERISTICS OF CLOUD COMPUTING

Characteristics of cloud computing is represented in figure1. Following are the characteristics of cloud computing:

i. Multi- tenancy

Cloud provides services to different employees of the same enterprise, such as the business units of different departments of the enterprise [1].

ii. On-demand self service

Cloud service provider provides on demand self service to the users without having human interaction. Services are email, applications, network etc.

iii. Broad network access

Cloud services are available over the network and can be accessed by heterogeneous platforms used by the clients, such as mobile phones, laptops etc.

iv. Resource pooling

The resources of cloud are storage, processing, memory, network bandwidth, virtual machines, email services etc. the service provider is responsible for the dynamically assigning and reassigning the resources according to the client.

v. Rapid elasticity

Cloud services can be rapidly provisioned to scale out and released to scale in quickly [6].

vi. Measured service

Cloud computing resources usage can be measured, controlled, reported and estimated providing transparency for provider and consumer both. The measure services are pay per use means the more you utilize the higher the bill [7].

vii. External data storage

All the data and documents of customers are stored externally at the location of the cloud computing vendor.

viii. Rented service delivery model

Cloud Computing is a Pay per use service. Customers pay for the service for using the applications and software instead of buying the license [1].

Cloud computing also shares characteristics with:

- Client server model
- Grid computing
- Mainframe computer
- Utility computing
- Peer-to-peer

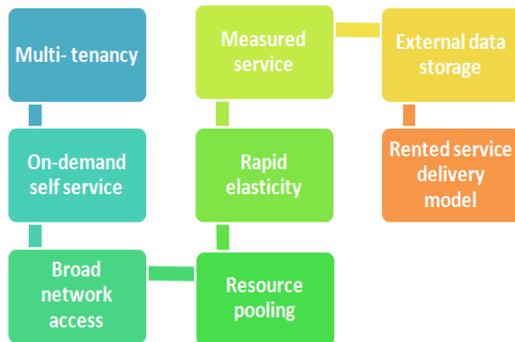


Figure1. CHARACTERISTICS OF CLOUD COMPUTING

i. Infrastructure as a Service (IaaS)

IaaS provides an on-demand infrastructure in the form of virtual hardware, storage and networking collectively called virtual machines. Virtual hardware provides on demand computation, virtual storage provides raw disk space and virtual networking has the collection of services which helps in managing the network and its connectivity among the virtual instances over the Internet. Some examples of IaaS are Amazon EC2 [8], S3 [9], vCloud etc [10].

ii. Platform as a Service (PaaS)

PaaS provides a platform for the IT resources to be used by the users. PaaS works similarly as an Operating System. OS work as an intermediate level between system hardware and software, likewise PaaS provides platform for the IT resources. Windows Azure, Hadoop, Google AppEngine are the examples of PaaS [11].

iii. Software as a Service (SaaS)

SaaS provides on demand services and applications to the users. Every application is share among all the users over the Internet, whose interaction is isolated from each other. Flickr, Google document are the examples of SaaS [12].

All the different layers are shown in figure 2.

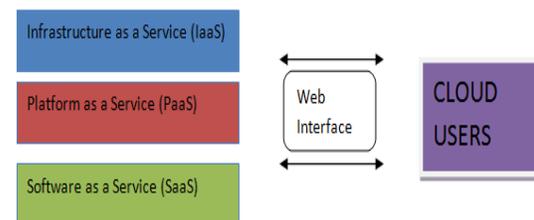


Figure2. MODEL FOR CLOUD COMPUTING

BENEFITS OF CLOUD COMPUTING

Several benefits are there of cloud computing. Some of them are as follows:

i. Reduction of expenses on technology infrastructure

Maintain easy access to your information with minimal spending [1].

ii. Globalization of workforce on cheap

People can use cloud anywhere in the world over the Internet.

iii. Improvement in accessibility

User can have anytime, anywhere accessibility.

iv. Improvement in flexibility

Users and resources can be scaled in and scaled out as per need.

v. Minimization in licensing new software

Without buying expensive software licenses or program user can access them [2].

vi. Less personnel training is needed

It is easy to work on cloud, with less training. Fewer people can do more work on cloud.

vii. Reduction in capital costs

There is no need to spend more money on hardware, software and licensing fees.

APPROACHES TO CLOUD COMPUTING

There are different approaches for the cloud computing. Few of them are:

i. Virtualization

One of the most important approach of the cloud computing. Without virtual machines, cloud services are nowhere [13]. The evolution of cloud computing

depends on three virtual forms, which are Virtual storage, Virtual server and Virtual network [14].

ii. Web services

Service provider use technologies over the Internet. The technologies are XML, SOAP etc. Service Oriented Architecture manages the cloud inside an organization. SOA makes use of multiple services to complete a specific task [15].

iii. Application Programming Interface (API)

All cloud services are depended on APIs. It allows deploying and configuring the cloud services. A cloud service has no existence without APIs.

These are the basic approaches for the cloud computing. The detail discussion is mentioned in [1][13]. Further we are discussing about advantages and challenges of cloud computing.

ADVANTAGES OF CLOUD COMPUTING

The main features of cloud computing are discussed in the above topics [1]. The advantages of using cloud computing services are as follows:

i. Cost savings

The most significant advantages of cloud computing is Cost saving. Without big spend a customer can use the hardware, software, storage and network [16]. There is no spending on infrastructure of the cloud.

ii. Reliability

Service providers assure 24x7x365 availability. Hence if the services are available every time, it increases the reliability of customer to use the cloud service [17].

iii. Manageability

IT infrastructure updates and maintenance are eliminated, as all the resources are maintained and managed by the service provider [18]. So customer can access simple web based user interface for accessing software, applications and services- without installing them. [19].

DISADVANTAGES OF CLOUD COMPUTING

Every advantage has its own disadvantages. Similarly in case of cloud computing which are as follows:

i. Security

The major drawback of cloud computing is Security. In a multi-tenant cloud architecture where multiple users are hosted on the same server, a hacker may try to crack into the data of other users hosted and stored on the server.

ii. Vendor lock-in

Although a customer is free to switch cloud services from one vendor to another, yet organizations find it difficult to migrate from their services.

iii. Limited control

The cloud services, infrastructure and resources are controlled, owned, managed and monitored by the service provider. The customer can only use and control the applications and data operated as a front end, but cannot control the backend infrastructure for itself.

CHALLENGES OF CLOUD COMPUTING

1. Security

The fundamental challenge of any traditional or modern technology is its Security and Privacy [2]. The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. With respect to cloud computing environment, privacy is defined as “the ability of an entity to control what information it reveals about itself to the cloud/cloud Service Provider, and the ability to control who can access that information”.

The other major parts of security are as follows:

i. Confidentiality

It is the process of making sure that the data remains private, confidential and restricted from unauthorized users [21]. Confidentiality means keeping users' data secret in the Cloud systems. Confidentiality has two approaches- physical isolation and encryption. Encrypting a data and putting it on cloud is more confidential than unencrypted data on local data centers. Confidential approach of encrypted data is successfully used by TC3 [22].

ii. Authentication

It is a mechanism where the origin of electronic message of document is correctly identified. It can clearly explain by an example where User1 sends and electronic message to User2. The difficulty is that User1 has posed as User3. Authentication mechanism helps User2 to know that the message was sent by User1 and is posing as User3.

iii. Authorization

It determines the level of access to a particular authenticated user to system resources. The access control determines who should get the access of what [23].

iv. Availability

Availability ensures that the user can use applications and infrastructure anywhere and anytime. A cloud user expect all time service availability with no or minimal downtime. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. Amazon Web Services provide S3, EC2 entirely depend on the virtual machines called Xen [24], and Skytap [25] offers virtual lab management application relaying on hypervisors, including VMware [26], Xen and Microsoft Hyper- V [27], and so on. Virtual machines have the capability for providing on demand services in terms of users' individual resource requirement for a large amount of users.

v. Integrity

Integrity protects the data from malicious modification. If the sender modifies the data after sending, then the receiver on the other side receives an unmodified data i.e. the integrity of message will be lost. Cloud Computing services maintain the integrity as the basic task. Digital signature is generally used for testing integrity in Cloud services. Hashing techniques and message authentication codes are the other way for testing integrity.

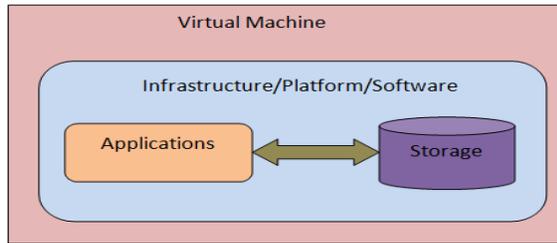


Figure4. Diagram for Virtual Machine

Figure 4 illustrates the functionality of Virtual Machines.

vi. Non Repudiation

Repudiation in networking means the denial of message or data to be participated in all or part of the communication. Non Repudiation is the guarantee that someone cannot deny something. Every message sent to the receiver generates a non repudiation receipt as non repudiation evidence.

vii. Control

Cloud users contribute their individual data to the cloud over the internet and making use of it. Users have no control on the threats that can affect their individual data. For effective control over data access service provider must enhance the safety of the users' data.

Privacy

Privacy along with security is the main challenge of the cloud computing service. User's reliability and legal compliance is the major necessity that has to be counter-checked at every design steps. Cloud services are designed in such a way that the privacy risk decreases and also ensures the legal compliance.

The other major parts of privacy are as follows [28]:

i. Loss of Governance

The cloud users are using the services from different countries and the service provider is located in one country. The user data which is stored by the user belongs to the country and the service provider who is from the different country has the control over the user data and services. In case of misuse, privacy, security and reliability get affected.

ii. Regulatory compliance

Cloud computing makes it harder for enterprises to be sure they are complying with industry and government regulations. The regulated data is on cloud, but regulatory compliance ends with the organization that owns the data.

iii. Lack of transparency

Cloud service providers never reveal that how they are controlling or monitoring their services. The agreement with third party, location of data stored, working of services, information of user data, security measures are not disclosed to users.

Security itself is a major challenge to deal with. Some other security threats are: data loss/ leakage, SQL injection attacks, data combination and commingling, sniffer attack, CAPTCHA breakings etc. which are describe as follows:

❖ **Data loss/ leakage**

Data loss/ leakage are the most challenging threats, which may cause due to how the data is structured. The data of an organization are saved on the server of other places. The duration of data retained by cloud providers, may continue to be stored on the provider's server even if it has been deleted by user [29]. Improper deletion of data records, alteration of data without proper backup may result to data loss.

❖ **SQL injection attacks**

A malicious code is inserted in the standard SQL code after which the attacker gets the unauthorized access to the database and the data [30]. The information entered by the hacker is misunderstood by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to get access and change the working of a website.

❖ **Data combination and commingling**

Cloud computing services are available for all the business user or private client to store their data separately. But when the data is needed to be combined or commingled it is much dangerous. If a client is a victim of an attack, the integrity and availability is affected by the attack to the other user in the same location.

❖ **Sniffer attack**

Sniffer attack captures the packet flowing in the network. If the data is unencrypted it can be read. NIC certified sniffer program ensures recording the data of the system on the network.

2. Performance unpredictability, latency and stanchness

The I/O performance can be improved by the architecture and operating systems to virtualized interrupts and channels. Flash memory is also the alternative way to improve performance. Flash memory saves the data even after power is off. It consumes less energy and gets faster access. Latency [29] is refers as any of several kinds of delays incurred in processing of network data. Low latency network connection is one with small delays. High latency refers to long delay in a connection. Packet loss, congestion and windowing are the other factors of latency. Reliability is the basic necessity of the network. Secure network is more reliable as the data is encrypted and moved around the network to reach the destination.

3. Network accessibility

Frequent availability of network is one of the major challenges in cloud computing. Anywhere and anytime network accessibility are required for users reliability. Network availability is required when a user is moving from one location to another and internet plays an important role in frequent network availability and accessibility.

4. Minimized data latency

Latency is defined in earlier topics. Data latency in cloud computing is not consistent which is responsible for longer latency for data transfer in times. The longer

time intervals observed in case of data transfer and other network related activities because of an increment in number of intermediate components of network.

5. Network monitoring and Scalability

Applications running on mobiles in a cloud computing platform should be intelligent enough to get used to the unreliable network capacities and also these should be accessible through different platforms without suffering any data loss. With applications lying in a cloud, it is possible for the hackers to corrupt an application and gain access to a private data on mobile device while accessing that application. In order to avoid these, strongly recommended regular virus-scanning and original malware protection software need to be installed to avoid any type of virus/malware check into the mobile system [1].

These are the major challenges in cloud computing. Some other challenges are portability and interoperability, data storage over IP networks etc.

III. CONCLUSION

Cloud Computing is the most trending service over the internet. It provides many services that are best to the users and without much training a new user can also take the benefits of these services. In our paper, we describes each and every pros and cons of cloud computing. There are still many other threats that are used to be resolved and make the best out of it to provide better services to the users. This paper will help the researchers to know more about cloud computing, about its challenges and also help for some innovative ideas for the future work.

References

1. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience", 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.
2. Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", International Journal of Emerging Technology and Advanced Engineering: ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, December 2013.
3. Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", *Wirel. Commun. Mob. Comput.* 2013; **13**:1587-1611 DOI:10.1002/wcm.1203
4. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", *Proceedings of Advances in Computing and Communications*, Vol. 193, pp. 445-454, 2011. DOI: 10.1007/978-3-642-22726-4_46
5. Thomas W. Shinder, "Security Issues in Cloud Deployment models", *TechNet Articles*, Wiki, Microsoft, Aug, 2011.
6. Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, "Mobile cloud computing: A survey" *journal homepage*; *Future Generation Computer Systems* 29 (2013) 84-106
7. National Conference on Innovations in Electrical Electronics and Computer Science Engineering, US 2014/0317616 A1, Oct. 23, 2014.
8. Qi Zhang, Lu Cheng, Raouf Boutaba, "Cloud Computing: State of the art and research challenges", *Journal of Internet Services and Applications*, pp. 7- 18, vol. 1, issue. 1, Feb, 2010. DOI: 10.1007/s13174-010-0007-6.
9. David Chappel, "A Short Introduction to Cloud Platforms: An Enterprise Oriented View", David Chappel and Associates, August, 2008. [Sponsored by Microsoft Corporation] Chappell.pdf
10. Amy Shuen, "Web 2.0: A Strategy Guide: Business thinking and strategies behind successful Web 2.0 implementations", O'Reilly Media; 1st edition; Apr 30, 2008; ISBN-13: 978-0596529963.
11. Jain et al., *International Journal of Advanced Research in Computer Science and Software Engineering* 3(7), July - 2013, pp. 966-972
12. R. Buyya, C. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos, CA, USA)*, 2008.
13. Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend", *Intl. Conference on Future Networks*, pp. 93- 97, China, 2010. DOI: 10.1109/ICFN.2010.58
14. Youseff, L; Butrico, M; Da Silva, D., "Toward a Unified Ontology of Cloud Computing", *Grid Computing Environments Workshop*, pp. 1-10, Nov, 2008, Austin, Texas. DOI: 10.1109/GCE.2008.4738443
15. James Governor, "Web 2.0 Architectures: What Entrepreneurs and Information Architects Need to Know by James Governor", May 15, 2009; O'Reilly; ISBN-13: 978-0596514433.
16. Carnegie Mellon, "System of Systems, Barriers to Adoption", [Online]. Available:
17. Antero Taivalsaari, "Mashware: The Future of Web Applications", *Technical Report*, Feb 2009. DOI: 10.1145/1878537.1878703
18. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360 Degree Compared," in *Grid Computing Environments Workshop*, 2008. GCE'08, 2008, pp. 1-10
19. Andrew J. Younge, Gregor von Laszewski, Lizhe Wang, onia Lopez-Alarcon, Warren

- Carithers, "Efficient Resource Management for Cloud Computing Environments".
20. Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation.
 21. Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", IEEE, 2010.
 22. Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010), "Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.
 23. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. *Communications of the ACM, Volume 53 Issue 4*, pages 50-58. April 2010.
 24. Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Conference on Hot Topics in Cloud Computing 2009, pages 1-5, USA.
 25. Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems", International Journal of Grid and Distributed Computing, March, 2010.
 26. Zhimin Yang et al, "A Collaborative Trust Model of Firewall through based on Cloud Computing", 14th International Conference on Computer Supported Cooperative Work in Design, 2010, China.
 27. Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia.
 28. Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. CLOUD '09, Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pages 44-52. May 2009.
 29. Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.
 30. John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again", Tech-world, Feb. 16, 2009.