

Survey Paper on Cloud Computing: Issues, Challenges and Outcomes

Parmeet Singh Saluja
Undergraduate Student

Shri Vaishnav Institute of Technology and Science,
Indore
Madhya Pradesh, India

Upendra Dwivedi
Assistant Professor

Shri Vaishnav Institute of Technology and Science,
Indore
Madhya Pradesh, India

ABSTRACT

Cloud Computing is a term which came into existence in 2007. It refers to applications and services that run on a distributed network using virtual resources and the Internet. It became popular because of the services which are provided by it. Cloud computing uses the technology, services, hardware etc. and turns them into a service and provides them to a user on basis of demand and pay.

In this paper we are analyzing the issues and challenges that are likely to be faced when we implement cloud computing platform. As cloud computing is the new technology the paper describes about it. The paper defines clouds and outlines its characteristics with its architecture and also provides information about various models. The paper majorly tells us about the issues, challenges and outcomes of cloud computing.

General Terms

Cloud Computing, Cloud Security

Keywords

Cloud Computing, Cloud Security, Cloud Portability, Cloud Applications.

1. INTRODUCTION

Cloud computing is a style of computing where virtual resources which are scalable on demand are provided as a service. Cloud computing provides services for a single person or for an organization. American National Institute of Standards & Technology (NIST) proposed definition of this revolutionary technology: [5]

“Cloud computing is a transparent model for providing flexible, scalable, on-demand network access to a pool of computing resources that can be rapidly shared, monitored and released with less effort and”.

Cloud is based on distributed systems. The user does not require any prerequisite knowledge to control the infrastructure of clouds that is it provides abstraction. Cloud Computing provides services using the internet with scalability, high computing power, good quality of service and high throughput. Cloud computing providers deliver common applications and services which are accessed from internet through a software like web browser [1].

The cloud is the service delivery vehicle and has improvised many practices by making resources as a service. Cloud Computing faces issues which are to be improvised by the time like the security of the data and privacy of cloud owner. It has become important to secure the data by properly

storing, managing and analyzing. Thus to use cloud computing in full form we have rely on the cloud service provider and thus data security has to be ensured.

2. LITERATURE SURVEY

Cloud Computing possess numerous characteristics and some of them are- Shared Infrastructure and Resources which uses a virtualization based software model, enabling the sharing of storage devices, and networking capabilities and other resources. Virtualization here helps us by hiding the place where the actual data is stored. Virtualization technology is used for providing the standard applications to the user. Virtualization in cloud reduces the load of cloud users and cloud providers as virtualized resources are maintained by third-party people. Dynamic Scaling a characteristic of cloud in which services are provided seeing current demands. The scalability of cloud computing is the flexibility which is provided by the service provider to user. This is done automatically by software automation that is by enabling the expansion and contraction of service when needed and without any interruption in services. This dynamic scaling is done while maintaining high levels of reliability and security. Pay-as-you-go another characteristics of cloud computing means cloud computing services have the capability of metering and thus controls and optimize resource use. Cloud Computing provides transparency between the service provider and clients by monitoring resource usage [2]. Broad Network Access helps in delivering cloud computing services on the network. It also helps clients with different platforms situated at consumer sites in using services with the help of the network.

Cloud Computing builds on architecture which is composed of different layers. In linear layer architecture of cloud there are generally four layers: Hardware Layer, Infrastructure Layer, Platform Layer and Application Layer. Hardware Layer is a layer which is responsible for managing the physical resources like servers, routers, switches etc. of the cloud. This layer is implemented in the data center. A data center usually contains a large number of servers which are organized in racks and connected to each other using switches, routers or other devices. Hardware layer faces some issues which include hardware configuration, traffic management, power management, fault tolerance and cooling resource management. Infrastructure Layer is a layer which is responsible for creating computing resources using technologies based on virtualization such as KVM [12], VMware [13] and etc. by partitioning the physical resources. The infrastructure layer is an important layer of cloud computing as it provides features like dynamic resource assignment through virtualization technologies. Platform

Layer is a layer which is built on infrastructure layer. It consists of application frameworks and operating systems. It minimizes the burden of deploying applications. For example, Google App Engine [10] provides support for implementing storage, database and business logic and analytics for web applications. Application Layer is a layer which consists of the actual cloud applications. Cloud applications are different from traditional applications as they can utilize the automatic scaling feature to achieve better performance and availability at lower operating cost.

Cloud in cloud computing can be deployed in various ways on the basis of different levels of security and management required in them. Private Cloud is a model of cloud computing which includes the secure cloud-based environment and in which only specified client can operate. Private cloud like other clouds will provide high computing power as a service with virtualized environment but the cloud is accessible only to the authorized single organization with high security and privacy. In the private cloud, there is no other security rules, legal information, or bandwidth limitation which are usually present in Public Cloud. By using Private Cloud, the user gets benefitted as they have optimized control of infrastructure and high security. One of the best examples of a private cloud is Eucalyptus Systems [4]. Public Cloud is the most known model of Cloud Computing to users under which users are provided computing power as a service with a virtualized environment and shareable resources with a benefit over private cloud by making it accessible openly over the public network like the internet. It provides service to multiple clients using same shared infrastructure. These clouds are fully hosted and managed by the cloud service provider and have some responsibilities like installation, management, scalability, and maintenance of cloud. Chances of underutilization are removed as a user are charged for only the amount they have used. Processes which require powerful security are not always appropriate for public clouds as a customer has low control over the resources. Public Cloud has no provision of Access Restriction or Authorization but Public cloud providers like Google or Amazon offer an access control to their clients. Examples of public cloud are Microsoft Azure [14], Google App Engine [11]. Hybrid Cloud is a model of Cloud Computing which consists of both Private and Public Cloud. Organization can use Public Cloud services for all areas where high security is not a prime concern and use Private Cloud services for only high-security areas thus using Hybrid Cloud. In this model, a company can outline the goals and needs of services [6]. The major drawback lies here in integrating Private and Public services as a single loophole will breach security through the public cloud. An example of Hybrid Cloud is Amazon Web Services (AWS) [9].

Cloud Computing is well known for its services and on the basis of its services there are three types of cloud computing models: Software as a Service(SaaS), Platform as a Service(PaaS), and Infrastructure as a Service(IaaS). In Software as a Service the service provider of cloud put their applications on a hosting environment which is accessed through the network by various authorized people. Here the service provider has no control over the infrastructure of the cloud. The application is delivered as a service to the user. Different service provider's applications are combined together in a single environment (Software as a Service) so that there is optimized speed, accuracy, security, failure recovery, maintenance. Examples of SaaS are Salesforce.com [14], Google mail, Google docs. In Platform as Service the service provider of cloud provides a development platform

which supports software development life cycle and which helps clients to develop a cloud application and services using Software as a Service without the cumbersome of maintenance. It provides a platform for provisioning and developing the software. Complexity is removed and flexibility is ensured which helps the application to be deployed quickly. The difference between SaaS and PaaS is that SaaS only hosts applications on cloud whereas PaaS provides development platform which can host application which is in-progress or completed. Examples of PaaS are Google App Engine [11], Microsoft's Azure [15], Salesforce.com [14] etc. In Infrastructure as a Service the service provider of cloud provides with hardware infrastructure and services (processing, storage, networks and other fundamental computing resources) to the clients. Here storage services and virtual servers are also provided to users. Virtualization is the technique which is used to integrate or decompose resources with respect to increasing or decreasing demands. This service manages applications, data operating systems, runtime etc. Examples of IaaS are Amazons EC2[8], Amazon S3, and Flexiscale [10].

Each service and deployment model of cloud has different requirement of privacy, security and maintenance for a proper functionality. Thus it makes the process more complex and tangled for the cloud service provider and increases the need of high security. Cloud Computing has brought some positive changes in the field of computing but also has some issues which are to be addressed like security, reliability, and performance etc.

3. CLOUD COMPUTING: ISSUES, CHALLENGES AND OUTCOMES

With the growing popularity, users and service providers of cloud computing there is also increase in data stored in cloud. As data increases challenges also increases to make the data secure [3]. Cloud Computing has various challenges and issues attached with it. Some of them are-

Security and Privacy- The main challenge to cloud computing is that how security and privacy are maintained as the data and information of a company is stored outside of its firewalls. Some of the security risks are Data loss and leakage, Malicious insider, Flood Attack, IP Spoofing, DDOS attack and etc. These risks can be lessened by using security applications, encryption, security hardware etc.

Service Billing- Another major concern is Service Billing as on demand nature of cloud exits so it becomes difficult to find exact amount for definite utilization.

Computing Performance and Cost- Sometimes it happens that more money is spent on bandwidth than that spent on hardware cost as high bandwidth is the requirement of the cloud and if we there is low bandwidth then we have to compromise with computing performance.

Portability- With the increase in a number of vendor and services has created a challenge that data can be easily moved between one vendor to another or from public to private environments.

Reliability- With the increase of client, the robustness of cloud is the important factor which makes it more reliable.

Cloud Security is the major concern which increases the computing performance, reliability and portability. Cloud Security can be ensured by providing secure access, backups, data integrity and encryption of data. Secure access can be

ensured by giving proper username and strong password and making sure that the internet connection which the user is using is secured with the latest browser. To avoid the chances of data loss we have to maintain a proper backup of data at proper frequency thus proper mechanism should be provided for it. Automatic data restoration is provided by services like Amazon S3, Amazon Dynamo DB [6]. To maintain proper data integrity, it is required that we monitor the changes in data as well as the resources we are using so that we can avoid vulnerability. Data encryption means providing data protection. Encryption is required before moving the data in cloud [7]. Encryption of data will make accessing of data difficult for unauthorized user.

4. CONCLUSION

In this paper, we have discussed various aspects of cloud computing which profoundly tells us about the topic and gives us a clear view. As cloud computing has evolved recently and is shifting the way of computation from the traditional approach to cloud-based approach by benefiting users by providing them services on demand and on pay per use basis. As cloud computing is enhancing more and more it brings with it many issues and challenges which include various security threads. Cloud computing has necessary potential to withstand these challenges and issues and become a leader in resource sharing technologies.

5. 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] Greg Goth, "Software-as-a-Service: The Spark That Will Change Software Engineering?", IEEE, vol. 9, no. 7, 1541-4922 © 2008.
- [3] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
- [4] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.
- [5] A view of cloud computing: M Armbrust, A Fox, R Griffith, AD Joseph 2010
- [6] Jinesh varia," AWS Cloud Security Best Practices", "White Paper", November 2013 Jinesh varia," AWS Cloud Security Best Practices", "White Paper", November 2013
- [7] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", "International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)", Volume2, Issue 7, July 2013
- [8] Amazon Elastic Computing Cloud, aws.amazon.com/ec2
- [9] Amazon Web Services, aws.amazon.com
- [10] FlexiScale Cloud Computing and Hosting www.flexiscale.com
- [11] Google App Engine, <http://code.google.com/appengine>
- [12] Kernal Based VirtualMachine, www.linux-kvm.org/page/MainPage
- [13] VMWare ESX Server, www.vmware.com/products/esx
- [14] Salesforce CRM, <http://www.salesforce.com/platform>
- [15] WindowsAzure, www.microsoft.com/azure