Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Computing Cloud

Surbhi Dodiya, Prof. Alpesh Patanwadia

Computer Science Engineering, S.L.T.I.E.T, Computer Science Engineering, S.L.T.I.E.T

Abstract — Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected cloud

Keywords: Cloud issues, Virtual machine layer, Data issues, Security issues

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Over the last few years, cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its users and providers [23]. The advantages of using cloud computing include:

- Reduced hardware and maintenance cost,
- Accessibility around the globe, and
- Flexibility and highly automated processes wherein the customer need not worry about mundane concerns like software up-gradation.

Cloud Computing is an emerging trend to deploy and maintain software and is being adopted by the industry such as Google, IBM, Microsoft, and Amazon. Several prototype applications and platforms, such as the IBM ―Blue Cloud infrastructure, the Google App Engine, the Amazon Cloud, and the Elastic Computing

Platform .Cloud Computing is perceived as the next progression that will impact organizational businesses and how they manage their IT infrastructures. The technology and architecture that cloud service and deployment models offer are a key area of research.

Even though there are numerous variations on the definition of Cloud Computing, some basic principles characterize this emerging computing paradigm. Cloud Computing provides technological capabilities—generally maintained off premises— that are delivered on demand as a service via the Internet. Given that a third party owns and manages public cloud services, consumers of these services do not possess resources in the cloud model but pay for them on a per-use basis. Thus virtualization of the resources is the key concept. In the real scenario, they are renting the physical infrastructure, platforms and applications within a shared architecture. Cloud offerings can vary from virtual infrastructure, computing platforms, centralized data centers to end-user Web-Services and Web applications to enormous other focused computing services.

Cloud Computing may be applied to solve problems in many domains of Information Technology like GIS (Geographical Information Systems), Scientific Research, e-Governance Systems, Decision Support Systems , ERP , Web Application Development , Mobile Technology etc.

II. TYPES OF CLOUD DEVELOPMENT

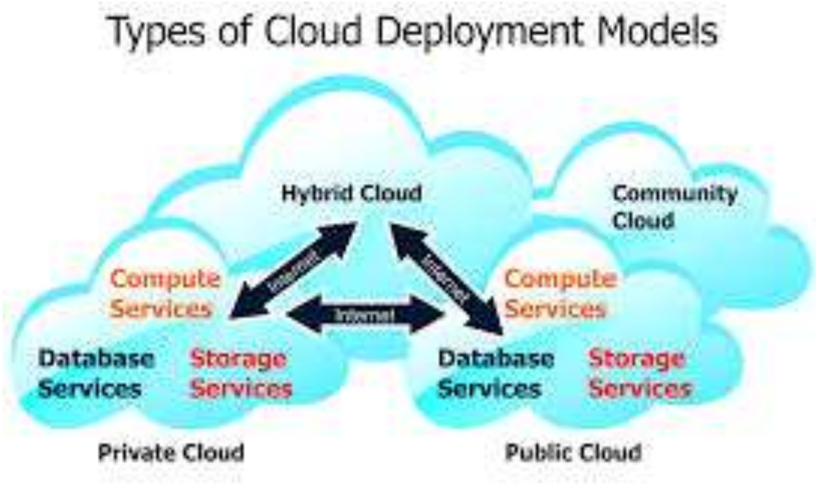

Figure 1: Types of Cloud Deployment Models

2.1 Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities

2.2 Public cloud

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private

Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

III. CLOUD COMPUTING BASIC OVERVIEW

3.1. Cloud Computing - Overview

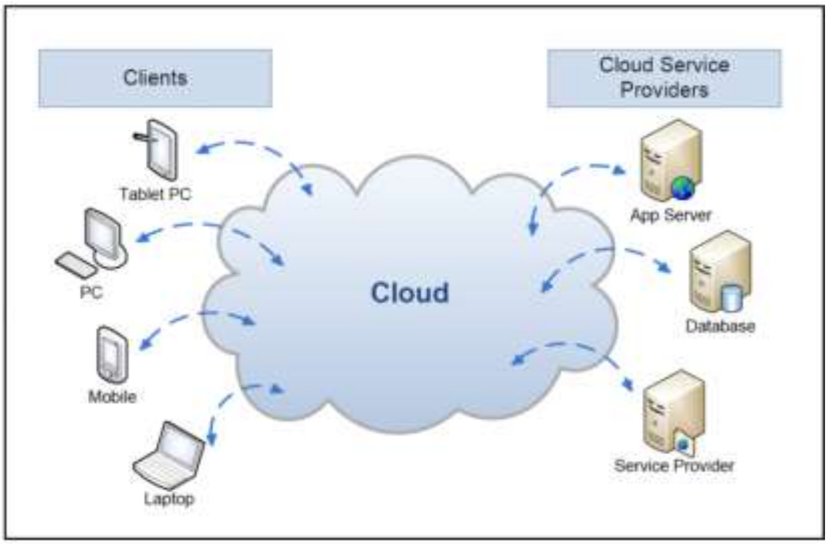

Figure 2: Cloud Computing - Overview

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud. There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Private cloud provides better control and more flexibility. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries. The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy. This paper firstly lists the parameters that affect the security of the cloud in section 2. Section 3 explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues. Section 4 discuses some of tips and tricks to tackle these issues.

3.2 Parameters affecting cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

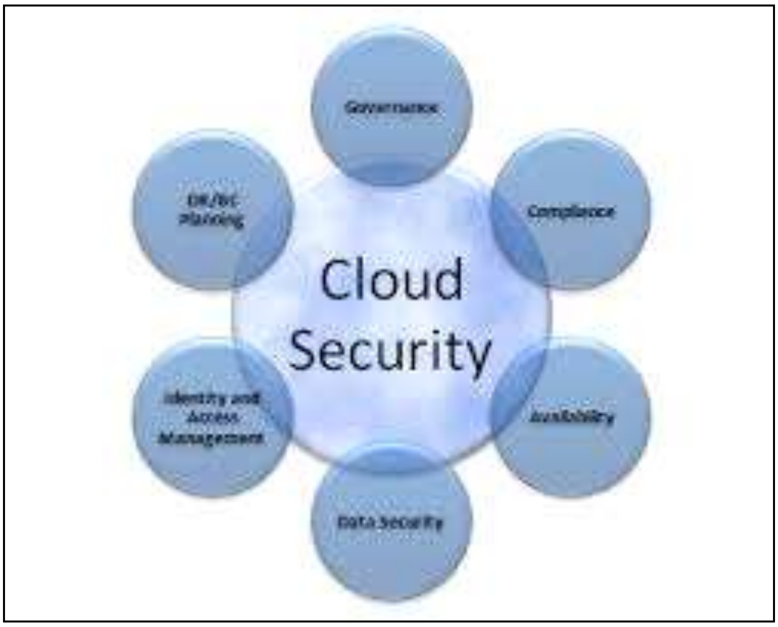

Figure 3: Parameter that affects cloud security

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

3.3 Security Issues faced by Cloud computing

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud.

- Data Issues
- Privacy issues
- Infected Application
- Security issues

IV. CLOUD SECURITY ISSUE

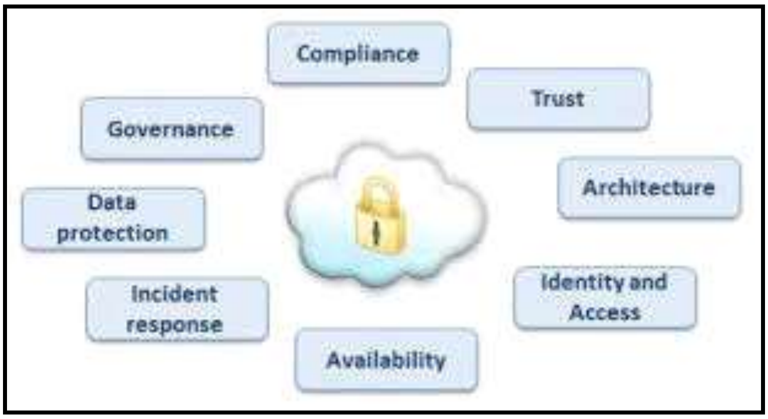

Figure 4: Cloud Security Issues

4.1 Data Issues: sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data

4.2 Secrecy Issues: The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer’s personal information.

4.3 Infected Application: cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

4.4 Security issues: cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

V. CONCLUSION

Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest gaps between cloud-security practice and cloud-security research theory lies in the fact that the assumptions in the research leave out some very important differences between actual cloud security and virtual machine security.

REFERENCES

[1] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM- Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[2] Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST, Germany.

[3] Tackle your client’s security issues with cloud computing in 10 steps.