© 2018 IJSRST | Volume 4 | Issue6 |Print ISSN: 2395-6011 | Online ISSN: 2395-602X

National Conference on Smart Computation and Technology in Conjunction with The Smart City Convergence 2018

A Review on Cloud Computing and its Security Issues

Akshat Rajpurohit*, Akshat Jain, Manish Sharma

Department of Computer Engineering, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India

ABSTRACT

Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. For the sharing resources that contains software, applications, infrastructures and business processes, cloud computing is the main key. Cloud computing is a significant advancement in the delivery of information technology and services. Cloud computing offers compelling advantages in cost, speed, and efficiency. Cloud computing has recently reached popularity and developed into a major trend in IT. This paper focuses on the deployment model of cloud which consists of private cloud, public cloud, hybrid cloud, community cloud .This paper also focuses on architectural components of cloud which consists of Saas, Paas, Iaas. This paper also focuses on security issues and security challenges.

Keywords: Cloud Computing, virtualization, deployment, architectural

I. INTRODUCTION

In Cloud Computing the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as Servers, storage and applications — are delivered to an organization's computers and devices through the Internet .Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually Cloud Computing services are delivered by a third party provider who owns the infrastructure [1].The exponential growth in the volume of data and information lead to problems in management, controlling effective and high costs of storage operation, where organizations are having problems: data retrieval and preparation and backups, and other acts of data. Therefore seeking companies and business organizations at the present time to achieve the highest return on their investments in technology through the planning and implementation of virtualization technologies and cloud computing, in order to protect data and manage more effectively and efficiently [2].

II. DEPLOYMENT MODEL OF CLOUD

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted. The Cloud Computing model has four main deployment models which are:

A. Private Cloud:

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the

organization itself, similar to Intranet functionality. In addition, private cloud offers hosted services to a limited number of people behind a firewall, so it minimizes the security concerns some organizations have around cloud. Private cloud also gives companies direct control over their data. In addition, private cloud offers hosted services to a limited number of people behind a firewall, so it minimizes the security concerns some organizations have around cloud. Private cloud also gives companies direct control over their data [3]

B. Public Cloud:

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. Examples of a public cloud include Microsoft Azure, Google App Engine. The public model offers the following features and benefits:

- Ultimate scalability: cloud resources are available on demand from the public clouds' vast pools of resource so that the applications that run on them can respond seamlessly to fluctuations in activity
- Cost effective: public clouds bring together greater levels of resource and so can benefit from the largest economies of scale.
- Reliability: the sheer number of servers and networks involved in creating a public cloud and the redundancy configurations mean that should one physical component fail, the cloud service would still run unaffected on the remaining components.
- Flexibility: there are a myriad of IaaS, PaaS and SaaS services available on the marke which follow the public cloud model and that are ready to be accessed as a service from any internet enabled device.

C. Hybrid Cloud:

Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and public cloud services with orchestration between the two platforms [5].

A cloud that is setup using a mixture of the above three deployment models each cloud in a hybrid cloud could be independently managed but applications and data would be allowed to move across the hybrid cloud. Hybrid clouds allow cloud bursting to take place, which is where a private cloud can burst-out to a public cloud when it requires more resources.

D. Community Cloud:

A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.) whether managed internally or by a third-party and hosted internally or externally .

This is controlled and used by a group of organizations that have shared interest. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook [6]

III. ARCHITECTURAL COMPONENTS OF CLOUD

According to the different types of services offered, cloud computing can be considered to consist of three layers: software as a service (SAAS), platform as a Service (PAAS), and infrastructure as a Service (IAAS). Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service. Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand.Cloud service models are commonly divided into SaaS, PaaS, and IaaS that exhibited by a given cloud infrastructure.

A. Software as a Service (SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients (e.g. Web browser, PDA, etc.) by application users. Cloud consumers do not have control over the cloud infrastructure that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth[7].

B. Platform as a Service (PaaS) :

This is where applications are developed using a set of programming languages and tools that are supported by the PaaS provider. PaaS provides users with a high level of abstraction that allows them to focus on developing their applications and not worry about the underlying infrastructure. Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine5 and Microsoft Azure6 are popular PaaS examples[8].

Author affiliation must be in 10 pt Italic. Email address must be in 9 pt Courier Regular font.

C. Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

IV. ARCHITECTURAL COMPONENTS OF CLOUD

There are some key security challenges which are:

Authentication: Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have interchangeability administration entity.

Access Control: To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA).

Policy Integration: There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their

policies because they user their own policies and approaches.

Service Management: In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procure divider to get the easiest localized services.

Trust Management: The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider[10].

V. SECURITY IN CLOUD

Based on the investigation security and privacy concerns provided by companies nowadays are not adequate, and consequently result in a big obstacle for users to adapt into the cloud computing systems. Hence, more concerns on security issues, such as availability, confidentiality, data integrity, control, audit and so on, should be taken into account.

Top seven security issues in cloud computing environment as discovered by "Cloud Security Alliance" CSA are:

- ✓ Misuse and reprehensible Use of Cloud Computing.
- ✓ Insecure API.
- ✓ Wicked Insiders.
- ✓ Shared Technology issues/multi-tenancy nature.
- ✓ Data Crash.
- ✓ Account, Service & Traffic Hijacking.
- ✓ Unidentified Risk report.

Misuse and reprehensible Use of Cloud Computing :Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password.

Insecure Application Programming Interfaces (API): Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks.

Wicked Insiders: Malicious insiders create a larger threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets.

Shared Technology issues/multi-tenancy nature: This is based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture.

Data Crash: Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data.

Account, Service & Traffic hijacking: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [11].

VI. CONCLUSION

This paper discussed the deployment model and architectural component of cloud computing. It also addressed challenges and issues of cloud computing in detail. In spite of the several limitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises. Cloud Computing initiatives

could affect the enterprises within two to three years as it has the potential to significantly change IT.

VII. REFRENCES

[1] Mohsin Nazir," Cloud Computing: Overview & Current Research Challenges", IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1 (Nov. - Dec. 2012)

[2] Mohmed Sirelkhtem Adrees1 , Majzoob Kamal Aldein Omer2 and Osama E. Sheta3," Cloud Computing Architecture For Higher Education In The Third World Countries (Republic Of The Sudan As Model)" International Journal of Database Management Systems (IJDMS) Vol.7, No.3, June 2015

[3] http://searchcloudcomputing.techtarget.com/definition/private-cloud

[4] http://www.interoute.com/cloud-article/what-public-cloud

[5] Mohmed Sirelkhtem Adrees1 , Majzoob Kamal Aldein Omer2 and Osama E. Sheta3," Cloud Computing Architecture For Higher Education In The Third World Countries (Republic Of The Sudan As Model)", International Journal of Database Management Systems (IJDMS) Vol.7, No.3, June 2015.

[6] https://en.wikipedia.org/wiki/Community_cloud

[7] Mohsin Nazir," Cloud Computing: Overview & Current Research Challenges", IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1 (Nov. - Dec. 2012), PP 14-22

[8] Ilango Sriram ,Ali Khajeh-Hosseini ," Research Agenda in Cloud Technologies",

[9] Santosh Kumar, R.H Goudar," Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

[10] Manpreet Kaur, Hardeep Singh," a review of cloud computing security issues", International Journal of Advances in Engineering & Technology, June, 2015.

[11] Varsha ,"Study of Security Issues in Cloud Computing", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 6, June 2015, pg.230 – 234.