Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Exploring cloud computing and identification of its security issues

Jyoti Kataria
Amity University
India.

Neetika Gupta
Amity University
India.

Abstract— Cloud computing is now a new emerging catchphrase which provide services to the customer over the internet. Now it is the future of the internet where you can pay according to usage. It is one of the productive grounds which is attracting many global investments. Cloud computing is providing a business model to the organizations so that they can have IT services without any upfront investment. Cloud computing offers remarkable benefits for the organizations. However, there are some issues also, one of the main issue is security which is becoming a competitive edge between so many cloud service providers. This paper focuses on delivery services, deployment models and also about security and data relocation issues in new era of cloud computing.

Keywords— cloud computing, security, issue, Internet based services, cloud computing models.

I. INTRODUCTION

Cloud computing is a new era of computing, as defined by the National Institute of Standards (NIST) [1, 2] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, services, networks and applications). Cloud computing is a method through which capacity can be increased and new capabilities can be added without any investment in new licensing software, infrastructure. It comes as a boosting power for keeping IT budgets under control. There are many cloud computing providers such as Google, Amazon, Microsoft, Yahoo etc. [3]. Cloud computing is composed of: 1)Three essential characteristics (On-demand service, Resource pooling, Broad network access), 2)Three service models (Software as a Service - SaaS, Platform as a Service – PaaS, Infrastructure as a Service – IaaS), 3) Four deployment models (Public cloud, Private cloud, Community cloud, Hybrid cloud) [4]. The cloud computing model provides a promise of high IT support with less cost. However, cloud computing model is still having many challenges especially with security. As information security and data location are main points and are also on top in issues of cloud computing [5]. This paper is divided into the following sections. Section II presents three service models of cloud computing. Section III presents four deployment models of cloud computing. Section IV presents the security issues in cloud computing environment. Finally, conclusion and direction for the future work are present in section V.

II. SERVICE MODELS

There are three main services models which are delivering services such as: Infrastructure services, Platform services and Software services.

•Infrastructure as a Service (IaaS): IaaS refers infrastructure IT resources (servers, networking and storage), which can be accessed with the help of service API. This model shows a self-contained IT environment. It runs on a tenant-based model, in which users hires the resources and pay according to the usage.

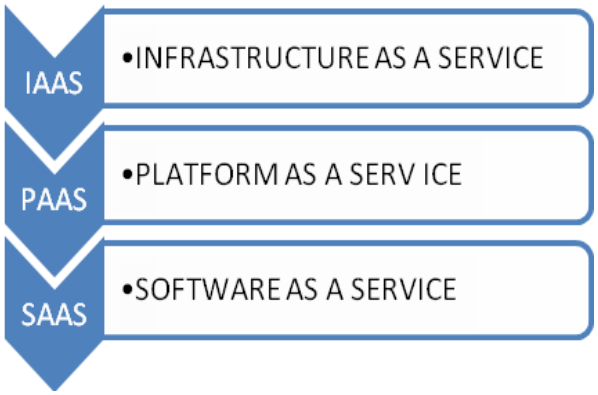

Fig 1: Service models

•Platform as a Service (PaaS): PaaS refers to a set of deployment tools and applications development toolkits (portal servers, middleware and application servers). It gives the flexibility to the client to generate applications on the platform issued by providers. In cloud computing usage of virtual machines acts like catalyst in the PaaS.

•Software as a Service (SaaS): SaaS refers to a software distribution model where applications are managed by provider and then provided to the customer over the internet (e.g., database processing, an email system, payroll processing, human resource management). The SaaS based application architecture is designed to provide services to multi tenancy users at once.

III. CLOUD DEPLOYMENT MODELS

In the deployment model of cloud, storage, platform, software infrastructure and networking are provide as services. There are four types of cloud that are used for different services.

•Public cloud: refers to a network where cloud services are managed and hosted by service providers. Installation, provisioning, management and maintenance are the cloud provider's responsibilities. It is one of the most cost-effective model and is based on pay-per-usage model. The services and resources are openly accessible and available to all [6].

•Private cloud: refers to a set up inside an organization's enterprise data center. In it services are managed either by third party or by tenant organizations [7]. Cost saving is less in private cloud as compared with public cloud but gives more control over resources and data is more secure inside private clouds [8].

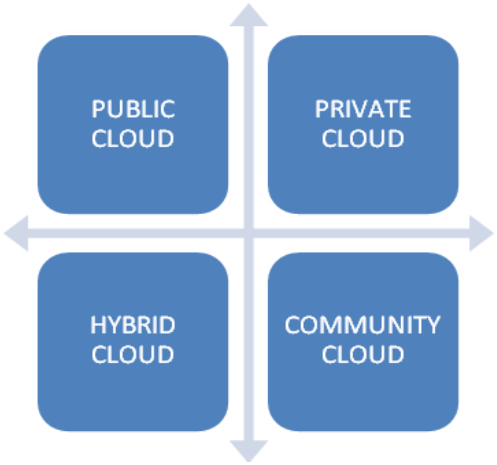

Fig 2: Cloud deployment models

•Hybrid cloud: refers to a combination of any of two or more cloud types. It is a private cloud which is linked with one or more other cloud services [9]. It gives more secure control over the data and also allows other parties to access data.

•Community cloud: refers to semi-private cloud which is used by some defined users. It can be managed by any one of enterprise or organization. It is almost similar to public cloud but access is constrained with some specific cloud users.

IV. SECURITY ISSUES

Security refers to "the combination of confidentiality, the prevention of the unauthorised disclosure of information, integrity, the prevention of the unauthorised amendment or deletion of information, and availability, the prevention of the unauthorised withholding of information" [10]. Services provided by cloud computing platforms, infrastructures and enterprise applications also includes one of the main issue which is data security in context with data availability, data privacy, data transmission, data protection and data location. Some security issues are highlighted below in the following section.

•Data mobility:

In cloud computing, location of data is not fixed at a point and it is also not known by consumers every time. However, whenever any organizations have some sensitive data which is stored in the cloud, they want to know the location of that data. Sometimes cloud providers also use others provider's resources, which increase more security risks. Reasons for using someone else's resources are following as under:

For saving of cost if another provider is having better price policy [11].

Not have enough numbers of resources.

Efficiency of availability of data.

Requirement to change the scale.

Fluctuation in temperature [12].

- Availability and backup of data:

Consumer data is stored in form of slots on different locations or inside different clouds, due to which availability of data becomes a legitimate issue. This issue was also suffered by Gmail service of Google in February 2009 [13]. The process of backup of data becomes more critical in cases of failure when data is hosted remotely. But cloud providers also work out on that but now this backup also becomes a high security issue as it can also be used by someone else without any consent of customer.

- Access of data:

In cloud computing, there is also a risk factor of access of data an unauthorised person due to inadequate. Security measure in the cloud sometimes risk also be by foreign governments. As in some countries government have authority to access anyone's data which is stored in their country and this can also be done without any notification of the customer [14, 15].

- Multi-tenancy:

It is an architectural feature in which single software is deployed on a SaaS provider's server which provides services to multiple numbers of organisations. Resource management and job scheduling is also used by some providers [16], but virtualization is used mostly. Virtual machine behaves like sandbox environment, which remains isolated from others. But these sandbox's boundaries can be jumped by attackers and then they can have full access of the data [17].

- Lack of standardization:

In cloud computing, there is no standardization format used for communication between cloud providers, which creates more difficulties for the user to change a cloud provider. Establishment of security architecture also becomes more difficult for these kind of heterogeneous environments.

- Control over lifecycle of data:

Data is stored in number of chunks and also on many different locations after creation of their replicas. But where customer want to delete some part of it then it should be erased from all of its replicas also. But this act not be proved by any source, it completely relies on the factor of trust. If data is not completely wiped then possibly some other user can recover it.

- Lack of governance in SLA:

User gives the control of data to the cloud provider on many issues, sometimes there are no commitments from the side of cloud e data. This provider in the SLA to provide these services due to which gap generates in the security framework which finally affects security of the data. This can lead to lack of availability, integrity and confidentiality of data.

- Insecure APIs:

To access the services of cloud computing, customers use some set of APIs. Services like management, monitoring and orchestration of the data. If security architecture is not much strong around these APIs then it may expose some sensitive information to malicious users.

V. CONCLUSION

Cloud computing is one of the new emerging technique which is provided on leased basis to the customers and if it issued appropriately then it can help in reducing management responsibilities, costing factor and can increase the efficiency of organisations. But there are some inherent issues also for which cloud providers need to enclose some more safeguards methods as they are holding the data on the behalf of the customers.

In this paper, we mainly focus on the security issues relating to the back-up or availability, access and storage location of the data. Now we are working on finding the solutions of these issues so that assurance can be provided to customers that their data is safe by developing a framework that could resolve these issues.

REFRENCES

[1] David W Cearly, Cloud Computing: Key Initiative Overview, Gartner Report, 2010.
[2] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, 7 Oct 2009.
[3] X. Chu et al., Next-Generation Enterprise Grid Platform for E-science and E-business Applications, Proceedings of the 3rd IEEE International Conference on e-Science and Grid Computing, 2007.
[4] Manish Pokharel, Young Hyun Yoon, Jong Sou Park, Cloud Computing in System Architecture, 2009.

[5] F. Gens., New IDC IT Cloud Services Survey: Top Benefits and Challenges, 2009.
[6] A Platform Computing Whitepaper, Enterprise Cloud Computing: Transforming IT, Platform Computing, pp6, 2010.
[7] Dooley B, Architectural Requirement of The Hybrid Cloud, Information Management Online, 2010.
[8] S. Arnold, Cloud Computing and The Issue of Privacy, K M World, pp14-22, 2009.
[9] Global Netoptex Incorporated, Demystifying The Cloud. Important Opportunities, Crucial Choices, pp 4-14, 2009.
[10] Algirdas A, Jean-Claude L, Brian R, Carl L. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, 2004.
[11] Jaeger, P. T., Grimes, J. M., Lin, J. and Simmons, S, Cloud Computing and Information Policy: Computing in a Policy Cloud?, Journal of Information Technology and Politics, 2008.
[12] Knight, W, Energy-Aware Internet Routing, 2009.
[13] BBC, Google Users Hit by Mail Blackout, BBC News, 2009.
[14] Regulation of Investigatory Powers Act, Part II, s28, UK, 2000.
[15] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Title V, 2001.
[16] Google App Engine. http://code.google.com/appengine.
[17] Kortchinsky, K. , Cloudburst: A VMWare Guest to Host Escape Story, BlackHat, USA, 2009.

