A Comprehensive Study on Architecture, Security issues and Challenges in Cloud Computing

Kishu Gupta
Research Scholar, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119, Haryana
Email: kishugupta2@gmail.com
Ishu Gupta
Research Scholar, Department of Computer Applications, National Institute of Technology, Kurukshetra-136119, Haryana
Email: ishugupta23@gmail.com

Abstract
The emergence of cloud computing promises to have far- reaching effects on the systems and networks. Cloud computing is becoming an increasingly popular enterprise model in which computing resources are made available on-demand to the user as needed. Cloud computing use the internet technologies for delivery of IT-Enabled capabilities 'as a service' to any needed users i.e. through cloud computing we can access anything that we want from anywhere to any computer without worrying about anything like about their storage, cost, management and so on. Many of the features that make cloud computing attractive, have not just challenged to the current security system, but also revealed new securities issues/problems. This paper provides comprehensive study of cloud computing security issues and a brief analysis on the challenges faced by cloud computing.

Keywords – Cloud computing, Iaas, Paas, Saas, Security issue, Challenges.

1. Introduction

In principle, Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction[8]. The core concept of cloud computing is reducing the processing burden on the users' terminal by constantly improving the handling ability of the "cloud, and the powerful computing capacity of the cloud on-demand. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. However, there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing.

2. Cloud Architecture

All 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. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and out sourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. There are two basic cloud models are discussed, first the Cloud service model and the second Cloud Deployment model.

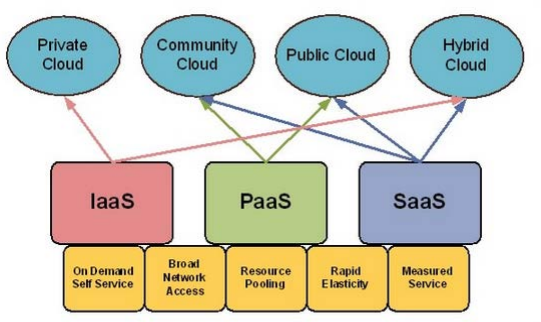

fig 1: cloud architecture based on the system's deployment and service model.

2.1 Cloud Deployment Model

2.1.1 Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

2.1.2 Community cloud
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

2.1.3 Public cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

2.1.4 Hybrid cloud
The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2.2 Cloud Service Model

2.2.1 Infrastructure as a Service (Iaas)
Iaas is the delivery of computer resources (servers, networking technology, storage, and security) as a service. It may also include the delivery of operating systems and virtualization technology to manage the resources. E.g. Amazon EC2 and Google compute engine etc.

2.2.2 Platform as a Service (Paas)
Paas includes the delivery of more than just infrastructure. It delivers an integrated set of software that provides everything a developer needs to build an application — for both software development and runtime. E.g. Google App engine, force.com etc.

2.2.3 Software as a Service (Saas)
Saas provides access to application software often referred to as on-demand software. We don't have to worry about the installation, setup and running of the application. Service provider will do that for you. E.g. Gmail, Face book etc.

2.3 Layered Architecture

2.3.1 Application Layer
Highest layer of the cloud, where request for services and resources push to the data centers. Here client use computing and perform his task which is possible by using application on cloud.

2.3.2 Platform Layer
This layer consists of operating system, application software and frameworks. The main aim of platform layer is to reduce the efforts for execution of application directly to the virtual machine. Therefore an application interfaces are used at this layer.

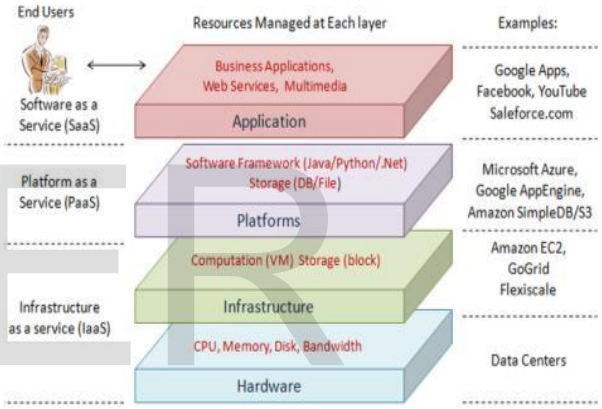

fig 2: layered architecture of cloud service model.

2.3.3 Infrastructure Layer
The resource virtualization creates on an infrastructure layer by dividing the physical resources using virtualization tools like VMware, Xen. The dynamic resource and service allocation is also done at this layer. Thus it can be say that infrastructure layer is very important part of cloud computing.

2.3.4 The hardware layer
This layer is responsible for arranging the physical resources of the cloud which have physical servers, routers, switches, power and cooling systems. The hardware layer is mostly applied in data centers.

3. Cloud Computing Security Issues
In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. But as more and more information on individuals

and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

3.1 Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

3.2 Privacy

Different from the traditional computing model, cloud Computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

3.3 Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

3.4 Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them limitations can be overcome by use of Defense-in-depth approach. Defense-in-depth approach against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring.

3.5 Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says.

4. Cloud Computing Challenges

4.1 Availability and Performance

While vital applications and infrastructure for an organization is an ever required necessity, cloud providers need to address the issues related to availability and performance. One way to achieve these metrics is by defining and adopting a well formed Service Level Agreement (SLA). It acts as a trust relationship between the provider and the customer (any organization in this case) to have a minimum set bar on the time during which the applications and/or infrastructure may not be available.

4.2 Malicious Insiders

How an organization can restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network, where a soft target exists.

4.3 Outside attacks

While insider threats pose a great threat to the Cloud
provider and their customers alike, the threats evolving from outside pose an even greater impact, not in terms of the damage done directly to the system or processes however, the damage done to the reputation and long term loss of leaving customers.

4.4 Mutlitenancy

Multi tenancy implies sharing of computational resources with other tenants residing on the same physical or logical platform at provider's site. Conflict arises because Tenants share a pool of resources and have opposing goals. The application and hardware sharing can enable information leakage and exploitation. These involves defending the cloud virtual infrastructure at different layers with different protection

mechanisms, as per the layer requirement and according to the layer characteristics. Applying such a defense strategy ensures that threats have to bypass by more than one defense layer, which in turn gives a degree of assurance that hackers have to do much more work than they anticipate and most of them, if not all will leave the attack mid way.

4.5 Loss of Control

Losing control over vital data and critical services can be both disturbing and disrupting for any institution. While this is a reality in the Cloud world, the effect can be minimized by working out a strategy to cope with data integrity and authentication mechanisms, between provider and end user. The organizations must understand cloud provider security policies so that, they can point out anything which is not at par with their internal security policies or processes and fix the same before migrating anything vital to the Cloud.

5. Conclusion

In this paper, we discuss about cloud Computing. Describe its definition and some existing issues. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on. But when security & privacy comes into existence then so many challenges and issues appeared according to hackers and security researcher's suggestion that cloud computing is not hundred percent safe due to information can be leak at any level of cloud. So this paper tries to analyze various challenges and issues related to the security of a cloud and need to work on those issues to protect manipulation of information.

References

[1] Barr Randolph, Qualys Inc, "*How to gain comfort in losing control to the cloud*".

[2] Behl Akhil, "*Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation*".

[3] Gartner. "*Seven cloud-computing security risks*". http://www.infoworld.com July 02,2008.

[4] Grover Jitender, "*Cloud Computing and Its Security Issues – A Review*", IEEE – 33044

[5] Jack Schofield. Wednesday 17 June 2009 22.00BST,http://www.guardian.co.uk/technology/2009/jun/17/cloud-computingjack-schofield.

[6] Jiang Jianchun, Weiping Wen, "*Information security issues in cloud computing environment*",Netinfo Security,doi:10.3969/j.issn.1671122.2010.02.026.

[7] Maggiani Rich, solari communication. "*Cloud computing is changing how we communicate*".

[8] Mell P., T Grance, The NlST Definition of Cloud Computing, Vol 15, 2009. http://csrc.nist.gov/groups/SNS/cloudcomputing.

[9] Mills Elinor, January 27,2009. "*Cloud computing security forecast: clear skies*".

[10] Puthal Deepak, "*Cloud Computing Features, Issues and Challenges:A Big Picture*", 2015 International Conference on Computational Intelligence & Networks.

[11] Shaikh Farhan Bashir, "*Security Threats in Cloud Computing*", 6th International Conference Internet Technology and Secured Transactions.

[12] V. Nandgaonkar Suruchee, "*A Comprehensive Study on Cloud Computing*", IJCSMC, Vol. 3, Issue. 4, April 2014, pg.733 – 738, ISSN 2320–088X.

[13] Wang Zhijun, Zhang Ni, "*A Survey on Cloud Computing Security*", 2012 IEEE International Conference on Oxide Materials for Electronic Engineering (OMEE).