Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques

Loganayagi.B, S.Sujatha, a*

a*Anna University of Technology, Tiruchirappalli, India

Abstract

Cloud Computing is accessing Services through Internet based on pay per usage model. Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are available in Cloud. Cloud based products will eliminate the need to install and manage client rich applications. Cloud Service providers are helping companies to reduce the high cost infrastructure installation and maintenance cost. The customer is charged only for the resources consumed like utility based computing. Data is a more valuable Asset. In business making decision is important from the data what is available. Security is one of the major problem of Cloud, where data can be stored anywhere, any part of the cloud. This paper gives details about the challenges and issues of Cloud Computing and solution to overcome those issues

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of ICCTSD 2011

Keywords: Cloud Computing; IaaS; PaaS; SaaS; Policy Monitoring; VM.

1. Introduction

Cloud Computing is defined by a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.[1]

Cloud is providing preconfigured infrastructure at lower cost, which generally follows the Information Technology Infrastructure Library, can manage increased peak load capacity and moreover uses the latest technology, provide consistent performance that is monitored by the service provider. Dynamic allocation of the resources as and when is needed.
Cloud computing reduces capital expenditure (CAPEX) and it offers high computing at lower cost. Upgrading your hardware/software requirement also easy with the cloud, without disturbing the current work. Scalability and maintenance is easy in the case of cloud. Easily user can rent/lease the services offered by cloud computing vendors. User will be charged as pay per usage like utility based services. It is easy to scale if the application is deployed in cloud. It takes away all the risks of managing resources [18]

Overall Cloud is giving good performance at lower cost instead of making more capital investment. Apart from IaaS, SaaS, PaaS, XaaS is possible in case of cloud. Users will be charged based on utility computing. Cloud adopts as pay per usage model. Besides having enormous good features like performance, scalability, flexibility, adoptability, cloud has some serious like security, availability, etc. The rest of the paper is organized as follows: Section 2 discusses about the Cloud providers, Section 3 discusses about the Cloud Computing Challenges and Issues, Section 4 discusses about Proposed Method and Section 5 discusses about the Conclusion.

2. Cloud Providers

Cloud computing [2] [7] [8] [14] [15] systems generally falls into three course grain categories. Infrastructure as a service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). Many companies are offering services.

2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) provisions hardware, software, and equipments to deliver software application environments with a resource usage-based pricing model. Infrastructure can scale up and down dynamically based on application resource needs.

Typical examples are Amazon EC2 (Elastic Cloud Computing) Service and S3 (Simple Storage Service) where compute and storage infrastructures are open to public access with a utility pricing model. This basically delivers virtual machine images to the IaaS provider, instead of programs, and the Machine can contain whatever the developer want.

Example:
- Full virtualization (GoGrid, Skytap), Grid computing (Sun Grid), Management (RightScale), Paravirtualization (Amazon Elastic Compute Cloud)

2.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) offers a high-level integrated environment to build, test, and deploy custom applications. Generally, developers will need to accept some restrictions on the type of software they can write in exchange for built-in application scalability.

An example is Google’s App Engine, which enables users to build Web applications on the same scalable systems that power Google applications, Web application frameworks, Python Django (Google App Engine), Ruby on Rails (Heroku), Web hosting (Mosso), Proprietary (Azure, Force.com)

2.3 Software as a Service (SaaS)

User buys a Subscription to some software product, but some or all of the data and codes resides remotely. Delivers special-purpose software that is remotely accessible by consumers through the Internet with a usage-based pricing model. In this model, applications could run entirely on the network, with the user interface living on a thin client.

Salesforce is an industry leader in providing online CRM (Customer Relationship Management) Services. Live Mesh from Microsoft allows files and folders to be shared and synchronized across multiple devices.
Identity (OAuth, OpenID), Integration (Amazon Simple Queue Service), Mapping (Google Maps, Yahoo! Maps), Payments (Amazon Flexible Payments Service, Google Checkout, PayPal), Search (Alexa, Google Custom Search, Yahoo! BOSS), Others (Amazon Mechanical Turk)

Other than the listed above companies, many companies started offering cloud computing services.

3 Cloud Computing Challenges and Issues

Cloud security is one of the major issue. In general Security means, focus will be giving attention on confidentiality, Integrity, Availability. But will that be sufficient? Cloud Computing is providing services such as Infrastructure as a Service, Platform as a Service, Software as a Service, or Anything as a Service through internet based as pay per usage model like utility computing.

In cloud, data can be stored anywhere. User no need to know exactly, from where they are accessing the service. But security and privacy concerns of cloud need that whether it is coming under regulatory compliance and not violating any user’s privacy.

![Cloud Challenges/Issues by IDC Survey](image)

The fig.1 shows the cloud challenges/issues, a survey taken by IDC in Aug 2008. Besides having nice features like Scalability, Availability, Performance, Cost-effective, Acquire resources on demand, Release resources when no longer needed, Pay for what you use, Leverage other’s core competencies, Turn fixed cost into variable cost, security is the major issue.

There are wide range of standards and organization working on security. Some of the Organizations and their core areas are listed below.

a. Cloud Security Alliance (CSA): CSA [12] gave a list of top threats to cloud computing such as Abuse and Nefarious Use of Cloud Computing, Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking, Unknown Risk Profile and they suggested tackling methods such as tools to monitor the IP, APIs, encryption, firewalls along with strong authentication.

b. ISO 27001-27006 series: Objective of ISO [19] itself, “provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System”. So it is having its own impact of applicability of these standards towards in the area of cloud security.
c. European Network and Information Security Agency (ENISA) [13]: It is an EU agency suggested one cloud computing information assurance framework which adopts ISO27000 series standards. In their publication of Cloud Computing Benefits, Risks and Recommendations for Information Security, they suggested in the area of Personnel security, supply chain assurance, operational security, identity and access management, asset management, data and services portability, business continuity management, physical security, environmental controls, legal requirements, legal recommendations and legal recommendations to the European commission.

d. Information Technology Infrastructure Library (ITIL) [21]: One of the service management framework adopted by major IT organization. Security management is a constant and continuous process which can be mentioned in SLA of the service provider. Identifying risks and improvement to overcome those risks are the continuous service improvement. Security management in ITIL is based on ISO/IEC 27002.

e. National Institute of Standards and Technology (NIST): NIST [3][20] has released two drafts, “Guidelines on Security and Privacy in Public Cloud Computing” and “The NIST Definition of Cloud Computing” (Draft Special Publication 800-144,145) giving a broad category of standards and guidelines even though oriented for US Government, widely adopted by most IT industries.

Likewise, many standard bodies and organizations work focused on their own country needs. Their works gives us valuable guidance and suggestions to improve the security controls and architecture. [4][5] [10] [11]. Users generally expect their service at optimal cost with performance. Besides providing service at optimal cost, cloud provider should give reliable, trustable, scalable services by adopting legal and regulatory compliances beside the security triad of CIA. Unless otherwise security is not there, this will raise problems in other feature also. So enhancing the security of the cloud is very much important to utilize all the nice features of cloud.

4. Proposed Method

Cloud Computing is accessing the services thru internet. Apart from IaaS, SaaS, PaaS, XaaS is possible in case of cloud. Users will be charged based on utility computing. Cloud adopts as pay per usage model. Fig.2. shows the general cloud computing model.

Cloud uses virtualization as its key technology [8] [9]. When end user submit their requirement, a separate Virtual Machine is created to run their specific application. In a single host machine itself multiple Virtual Machines can be run to utilize the resources. Fig. 3. Shows the Virtualization technique used for cloud.
Virtualization [6] helps multiple instances of same application can be run on one or more cloud resources. It automatically provides scalability when more number or user wants to run their application. It gives each user that their application is running on a single virtual machine. Here end user cannot see other user’s data. Proper isolation of virtual machine is important. Fig. 4. shows multiple VMs running on a single host machine with hypervisor. [16]

Multiple instance of an application can run on a single server or many server, provided by a trusted cloud service provider. Cloud user selects his provider based on their Quality of Service and their service level agreement. According to their usage, user can make an service level agreement covering such as uptime, response time, throughput, scalability, security issues.

Cloud Service can be deployed directly on a cloud providers without CAPEX. Many cloud providers are there. Amazon, Microsoft, IBM, Google are the major providers. Here Fig. 5. shows service deployment in an external cloud provider, CloudBees [7] [17] provider which in turn utilizes resources from Amazon.
Many providers give free tier limit to deploy our services in cloud. Once if we cross the limit, based on the usage, user will be charged. So anybody who wants to start their company without a CAPEX is possible. It is a flourishing technology.

An automated monitoring tool along with virtualization will solve the security problems of cloud. When we use the monitoring tool, it checks for the port scanning as well as for service scanning and protocol scanning and we can check the incoming request for the service and its route IP also from where request has generated. The following fig. 6. shows system running with some unknown services.

By combining Authentication and Authorization (JAAS) along with the service policy monitoring besides updating virtual machines periodically will enhance the security of cloud.

Each virtual machine can be allocated for each user requirement, isolating their virtual machine from other machine is important. Once there is a hidden service, an unknown service or other vulnerabilities, report can be generated. Based on the vulnerability assessment report, appropriate steps can be taken.

Even by taking appropriate snapshots, we can bring back to the system to the previously running state, in case any failure is there.

Easy rebuild of virtual machine is possible along with all the currently running applications. Because virtual to physical and physical to virtual migration easy. Teleporting is one of the nice feature of virtualization. From the images taken, Virtual machines can be easily rebuilt. Cloning of Virtual machine also very easy. So when many request is coming, by easily cloning the service instance machine running already, multiple instances can be generated to meet the scalability requirement.
Moreover, since because of this virtualization key technology, effective utilization of resources are more promising feature of cloud computing. Since many servers can run on a single server, many virtual machine can run on a single host machine with a help of a hypervisor which in turn saving power, which shows the way to green computing. Some of the key points to maintain security of the cloud is listed below:

• Any VM is intruded, or any kind of error, it can be isolated separately, without affecting other VMs, since isolation is possible in virtual machines.
• By carefully monitoring the resource utilization like CPU, memory, network, port, Isolating the intruded Virtual Machine is possible.
• By taking appropriate steps to recover or it can be destroyed for security purposes.
• Easily system can be rebuilt with the images taken already. Since Many VMs running on a single machine, effective utilization of resources are possible.
• Moving the VM from one Physical Machine to Another Physical Machine is Possible. Green Computing is achieved with the help of Virtualization technology.
• Some services and application may conflict with each other, that can be run on different VMs.
• With the help of Virtualization we can achieve Security, Reliability, Performance, Availability, Portability, Less Cost, Easy Manageability, Less downtime, etc.
• Besides having nice features, single physical machine break down will bring down all the VMs running in that.
• By properly updating the VMs Operating system, installing and updating the firewalls in VMs like the physical machine.
• A single VM can be specifically used for all the incoming request whether it is genuine request or not then it can be forward.
• If there is any hidden request, along with proper resource monitoring and port scanning, intruded VM can be easily identified.
• Upon error, necessary steps can be taken down to overcome by isolating the intruded VM.
• Proper isolation is important. Since resources allocated for each machine is different, that cannot be accessed through other virtual machine.
• By giving restricted access/ by devising proper privilege level all the VMs to access the physical resource, security of Virtualization can be fully achieved. With Secured Virtualization technologies, cloud security can be improved.

Not only security availability, performance improvement and moving our service from one provider to other provider also possible. Bringing back to our own infrastructure also easy with virtualization using virtual to physical migration concept.

5. Conclusion

Nowadays, Most of the vendors provide free usage to deploy their services in their cloud with certain limits like hours of usage, or hard disk space, storage or data transfer or number of end users. As a cloud user or developer, they have to choose the vendor based on their Service Level Agreements, security service standards and compliances.

Even though Cloud has some serious issues like security, privacy, social and political issues [14] [15], Cloud computing is going to be one of the venture technology in future. Cloud user should understand their own network, system, applications and data are moving to an unknown network which poses serious threat to security and privacy.

Using virtualization server, resources, network, desktop, application, operating system and storage can be virtualized. One of the major concerns in future is computing with less power. With virtualization, apart from flexibility, scalability, security, utilizing underutilized resources/idle resources, manageability,
cost effective cloud computing with virtualization technology takes less power since more than one virtual machines can be run on a single physical machine.

The above discussed monitoring technique along with virtualization, which helps the provider to achieve full security of the virtual machine is possible. Since virtualization is the key technique of cloud computing, enhanced secure cloud service can be achieved with the help of an automated monitoring techniques. In future like IaaS, PaaS and SaaS, Anything as a Service (XaaS) is going to be possible and can be achieved through Virtualization. Challenges and issues of cloud computing can be overcome by combining JAAS, Virtualization and an automated service monitoring tool with proper SLA agreement.

References
[1] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. “Cloud Computing and Grid Computing 360-Degree Compared”, Grid Computing Environments Workshop, 2008, GCE’08, 12-16 Nov. 2008.
[2] John Harauz, Lori M. Kaufman, Bruce Potter, “ Data Security in the World of Cloud Computing”, IEEE Security and Privacy, July/Aug. 2009, vol. 7, no. 4, pp. 61-64.
[3] Wayne Jansen, Timothy Grance, “Guidelines on Security and Privacy in Public Cloud Computing (Draft)”, NIST, NIST Special Publication 800-144; Jan. 2011.
[4] Siqin Zhao, Kang Chen, Weimian Zheng, “The Application of Virtual Machines on System Security”, Fourth ChinaGrid Annual Conference, chinagrid; 2009, pp.222-229.
[5] Xuan Zhang, Nattapong Wuwong, Hao Li, Xuejie Zhang, “ Information Security Risk Management Framework for the Cloud Computing Environments”, cit. 10th IEEE International Conference on Computer and Information Technology; 2010, pp.1328-1334.
[6] Loganayagi B, Sujatha.S., “Creating virtual platform for cloud computing”, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2010); 28-29 Dec. 2010, pp.1-4
[7] Loganayagi B, Sujatha.S., “ Cloud Computing in Stax Platform”, IEEE International Conference on Computer Communication and Electrical Technology, (IEEE- ICCCET 2011); 18-19 Mar. 2011, pp.1-5.
[8] Dawei Sun, Guiran Chang, Qiang Guo, Chuan Wang, Xingwei Wang, “A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques”, First International Conference on Pervasive Computing, Signal Processing and Applications pcsap; 2010, pp.305-310.
[9] Qian Liu, Chuliang Weng, Minglu Li, Yuan Luo, “An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds”, IEEE Security and Privacy, vol. 8, no. 6, pp. 56-62, Nov./Dec. 2010, doi:10.1109/MSP.2010.143.
[10] M. Sharif et al, “Secure In-VM Monitoring Using Hardware Virtualization”, Proc. 16th ACM Conf. Computer and Communications Security; ACM Press, 2009, pp. 477-487.
[11] Jia Xu, Jia Yan, Liang He, Purui Su, Dengguo Feng. ”CloudSEC: A Cloud Architecture for Composing Collaborative Security Services”, 2nd IEEE International Conference on Cloud Computing Technology and Science cloudcom; 2010, pp.703-711.
[12] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1; 2009, https://cloudsecurityalliance.org/csaguide.pdf
[13] D. Catteddu and G. Hogben. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA; 2009, http://www.enisa.europa.eu/
[14] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy. O’Reilly; 2009
[15] John W. Ritinghouse, James F. Ransome. Cloud Computing: Implementation Management and Security. CRC Press; 2010
[16] http://www.virtualbox.org/wiki/Documentation
[17] http://www.cloudbees.com/
[18] http://en.wikipedia.org/wiki/Cloud_computing
[19] http://www.27000.org/iso-27001.htm
[20] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[21] http://www.itil-officialsite.com/