Volume 3, Issue 9, September 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Security in Cloud Computing Environment using Intrusion Detection System

D S Bhilare
Head, Computer Centre,
Devi Ahilya University, Indore, India

Nilotpal Chakraborty
School of Future Studies and Planning
Devi Ahilya University, Indore, India

Abstract— Cloud Computing is essentially one of the most prominent and on demand technological aspect that IT offers today. It attempts to provide services to users on a leased basis which the user can get upon request. With its various service models, Cloud computing promises to cut the operational and capital costs for the service providers on one hand, and for the users by providing the opportunity to access services according to their needs on the other hand. However, despite the surge in activity and interest, there are significant, persistent security concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Cloud computing offers has many advantages, but is also vulnerable to threats. With the increasing demand of cloud computing, it is highly likely that more criminals will try to find new ways to exploit vulnerabilities in the system. There are many underlying challenges and risks in cloud computing that increase the threat of data being compromised. Intrusion detection systems (IDS) are a technology to handle one of the many security challenges faced by the cloud services. IDS can help in detecting intrusive activities, helping the network manager in taking appropriate actions to mitigate the problems.

Keywords— Cloud Computing, Cloud Security, IDS, HIDS, NIDS

I. INTRODUCTION

Since the inception of the concept, Cloud computing has been the most enticing field of Computer research mostly due to its cost efficiency and flexibility. The NIST definition of Cloud computing is "It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Thus cloud computing is considered to be a computational model, rather than being a Technology. In this model "customers" plug into the "cloud" to access IT resources which are priced and provided "on-demand". Essentially, IT resources are rented and shared among multiple tenants. Delivered over an Internet connection, the "cloud" replaces the company data center or server providing the same service.

Cloud computing represents a different way to architect and remotely manage computing resources. One has only to establish an account with any cloud service provider, such as Microsoft or Amazon or Google, to begin building and deploying application systems into a cloud. These systems can be, but certainly are not restricted to being, simplistic. They can be web applications that require only http services. They might require a relational database. They might require web service infrastructure and message queues. There might be need to inter-operate with CRM or e-commerce application services, necessitating construction of a custom technology stack to deploy into the cloud if these services are not already provided there. They might require the use of new types of persistent storage that might never have to be replicated because the new storage technologies build in required reliability. They might require the remote hosting and use of custom or 3rd party software systems. And they might require the capability to programmatically increase or decrease computing resources as a function of business intelligence about resource demand using virtualization. While not all of these capabilities exist in today's clouds, nor are all that do exist fully automated, a good portion of them can be provisioned.

While there are important security, privacy and regulatory issues that enterprises need to sort through before full migration to the cloud, and cloud vendors need to strengthen cloud capabilities in these areas before enterprise applications can be effectively hosted in the cloud, there are benefits that cloud computing offers today that can be leveraged in the deployment of many enterprise applications. To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance. Security concerns must be taken care of in order to establish trust in cloud computing technology. In this paper, we focus on one of the numerous security issues of cloud based environment, i.e., Intrusion. The discussion starts with the characteristics and service models of cloud computing. Then we put up the security and privacy issues associated with cloud environment. And finally introduce IDS and discuss its impact on cloud computing environment.

II. SERVICE MODELS

Cloud computing provides different services rather than a unit of product. The term services in cloud computing is the concept of being able to use reusable, fine-grained components across a vendor's network. This is widely known as "as a service". Offerings with as a service as a suffix include traits like the following—

- Low Barriers to entry, making them available to small businesses
- Large scalability
- Multitentancy, which allows resources to be shared by many users
- Device independence, which allows users to access the systems on different hardware.

These services put forwarded three models: software as a service (SaaS), platform as a Service (PaaS), and infrastructure as a Service (IaaS).

A. Software as a Service (SaaS)

In this service model, the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. When the software is hosted off-site, the customer doesn't have to maintain it or support it. On the other hand, it is out of the customer's hand when hosting service decides to change it. The idea is that you use the software out of the box as is and do not need to make a lot f changes or require integration to other systems. The provider does all the patching and upgrades as well as keeping the infrastructure running.

There are many types of software that lend themselves to the SaaS model. Typically, software that performs a simple task without much need to interact with other systems makes them ideal for SaaS. Some of these applications include—

- Customer Resource Management (CRM)
- Video Conferencing
- IT service management
- Accounting
- Web Analysis
- Web Content Management

SaaS applications differ from earlier distributed computing solutions in that SaaS was developed specifically to use web tools, like the browser. This makes them web native. It was also built with a multitenant back end in mind, which enables multiple customers to use an application. SaaS provides network based access to commercially available software. Since the software is managed at a central location, customers can access their applications wherever they have web access. Highest-profile examples are Salesforce.com, Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google, and VoIP from Vonage and Skype.

B. Platform as a Service (PaaS)

Delivers virtualized servers on which customers can run existing applications or develop new ones without having to worry about maintaining the operating systems, server hardware, load balancing or computing capacity. These vendors provide APIs or development platforms to create and run applications in the cloud – e.g. using the Internet. PaaS services include application design, development, testing, deployment and hosting. Other services include team collaboration, web service integration, database integration, security, scalability, storage, state management and versioning. Managed Service providers with application services provided to IT departments to monitor systems and downstream applications such as virus scanning for e-mail are frequently included in this category.

Well known providers of Platform as a Service would include Microsoft's Azure, Google Maps, ADP Payroll processing, and US Postal Service offerings.

C. Infrastructure as a Service (IaaS)

In the Infrastructure as a Service (IaaS) model, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components. IaaS delivers utility computing capability, typically as raw virtual servers, on demand that customers configure and manage. Here Cloud Computing provides grids or clusters or virtualized servers, networks, storage and systems software, usually (but not always) in a multitenant architecture. IaaS is designed to augment or replace the functions of an entire data center. This saves cost (time and expense) of capital equipment deployment but does not reduce cost

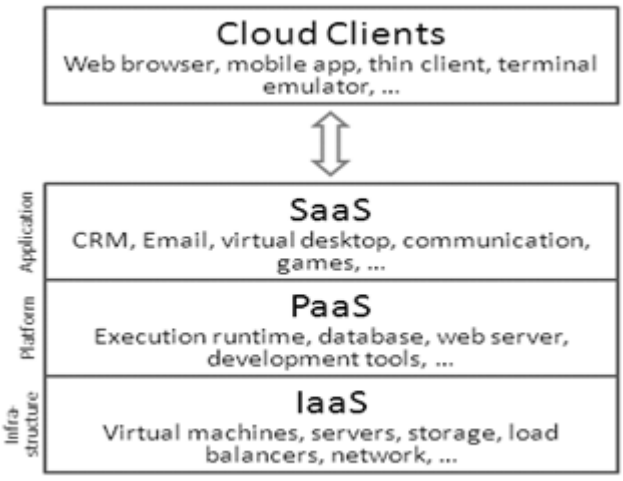

Figure 1: Cloud Service Models

of configuration, integration or management and these tasks must be performed remotely. Vendors would include Amazon.com (Elastic Compute Cloud [EC2] and Simple Storage), IBM and other traditional IT vendors. The diagram beside depicts the various cloud service models.

III. TYPES OF CLOUDS

For most businesses, organizations, or governmental agencies, there are three relevant types of clouds: Private (internal or vendor-hosted), Public (external), and Hybrid (mixed). Each cloud infrastructure has unique characteristics and offers different advantages and disadvantages.

A. Private Cloud

A private cloud is a cloud computing platform enables enterprises to implement cloud technologies at their onsite hardware and software. Enterprises are implementing a private cloud within areas of their infrastructure in which a cloud model makes the most sense. A private cloud provides many of the benefits of cloud computing without the loss of control and security risks associated with other cloud infrastructure models. A private cloud includes virtualization technology to enhance scalability, resource management, and hardware utilization. In addition, it incorporates data center automation of provisioning and chargeback metering for consumption and services-based billing capabilities. Identity-based security protocols ensure that only authorized personnel have access to appropriate applications and infrastructure.

Private cloud refers to cloud infrastructure developed internally by organizations that need to combine the agility of the cloud with the security and control of in-house systems. Infrastructures of private cloud are completely managed and corporate data are fully maintained by the organization itself.

Private clouds provide the following advantages—

- Ability to rapidly bring new services online without delays caused by commissioning or provisioning server infrastructure.
- Increased utilization of hardware and software infrastructure yielding greater ROI for capital expenditure.
- Greater data security, control and compliance with industry-specific regulations.
- Centralized control of usage, compliance and security policies via the use of shared resources.
- Frictionless development as developers can get results and iterate develop cycles rapidly.

B. Public Cloud

Public 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. Public cloud applications, storage and other resources are made available to the general public by service providers. End users without actually possessing these resources can gain access to them easily on demand via a Web browser from a simple laptop or terminal, wherever they are needed and with minimal management or service provider effort.

Some characteristics of Public Cloud are—

- Increased agility in terms of response to changes in the business environment.
- Reduced capital expenditure in IT hardware and software, in favor of operational expenditure.
- IT outsourced to specialists, providing access to greater expertise at lower cost.

C. Hybrid Cloud

The Hybrid cloud infrastructure is a combination of the Public and Private Cloud, often adopted by organizations that require greater control over come of the data they hold, yet still wish to run certain workloads on public cloud infrastructure as required. For example, a company may employ an internal cloud to share physical and virtual resources over a network, but extend these capabilities when needed such as at peak processing times. Implementing a mixed cloud infrastructure enables enterprises to pick and choose which applications within the portfolio reside on a public versus private cloud. For example, this model permits financial applications with the most proprietary information to remain behind a firewall, while other software such as collaboration, customer service, or supply chain can reside on a public cloud.

The various types of cloud infrastructure have been depicted in the following figure.

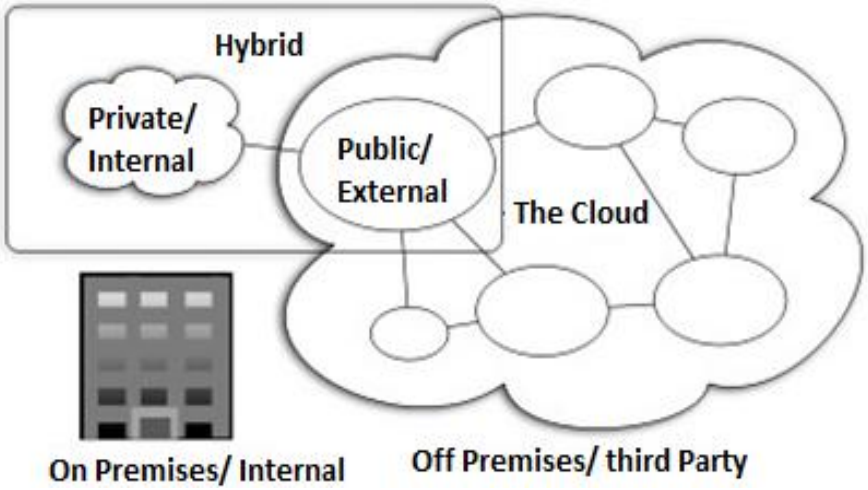

Figure 2: Types of Cloud Computing

IV. SECURITY AND PRIVACY FOR CLOUD

The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it critical to understand the security measures that the cloud provider has in place, and it is equally important to take personal precautions to secure the data. 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. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

Cloud security involves the fundamental issues as any computer security program: restricting access to authorized users, maintaining the integrity of data, and ensuring the availability of data and services. Cloud computing typically uses server virtualization, and if the virtualization isn't secure, data from one segment of a server could "escape" into another area, causing potential intrusive actions. The service level agreements (SLAs) that cloud providers offer are often not sufficiently specific to meet the requirements of a college or university. Cloud customers would usually undertake a risk assessment of any third-party provider, and increasingly organizations such as Shared Assessments provide resources to assist in this effort.

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices. While cloud security concerns can be grouped into any number of dimensions these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

Advocates of cloud computing promise great things, and many believe that the claims are not merely hype—that cloud services will be a defining characteristic of the next era of computing. Security could be the cloud's Achilles' heel, however, and must be sorted out for cloud computing to reach its potential. Information systems cover a spectrum of requirements—from total protection to complete openness—and internal risk assessments are the means by which an organization evaluates the trade-offs and decides what level of security is acceptable and appropriate. Cloud computing not only adds new layers to the question of computer security; it often also adds complexity in understanding the parameters that feed into a risk assessment. Because the systems and staff of a cloud provider are not under the control of a customer, institutions that use cloud services rely on contracts—and, to be sure, a certain amount of trust—for security information. Vendors offer different levels of transparency, and this becomes an important component of institutional efforts to evaluate cloud services.

V. INTRUSION DETECTION SYSTEM

Intrusion can be termed as an unauthorized entry to another's property or area, but in terms of computer science, it is the activities to compromise the basic computer network security goals viz. confidentiality, integrity, and privacy. Intrusion Detection (ID) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies. Intrusion Detection System (IDS) is a software or hardware component that automates the intrusion detection process. It is designed to monitor the events occurring in a computer system and network and responds to events with signs of possible incidents of violations of security policies. IDS use its various intrusion detection methodologies viz. Signature based intrusion detection; Anomaly based intrusion detection and Stateful Protocol Analysis, to detect malicious, unauthorized or harmful events occurring in the network or host in which they were deployed. According to their type of deployment, an IDS can be called as Host based IDS (HIDS) in which the IDS is deployed in a single host to monitor the events occurring in a particular host; and Network based IDS (NIDS) in which it is installed in the entry point of a network to monitor the traffic and events passing through the network.

The functioning of typical IDS is depicted in the figure 3.

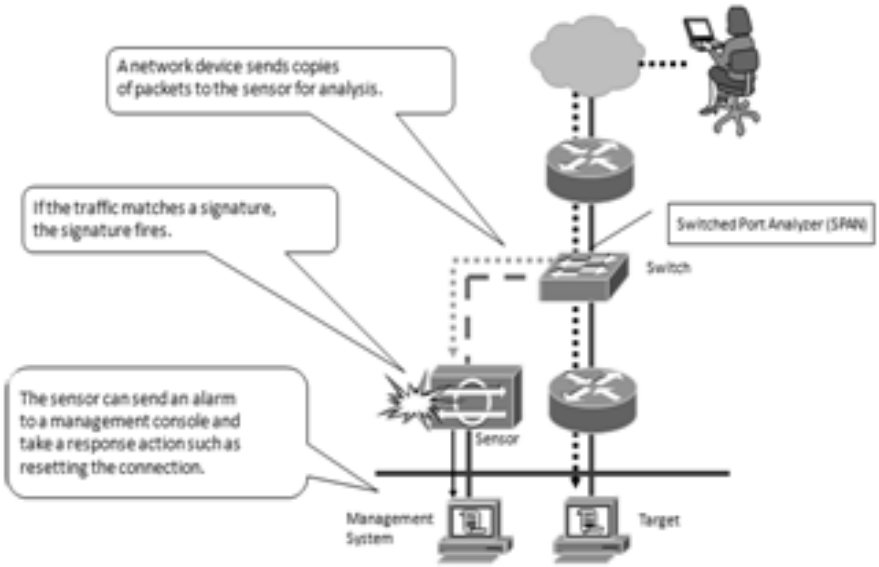

Figure 3: Intrusion Detection System

VI. IDS ON CLOUD COMPUTING

The ability to detect malicious activities and events occurring in a cloud computing environment is heavily dependent on the service model being used. In case of SaaS, users must rely almost exclusively on their providers to perform ID. You may have the option of getting some logs and deploying a custom monitoring and alerting on that information, but most ID will be done by the provider. In PaaS, like SaaS, most of the ID for this level of service will be done by the provider. Since intrusion detection systems (IDS) are typically outside the application, user must rely on the provider to deploy IDS in a PaaS. They can, however, configure their applications and platforms to log onto a central location where monitoring and alerting can be set up.

IaaS is the most flexible model for ID deployment. Unlike the other two, IaaS gives the users more options as a consumer. IDS in IaaS can be placed in a Virtual Machine, in the Host System or in the Virtual Network.

VII. PERFORMING INTRUSION DETECTION ON CLOUD

Providing security in a Cloud Environment requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. IDS in Cloud Computing integrate knowledge and behavior analysis to detect intrusion. We can perform Intrusion Detection in three ways as explained below—

A. Traditional Host based IDS

The first option is the traditional host intrusion detection system (HIDS). HIDS can be used on the VM, as well as the host/hypervisor. The HIDS on the VM would be deployed, managed and monitored by the user. The HIDS on the hypervisor would be the responsibility of the provider. If consumers desire to incorporate any of the hypervisor ID information in their own IDS, then they would have to coordinate with the provider.

Deploying and managing a HIDS on the VM would be the customer's responsibility, while HIDS on the hypervisor would fall under the responsibility of the provider.

B. Traditional Network based IDS

A second option is a traditional network intrusion detection system (NIDS). This type of deployment is useful in detecting some attacks on the VMs and hypervisor. It does, however, have several limitations. The first is that it cannot help when it comes to attacks within a virtual network that runs entirely within the hypervisor. Second, it has very limited visibility into the host itself. Lastly, if the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis.

In the cloud, NIDS falls completely in the realm of the provider to deploy and manage.

C. Hypervisor based IDS

The third option would be the use of an intrusion detection system that runs at the hypervisor layer but is not strictly a HIDS for the hypervisor. One of the promising technologies in this area is the use of VM introspection. This type of IDS allows you to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. The advantage of hypervisor-based ID is the availability of information, as it can see basically everything. The disadvantage is that the technology is new and you really need to know what you are looking for.

As with NIDS, this falls completely within the scope of the provider to deploy and manage.

VIII. CONCLUSIONS

Cloud computing is a paradigm shift in which computing is moved away from personal computers and even the individual enterprise application server to a 'cloud' of computers. A cloud is a virtualized server pool which can provide the different computing resources of their clients. Users of this system need only be concerned with the computing service being asked for. The underlying details of how it is achieved are hidden from the user. However, as with any other technological shift or change, security benefits and risks need to be addressed before the full benefits of cloud computing can be realized. Because of their distributed nature, cloud Computing environments are easy targets for intruders looking for possible vulnerabilities to exploit. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

ACKNOWLEDGMENT

The authors present sincere thanks to Dr. V.B. Gupta, Head, School of Future Studies and Planning, Devi Ahilya University, Indore and all the faculty members of the School and Computer centre, Devi Ahilya University, Indore for their encouragement and kind cooperation.

REFERENCES

[1] William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4th Edition, 2011

[2] Charles Pfleeger, Security in Computing, 4th edition, Prentice Hall, 2006

[3] Peter Mell, Timothy Grance; The NIST Definition of Cloud Computing; NIST Special Publication 800-145, 2011

[4] A. Iosup, N. M. Yigitbasi, and D. Epema, "On the performance variability of production cloud services," TU Delft, Tech. Rep. PDS-2010-002, Jan 2010

[5] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, Dawn Leaf ; NIST Cloud Computing Reference Architecture; NIST Special Publication 500-292, 2011

[6] Alexandru losup, Simon Ostermann,Nezih Yigitbasi, Radu Prodan, Thomas Fahringer, Dick Epema; Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing; IEEE TPDS, Many Task Computing, November 2010
[7] Richard Chow, Philippe Golle, Markus Jakobsson, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.
[8] Armbrust, M., Fox, A., Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.
[9] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.
[10] Jamil, D., & Zaki, H. (2011a). Cloud Computing Security; International Journal of Engineering Science and Technology (IJEST), Vol.3 No.4, 3478-3483.
[11] Kevi Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham; Security Issues for Cloud Computing; International Journal of Information Security and Privacy, 4(2), 39-51, April-June, 2010
[12] Flavio Lombardi, Roberto Di Pietro; Secure Virtualization for Cloud Computing; Journal of Network and Computer Applications, 2010
[13] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing: http://www.cloudsecurityalliance.org/csaguide.pdf
[14] Tim Mather, Subra Kumaraswamy, and ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009
[15] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc.
[16] U. F. Minhas, J. Yadav, A. Aboulnaga, and K. Salem, "Database systems on virtual machines: How much do you lose?" in *ICDE Workshops*. IEEE, 2008
[17] Karen Scarfone , Peter Mell, " Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology,2007
[18] Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004
[19] Desai, Neil. "Intrusion Prevention Systems: the Next Step in the evolution of IDS." Security Focus, 27 February 2003
[20] Robert Drum," IDS & IPS Placement for network protection" , CISSP 26 March 2006.
[21] Kleber, schulter, "Intrusion Detection for Grid and Cloud Computing", IEEE Journal: IT Professional, 19 July 2010.
[22] Kleber, Schulter, "Intrusion Detection for Grid and Cloud Computing", IEEE Journal: IT Professional, 19 July 2010.
[23] C. Boeckman, "Getting Closer to Policy-Based Intrusion Detection," *Information Security Bulletin*, Vol. 5, No. 4, May 2000.
[24] Nilotpal Chakraborty, "Intrusion Detection System and Intrusion Prevention System: A Comparative Study", IJCBR, ISSN: 2229-6166, Vol. 4 Issue 2, May 2013.
[25] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", IEEE sixth international conference on Information Assurance and Security, 2010.
[26] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.
[27] Sebastian Roschke, Feng Cheng, Christoph Meinel, "Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[28] http://www.cloudsecurityalliance.org/guidance
[29] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
[30] http://www.hpcinthecloud.com/hpccloud/2010-11-09/cloud_security_the_federated_identity_factor.html
[31] Google Cloud. Available at:www.googlecloud.com
[32] Microsoft Azure home page: http://www.microsoft.com/azure
[33] Amazon Web Services. Amazon Elastic Compute Cloud homepage: http://aws.amazon.com/ec2
[34] https://cloudsecurityalliance.org/
[35] www.ibm.com/security/cloud-security.html
[36] www.hpl.hp.com/research/cloud_security
[37] https://blog.cloudsecurityalliance.org/

