Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study of Security Challenges and Next Generation of Cloud Firewall

[1]F. Bezzazi*, [2]M. EL Marraki, [3]A. Kartit
[1, 2] LRIT Unité associée au CNRST(URAC29)- Faculty of Sciences University of Mohammed V-Agdal,
B.P.1014 RP Rabat, Morocco
[3]Laboratoire de Technologie de l'Information University of Chouaib Doukkali EL Jadida, Morocco

***Abstract**— the concept of cloud computing has become the most spreading orientation over the last few years. Indeed, due to the large advantages that offer this new promising paradigm such as scalability, availability, reduced costs and so on, many organizations moved onto the cloud computing environment. This technology aims to power the next generation of data centers and attracts more and more costumers, however, the grow of number of users means the increasing of number of machines utilized, important data shared that need to be managed, and many issues appears with it. For this reason, cloud service providers must deal with those challenges and ensure the trust for users to encourage them to join the cloud computing and take benefit from this new area. In this paper we will focus on the part of security in the cloud architectures. Since the traditional firewalls are no more suitable for cloud platforms, we discuss new security challenges that face cloud computing and how new generation of firewalls can provide trustfully mechanism to prevent the network traditional and new attacks.*

***Keywords**— cloud computing; security; firewall; cloud challenges.*

I. INTRODUCTION

Based on the principle of delivering infrastructure, platform and software as services in on-demand manner over the internet with reduced costs, cloud computing attracts a large number of customers and IT industry. This new paradigm is considered as the next generation trend in computing, thanks to the huge opportunities that it offers to its users. The most important advantages provided by cloud computing is that resources are delivered as general utilities that can be rented and released by users through the internet, it also allows small businesses to increase their resources in case of need to get larger. Major companies benefit from cloud platforms such as Google, Microsoft, Amazon and Facebook in order to supply more powerful, reliable and cost-efficient cloud environment. Google Trend shows in figure 1 the evolution of the migration of users and enterprises onto the cloud for the last 10 years.

Many versions of cloud computing were proposed, we consider in this paper the definition of NIST (National Institute of Standard and Technology):

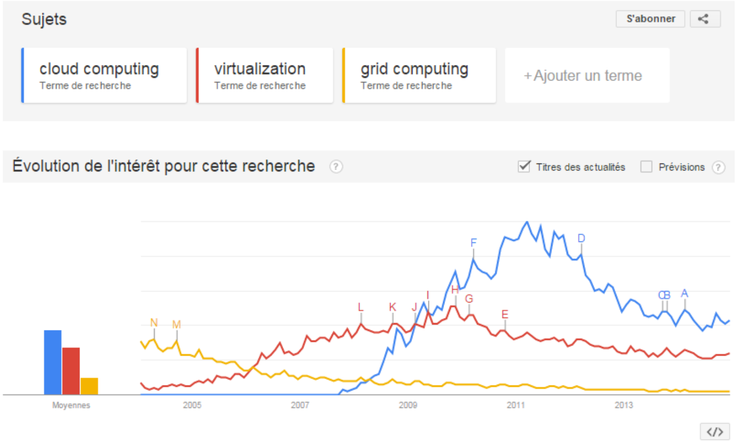

Figure 1: Cloud Computing in google trend

"Cloud computing is 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 service provider interaction."

Indeed, cloud computing allows customers to expand their resources from infrastructure services and data centers when they need to manage more data and users, which means high scalability or surge computing [3], users can also easily access their data from anywhere anytime since the services hosted are generally web-based and this from different devices, it can be laptop computers, cell phones, PDAs and so on. Cloud computing uses a pay-as-you-go pricing model in order to reduce costs by allowing users to rent resources from the cloud according to its own needs and pay only for the usage.

All these elements proof that the future is cloudy, that means that in near future everything will be offered as on-demand service. However, it also brings some potential security threats limiting the chance for companies and personal users to shift to the cloud environment. According to researchers three main challenges have to be discussed, namely, security, privacy and trust. Recent researches gave much importance to this major part of the cloud computing, most of authors discussed the security problem in their works especially how to secure storage of data, the management of those data but rare of them who evoked the security tools such as firewalls in the virtual context. In this paper will be interested by the part of security in cloud architecture, in particular firewalls, the different types of firewall in recent works and what are expectation for the next generation of firewalls.

The remainder of this paper will be as follow: section II is dedicated for the cloud computing technologies, the common layer and different types of cloud, followed by a third section exposing the main challenges that cloud have to deal with. In section IV we will talk about the firewall in a cloud conditions and what is the next generation of firewall while existing methods and approaches in recent researches will be discussed in section V and concluding by some propositions and future works.

II. CLOUD COMPUTING TECHNOLOGIES

The cloud computing technology is actually changing the meaning of business. Two basic types are provided by cloud computing environment; computing, data storage. Therefore, user doesn't need anything but internet access, in order to manage his data or to do some computing tasks easily. Before touching the mechanism of cloud computing, let's define first its architecture.

A. *Cloud computing architecture:*

The common layer design of cloud computing as shown in fig 2, is constituted by four principles layers: PaaS, IaaS, SaaS, data center.

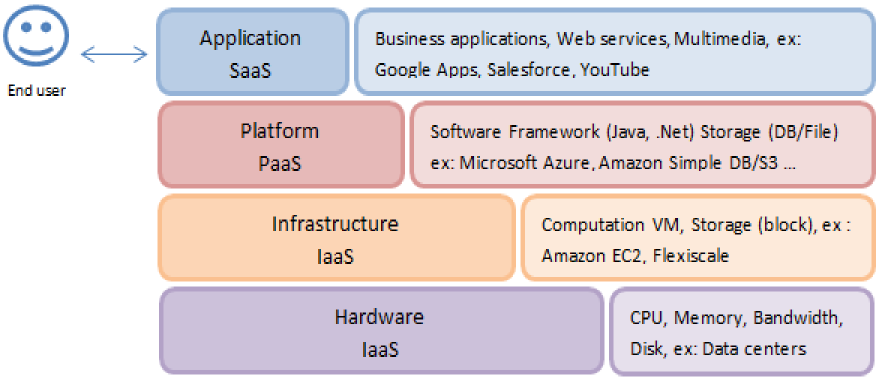
End user
Application
SaaS
Business applications, Web services, Multimedia, ex:
Google Apps, Salesforce, YouTube
Platform
PaaS
Software Framework (Java, .Net) Storage (DB/File)
ex: Microsoft Azure, Amazon Simple DB/S3 ...
Infrastructure
IaaS
Computation VM, Storage (block), ex :
Amazon EC2, Flexiscale
Hardware
IaaS
CPU, Memory, Bandwidth,
Disk, ex: Data centers

Figure 2: Cloud computing architecture

- *Infrastructure as a service (IaaS):* Service provider outsources the equipment used for storage, such as hardware, servers or networking components, it is also responsible for housing, running and maintaining the operations.
- *Software as a service (SaaS):* Service provider offers the hosted software applications to customers over the internet based on a software distribution model.
- *Platform as a service (PaaS):* Service provider offers platform where customers develop, run and manage their web applications. Users rent virtualized servers, hardware or operating systems over the internet.

B. *Cloud computing types:*

As believed by researchers, we can define four different types of cloud according to the access scope: Public cloud, private cloud, hybrid cloud and community cloud. In fig 3 we present only the most important ones:

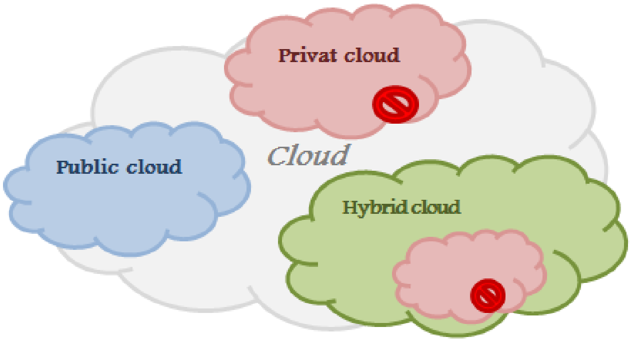

Figure 3: Types of cloud computing

- Public cloud: Is a 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.
- Private cloud: Which is proprietary network or a data center, that uses cloud computing technologies; such as a virtualization. A private cloud is managed by the organizations it serves.
- Hybrid cloud: Is maintained by both internal and external providers.
- Community cloud: Is a cloud service model that provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider [4].

III. CLOUD COMPUTING CHALLENGES

Cloud computing provides to its users huge opportunities which represent its strong point, large companies such as Google, Amazon, Facebook and Microsoft strive to gain benefit from its significant advantages:

- *Scalability:* Is one of major advantages of cloud computing. Service providers offer sufficient resources from data centers and racks of servers making them easily accessible. When business increases, user needs more resources; service provider expands its resources in order to handle the speed increase in service demand (e.g. flash-crowd effect). We sometimes called it surge computing [3].
- *Minimal costs:* Cloud computing uses a pay-as-you-go pricing model. In addition, resources can be rented and de-allocated on demand. This allows reduce operating costs by releasing resources in case of low service demand.
- *Accessibility*: Users can easily get access to their data from anywhere, anytime and from different type of devices, it can be laptop, PDAs, smartphone and so on. All they need is internet connection.
- *Reduction of maintenance expenses:* The best part about cloud computing services is that it is maintenance-free, update-free, and free of every other job that is done by a user in other computing services. Everything out here is taken care of by the service provider.

It's necessary to mention that all these advantages are not without costs. Indeed, cloud computing have many proof to show in term of privacy, trust and confidentiality, which lead several researchers to discuss this other side, in order to improve the level of trust between cloud and customers.

The most interesting challenges in cloud computing trend are:

A. Data management

Cloud computing allows customers to gain benefit of computer processing, storage and software delivery by a third party which is the next generation of data centers, away from the local servers across the network. Those data centers are hosted by large infrastructure such as Amazon, Google, Microsoft, Yahoo or Sun.

Several data management applications exist, each company approve the application that suites their needs for example pay-as-you-go pricing model or the maintenance of the hardware by the vendor is the perfect scenario for the star-ups and medium-sized businesses in this way they are free from having to generate their own power, enabling them to benefit from powerful computing resources over the network and focus on their business activities

Vendors propose many services over internet in their cloud such as computer processing, storage and management of data, software deployment and hardware location. Indeed, service providers give clients a set of virtual machines in order to store their own software and data. Resources are allowed on demand regarding the need of the client.

Each database system have advantages and disadvantages, and each enterprise decide based on cloud characteristics, which data management applications are best suited for deployment on top of their business infrastructure. We remind some of pertinent cloud characteristics:

- The elasticity of cloud power which is possible only if workloads are parallelizable [5]. In case of need of more resources (ex: e-commerce company, social networking website…), providers offer additional server instances to a task. Some applications cannot be run in parallel with the old instances, but generally applications are designed to run on top of shared-nothing architecture to facilitate elastic scaling, which force developers to write that can run in a shared-nothing environment.
- Data are stored in untrusted host: When a client stores data in the cloud, service provider rent for him a set of racks of servers and virtual machines to save his data. However, the service provider doesn't give all information about the services he is offering, such as localization. In general, the fact that client put his data out of his local servers need to improve the level of security and much proof of trust. Data are stored in different localization to guarantee the privacy but at the same time, if a violation of this information happened, client may never know about it. Client does not have control of the storage of the management of data, some known companies (e.g. Amazon S3) allow their customers to choose the localization between US or EU, but it's not sufficient.
- Data are replicated, often across large geographic distances in order to ensure the availability and durability of data. This operation is done through under-the-cover replication i.e. automatically without permission or request from client. Some large companies (Amazon S3) ensure the replication across "Regions" and "availability zones" so it can persist even in case of failure of an entire location while others (Amazon EBs) replicate only in the same availability zone which is error prone.

Based on this characteristics clients have the power to choose which data management applications suited their business. Two data management market exist into the cloud: Transactional and analytical.

1. Transactional data management:

Referring to the bread-and-butter of online e-commerce, airline reservation, databases that back banking applications which rely on the ACID guarantees that databases provide [1]. Transactional data management systems don't use a shared-nothing architecture; this implementation is designed only to be used for data warehouse [6]. In fact, data is divided and put across sites that are not limited to be reached from one site. The main benefit of shared-nothing architecture is its scalability (fig. 4). Therefore, the fact that data is replicated over large geographic distances, make the maintenance of ACID guarantees a very hard stuff.

2. Analytical data management:

We talk about the applications that demand data store for use in business planning, decision support or problem solving [6]. The analytical data management well matches with the share-nothing architecture. Indeed, Teradata, Netezza, DATAllegro use a shared nothing architecture in their analytical DBMS products. Small and medium-size businesses prefer this type of data management because it allows saving sensitive data from the analysis, including it after encryption process or after applying an anonymizing function. Therefore the use of a recent snapshot of data in analytical data management makes the ACID obviously guaranteed.

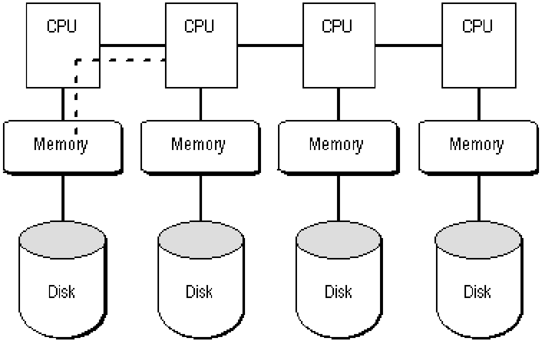

Figure 4: Shared-nothing architecture [24]

B. Data privacy

Security in cloud computing represents the major barrier for organizations to adopt this important paradigm. Instead of all benefits that cloud offers it inherits some security risks and vulnerabilities from the conventional Internet, such as integrity, availability and data privacy and so on. Due to the sharing of resources between all the subscribers in the cloud, the users are confused if they can trust the service provider or not especially when it's about storing their private data, since there is no physical localization for the servers used, with probability to reside in other country. This confusion relieves different regulations and security parameters [4].

As data are conserved in different servers that are not in the same set of racks, so that data availability will become a big concern due to many factors, like bandwidth efficiency, or service cloud availability. In order to secure the data shared, some researchers propose to store the data in encrypted format, to solve the problem. However, the method used is very important to define if the technique is efficient or not. Client must be satisfied by the services offered by the service providers but also, ensured about their data which are private in many cases.

C. Virtual machine migration

The aim of migration virtual machines is to separate between hardware and software considerations, and consolidation clustered hardware into a single coherent management domain, we say that live OS migration is a powerful tool for cluster administrators. One of the advantages of virtualization is to allow the transmission of the entire VM across the network to move from a physical machine to another one as shown in following figure (fig 5).

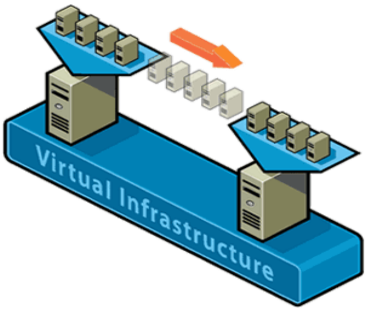

Figure 5: Virtual machine migration [23]

Therefore, when a physical machine needs to be removed or when a cloud computing hosting service want to change the communication patterns to accomplish statistical or dynamical multiplexing tasks, administrators may migrate OS including the applications that are running to an alternative machine(s), in order to achieve high bandwidth for firmly couple of hosts or power availability in the data center, also in many cases for freeing the original machine for maintenance. For this, the communication topology must be designed in order to make virtual machine migration easy, rapid and significantly manageable.

Two type of migration exist, the managed migration; performed by migration daemons running in the management VMs of the source and destination hosts, and the self-migration which places the majority of the implementation within the OS being migrated.

It necessary to remind that VM migration is done only in case of the trustfully of both servers source and destination. In fact, before the live migration both nodes Ns (source node) and Nd (destination node) negotiate a session key Ks [7]. This key Ks will be used to secure the transfer of the VM from Ns to Nd. After the authentication and verification Ns transfers the encrypted and hashed VM to the Nd. Recent works have been interested to design efficient protocols for trust establishment and management [8, 9].

D. Flow management and analysis

Cloud computing allows customers to host databases or software in a large cloud servers of third party. However, large companies preferred to host their sensitive information in restricted servers rather than store it in the public cloud. This led network operators to find how traffic flows through the network, in this way they can make many of the management and planning decisions. Indeed, the analysis of data traffic in recent data centers is primary for web applications to optimize customer experiences. Several challenges for existing analysis method and traffic measurement to extend to data centers:

- The density of links is much important than that in ISPs (Internet Service Provider) or enterprise networks, which makes the worst case scenario for existing methods.
- Most existing methods cannot handle the traffic matrices of more than a few hundreds end hosts, while even a modular data center contain several thousand of servers.
- Applications deployed on data centers such as MapReduce jobs change the traffic pattern assumed by existing methods.

In recent works there is a lack of measurement and analysis of data center traffic. Some researchers propose the use of Federated cloud computing (FCC) which comes to solve similar problem by using both private cloud and public one [10]. Greenberg et al. [11] talk about network infrastructure design based on the characteristics of data center traffic on flow sizes and concurrent flows. Benson et al. [12] perform a complementary study of traffic at the edges of a data center by examining SNMP traces from routers. Therefore, this analysis is very important for administrators who aim to perform the most suitable firewall that can analysis incoming or outgoing traffic across network and to secure the communication between clients and the cloud.

IV. CLOUD FIREWALL

In the first part of this paper we talked about the characteristics and challenges that concern the cloud environment. Based on this information, we will discuss in this part, the next generation of cloud firewall but first let's remind its definition.

Firewall is an essential component in any network architecture. It's actually the first line of defense which aims to protect and manage incoming and outgoing traffic across network. Several types of firewall exist; each type is designed to work in certain conditions. Administrators have to choose the most suitable type to their network infrastructure to control incoming or outgoing flow across network. They manage a firewall policy which is a list of rules that block or permit traffic from a source to a destination. However, in a world of virtualization things have changed, number of users increase constantly, data are saved away from a local servers, all services are shared and users still don't understand the real broader concept of this converged infrastructure. New attacks and threats appeared too, and are still under study from researchers. This new conditions imply the need of other parameters in order to adapt firewalls which are probably, a virtual too (at least use the benefits of virtualization) to this new concept. One of the advantages of cloud computing is its scalability and the rapid increase of data that must be managed in real time. Therefore, the most secure behavior of firewalls is to avoid the delays caused by stopping traffic, analyzing flows and the redirection to the right way. In this sense, when organizations move onto the cloud they will need a next generation of firewall to secure their networks, which have different properties compared to the traditional one.

From this, we can say that next generation of cloud firewall must:

- Respect the engagement of millions of users simultaneously and have the capacity of handling massively increase data throughput, without compromising security.
- Contribute positively to data applications and accelerate the decision making to access or not.
- Perform a deep analysis using more parameters in order to priorities good applications not only blocking illegal or suspicious traffic.
- Encourage more users by using easy managed and deployed cloud firewall infrastructure that suits business-critical applications.
- Handle the migration of virtual machines and key resources in the cloud.
- Handle the heavily traffic of smartphone and tablet to and from the cloud, recognizing that these tools are consuming important bandwidth and forcing significant traffic through the content filter.
- Support most of data management applications and resource provisioning.
- Enable user who had internet to access an application anytime from anywhere using any type of device.

Cloud computing propose some solution but the problem of control still not satisfy the criteria of trust [9]. Indeed, the cloud service provider must share the responsibility with the client, which means that both entities must have the control of the management of the cloud firewall considering that both parts are trustworthy.

V. EXISTING SECURITY APPROACHES

It's necessary to mention that there is a lack of works focused on next generation of firewall in the cloud, most of works are about the data management, data privacy using encryption methods, the analysis of sensitive flow or the virtual machine migration. Rare are researchers who have the interest of designing a model of firewall which can represent the next generation of cloud firewall. Here is some works about the security in the cloud environment.

Geethapriya and Shantha [13] proposed a model of firewall designed especially for VMs, since IaaS is very similar to a distributed computer environment. This suggested distributed firewall model comprises of four main elements: CFMS (Cloud Firewall Management Server), FC (Firewall Client), LS (Log Server), CS (Certificate Server). The tenant has full control over this model. The different parts of the distributed firewall have an essential aim, like the CFMS which function is the configure firewall policies in the distributed firewall system, and distribute those policies to the end firewalls, in the other side we have the FC which is installed in the VM, at the first of creation of the VM, CFMS send for it firewall policies to convert them into firewall rules, each VM issues log information to CFMS to store them in the Log Server. The aim of the certificate server is to certify the CFMS and the VMs.

Many researchers have proposed the encryption of the user's data stored on service provider equipment. [14] define an extern cloud which aims is to certify the authentication, the encryption decryption of the data in term of generate the keys for both entities, and do the auditing as well, so they proposed a mechanism to improve the level of security with the use of RSA encryption; symmetric key. The model uses three separated parts, one for the storage and one for the auditing the authentication and the encryption process, while the third part is for the client who wants to store data.

Bellovin proposed a topology independent distributed firewall architecture [15]. Topology limitations are overcome with the use of a cryptographic certificate used as the host identifier. Unlike having Internet Protocol (IP) addresses in most of the firewalls, these signatures are independent of the network topology and cannot be easily spoofed. This tools us with a good method to identify VMs of IaaS in the cloud.

Thames, Abler, and Keeling describe an architecture that implements a distributed firewall with distributed active responses [16]. This architecture is based on the concept of hosts within a trusted domain of administration that can detect anomalous behaviors and create blocking policies against the anomalous hosts. Once a host has detected an attack, a blocking rule is created for the offending IP address and the host distributes the information on the attack condition to its neighbors, who also creates blocking rules upon receiving this information. [17]Discuss in their work the feasibility of deploying Information Flow Control (IFC) as a part of next generation of secure cloud infrastructure. They showed that despite of the open challenges that remain to be addressed, IFC models can lead to practical and more secure cloud computing. This method doesn't escape to failure in case of cover channel [18] or implicit flow [21, 22] for this; it must introduce a process sensitivity level [19]. [20] Proposes multi-threaded NIDS model for distributed cloud environment that handles large flows of data packets, analyze them to generate reports efficiently by integrating knowledge and behavior analysis to detect intrusion. The model is based on three modules: capture & queuing module, analysis and processing module and reporting module. Therefore this approach seems to be able to handle high volume of data by a single node IDS. Authors assume that it also carry out concurrent processing of data analysis.

VI. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users. However, it also raises some security problems which may slow down its use. Understanding the types of the existing vulnerabilities in Cloud Computing will help organizations to the shift towards the Cloud. Since the appearance of the idea of cloud computing, traditional web applications, data hosting, and virtualization have been reviewed to be adaptable to it. However, most of the suggested solutions were immature or inexistent. In this paper we summarized several propositions that still don't give an efficient model suitable and easy deployed in cloud computing infrastructure. In order to handle massive data, well manage the number of users that increases significantly and regarding the new data management applications, firewall must use new parameters to analyze the traffic efficiently and in rapid time while avoiding delays that cause some failure of the system.

In our future work we will aim to design a new model of next generation of cloud firewall. Our model will use the system of distributed firewall. Indeed distributed firewall offers many advantages and can be managed by more than one part. It allows the prevention from intern attacks and extern as well. We have the possibility to implement it in each part of the materials. The use of the MPLS protocol [25] will improve the level of trust of the model. Strong system of authentication is necessary for guarantying confidentiality for users. After establishing this optimized model or strategy, clients of cloud service are able to use more than one cloud service in a secure environment, and share data or communicate safely in a cloud using laptop, PC, smart phone/PDA etc.

REFERENCES

[1] Daniel J. Abadi and Yale University "Data Management in the Cloud: Limitations and Opportunities" IEEE Data Eng. Bull 01/2009; 32:3-12.

[2] Q. Zhang, L. Cheng and R. Boutaba "Cloud computing state of the art and research challenges" J Internet Serv Appl (2010) 1: 7–18 DOI 10.1007/s13174-010-0007-6, 20 April 2010

[3] Armbrust M et al (2009) Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report

[4] A.C. Weaver, “Secure socket layer”, IEEE Journal & Magazine on computer, vol. 39, Issue 4, pp.88-90, April 2006.

[5] http://www.oracle.com/solutions/business_intelligence/exadata.html

[6] D J.Abadi, “Data Management in the Cloud: Limitations and Opportunities”, IEEE Data Eng. Bull 01/2009, 32:3-12

[7] Clark C, Fraser K, Hand S, Hansen JG, Jul E, Limpach C, Pratt I, Warfield A (2005) Live migration of virtual machines. In: Proc of NSDI

[8] Krautheim FJ (2009) Private virtual infrastructure for cloud computing. In: Proc of HotCloud

[9] Santos N, Gummadi K, Rodrigues R (2009) Towards trusted cloud computing. In: Proc of HotCloud

[10] P. Watson, “A multi-level security model for partitioning workflows over federated clouds,” Journal of Cloud Computing, vol. 1, no. 1, pp. 1–15, 2012.

[11] Greenberg A, Jain N et al (2009) VL2: a scalable and flexible data center network. In: Proc SIGCOMM

[12] Dean J, Ghemawat S (2004) MapReduce: simplified data processing on large clusters. In: Proc of OSDI

[13] Geethapriya Liyanage, Shantha Fernando, “Firewall Model for Cloud Computing” 2013 IEEE 8th International Conference on Industrial and Information Systems, ICIIS 2013, Aug. 18-20, 2013, Sri Lanka

[14] Ashutosh Satapathy, J. Chandrakanta Badajena, Chinmayee Rout « A Secure Model and Algorithms for Cloud Computing Based on Multicloud Service Providers” International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 12, December – 2013 ISSN: 2278-0181

[15] Steven M. Bellovin, “Distributed Firewalls,” in login:, Vol. 24, 1999, pp. 37–39.

[16] J. L. Thames, R. Abler, and D. Keeling, “A distributed firewall and active response architecture providing preemptive protection,” in Proceedings of the 46th Annual Southeast Regional Conference on XX, New York, NY, USA, 2008, pp. 220–225.

[17] W. Zeng, C. Mu and M. Koutny “A Flow Sensitive Security Model for Cloud Computing Systems” School of Computing Science, University of Newcastle upon Tyne, June 2013

[18] V. Kashyap, B. Wiedermann, and B. Hardekopf, “Timing- and termination-sensitive secure information flow: exploring a new aproach,” in 2011 IEEE SOSP.

[19] US Department of Defense, “Trusted Computer System Evaluation Criteria (Orange Book),” 1983.

[20] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande “Intrusion Detection System for Cloud Clomputing” International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012

[21] D. E. Denning and P. J. Denning, “Certification of programs for secure information flow,” CACM, vol. 20, no. 7, pp. 504–513, 1977.

[22] M. Gyung, S. McCamant, et al., “DTA++: dynamic taint analysis with targeted control-flow propagation,” in Network and Distributed System Security Symposium. Internet Society, 2011.

[23] http://fatmin.com/2010/03/04/how-to-disable-drs-for-one-vm-in-a-drs-enabled-cluster/

[24] https://docs.oracle.com/cd/A57673_01/DOC/server/doc/SPS73/chap3.htm#shnothing

[25] http://www.nolot.eu/Download/Cours/reseaux/m2pro/WAN0809/MPLS.pdf