ISSN 2320 - 2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol. 4 No.1, Pages : 01 – 07 (2015)
Special Issue of ICCSIE 2015 - Held during January 16, 2015, Bangalore, India
http://warse.org/pdfs/2014/iccsie2015sp01.pdf

Research Challenges in the Emerging trends of Cloud Computing

Shaik Khaja Mohiddin[1], Dr.Suresh Babu Yalavarthi[2]
1.Asst. Proff, VVIT, Nambur,Guntur, mail2mohiddin@gmail.com
2.Prof. in Computer Science,JKC College Guntur, yalavarthi_s@yahoo.com

ABSTRACT: with the recent development and vast growing of the technologies with a variety of flavors cloud computing has attracted many IT industries irrespective to their vastness , towards itself either it may be a service providing side where a variety of services are provided with low cost and down to the public or it may be related security providing aspects but with the growing sound of cloud computing its challenges and issues are also growing as there is positive and negative side of every technology in the same way cloud has also the same but here the advantage is that these negative i.e. practical problems can be converted to the positives , which stand as the solutions for the upcoming issues, cloud service users are more worried about the availability , quality and security issues of cloud ,In this paper we have traced out the various upcoming research challenges that the cloud is facing and also proposed certain measures to overcoming them where ever they are required. Though cloud computing has became a popular thing now also the researches are going on it as new things are being developed in it at the same time certain challenges are also developed in it. In this paper challenging research issues in cloud computing are discussed in detail:
Key words: Cloud Computing, DIDS, HIDS , IDS, IPS, , NIST.

INTRODUCTION

Many businesses think cloud computing is only for the big operators: the Google and Microsoft's and international names that seem to have unlimited reserves of cash and staff to make it work. But businesses of all sizes and ages are using cloud computing

'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.

There is a great impact of Cloud Computing on the IT industry for the past few years large companies such as Google, Amazon and Microsoft tend to provide more powerful, reliable and cost efficient cloud platforms, and business enterprises, besides these cloud computing provides several forceful features which takes it nearer to the business owners, some of them are labeled as

Fig1shows showing a representation of cloud services

No upfront investments: Cloud computing provides pay for what you use pricing model, here a cloud users lends the sources from the cloud service provider and they pay for the resources for how much they have used from it so it avoids a pre investment cost to a lot.

Lowering operating cost: as the resources can be allocated and de allocated depending upon the load, due to which operations can be carried out at low cost.

Highly Scalable*:* infrastructure providers pool large amount of resources from data centers and make them to be easily accessible, where a service provider can expand the services to large scale in order to overcome the rapid increase in service demands.

Easy access*:* all the services provided by the cloud are web based so an authenticated user can access these services simply by getting through the internet, there is no limitations for the access of cloud services i.e. they can be accessed easily device independent and get accessed even with cell phones, PDAs, laptops.

Reducing business risks and maintenance expenses: as the cloud services users are lending the infrastructure from the cloud providers so they do not go with its maintenance expenses everything is going to be handled by these infrastructure providers, so the service providers can cut down hardware maintenance and the staff training costs.

The remaining part of the paper is organized as follows section 2 describes the overview of cloud computing, in section 3 the architecture of cloud computing is described and in section 4 various threats and their respective measures have been specified, in section 5 we have specified certain Intrusion Detection systems and Intrusion prevention Systems have been described, finally the paper is concluded in Section 6.

OVERVIEW OF CLOUD COMPUTING

Here we take the definition of cloud computing provided by National Institute of Standards and Technology (NIST) [1].

NIST definition of cloud computing is given as
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.*

In cloud computing, the various kind of available service models are:
Infrastructure as a Service (IaaS). Here the cloud providers provide the consumers with on demand provisioning of infrastructural resources, which are usually VMs, here the cloud owners are called as Iaas Providers examples of IasS Amazon EC2[2],Go Grid [3] and flexiscale [4]

Cloud computing provides the consumer with the capability of conditional dealing related with storages, networks and other computing resources, and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications, storage been controlled by the consumer having a limited control on the selected networking components.

Platform as a Service (PaaS). Here the cloud providers provide the consumers with ability to install on the cloud infrastructure; consumers do not have any requirements for this beside a simple network connection, here also consumers do not have to maintain these cloud infrastructures which may include servers, operating systems or storage. Examples of PaaS providers include Google App Engine [5], Microsoft windows azure and force .com.

Software as a Service (SaaS). Here cloud providers applications are utilized by the consumers which are running on the cloud infrastructure. Client can access these various flavor of applications from any one of their devices, with the help of thin client interface, which may be either a web browser. Client has an advantage that they do not involve in managing infrastructure, which may include servers, operating systems, storage, any individual application capabilities. Examples of SaaS salesforce.com, racks pace [6].

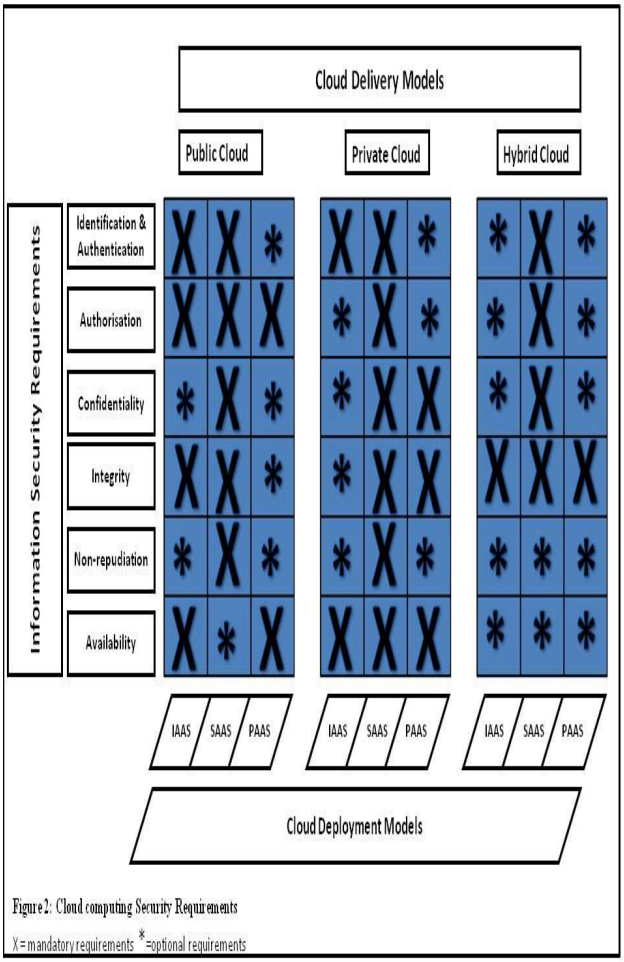

Fig2 shows cloud computing security requirements

There exist four deployment models in cloud architecture, which are described below:

Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

Community cloud. This kind of cloud has been developed for sharing data by several organizations and supports a specific community which has common things such as mission, security requirements, and policy and compliance considerations). This kind of cloud is managed by a third party or an organization it may exist either on or off premise

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (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) [7].

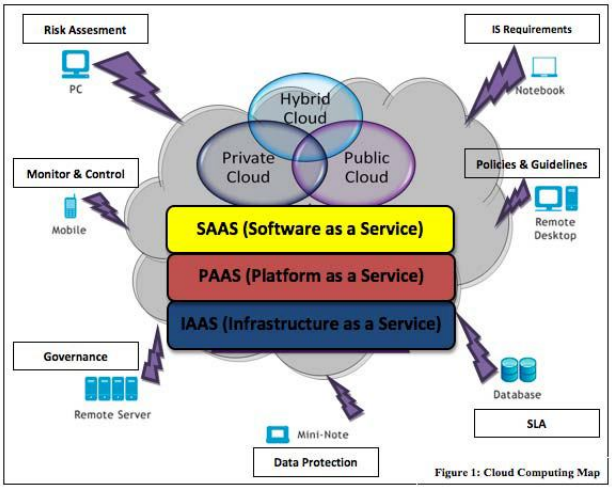

Fig 3shows deployment models in cloud

A number of key characteristics of cloud computing has been identified.

Flexibility/Elasticity: cloud users can utilize the computing recourses without any human interaction; this facility can be done either rapidly or slowly and can be either increased depending on the number or users or can be either decreased on requirement.

Scalability of infrastructure: nodes can be either added or terminated depending on the requirement with slight modifications to infrastructure set up and software. Cloud architecture can be scaled either horizontally or vertically depending on the requirement.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms (e.g., mobile phones, laptops, and PDAs).

Location independence: There is a sense of location independence, in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).

Reliability: cloud can be accessed from multiple sites, which makes cloud to be suitable for business community and disaster recovery.

Economies of scale and cost effectiveness: Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located close to cheap power stations and in low-priced real estate, to lower costs.

ARCHITECTURE OF CLOUD COMPUTING

Cloud computing Architecture: A Cloud Architecture consists of certain types of entities, according to NIST which are labeled as below:
Consumer: This could be a bank or any other consumer that would avail of services on the cloud.
Provider: This would be a system integrator who would integrate offerings from multiple parties to provide a solution and sign contracts with cloud consumers. These parties would be (a) Data center and hardware provider (b) Infrastructure (software) providers (c) Virtualization (software) providers (d) Application providers and optionally (e) Network provider

Auditor: This could be a reputed audit firm who can conduct an independent security, data privacy and performance audit of operational processes and deployment infrastructure. The scope of the audit could include banking aspects depending on the charter, which could be specified

Broker: These parties would provide value added services using aggregation or arbitration on the top of business services provided by cloud providers.

Carrier: This would be the provider of network infrastructure to connect various bank branches to the data center.

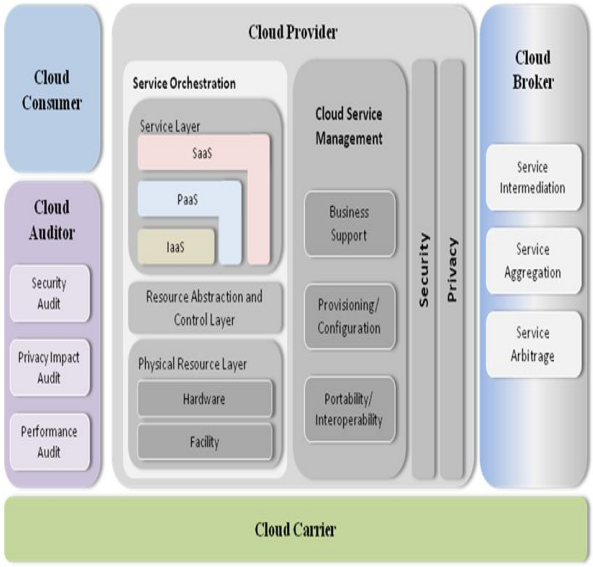

Fig 4 shows cloud architecture

Cloud services helps consumer to outsource the maintenance burden of servers and applications; scale systems up or down on demand; being able to access data from anywhere with a network connection; and the ability to replace occasional heavy capital expenditure (CAPEX) on IT with regular and predictable operational expenditure (OPEX). Cloud computing is evolving technology and will contain flaws, experience failures, and experience security compromises.

THREATS IN CLOUD COMPUTING

There has aroused a number of security issues from tradition computing to cloud computing which may be classified into physical and cyber security.

Physical security: They deal with the physical properties of the system such as data centre, which is owned by the infrastructure provider, who has to maintain the security standards and hold security certifications globally, supervision manageability on security preventions, in combustibility, uninterrupted power supplies, precautions for natural disasters etc.

Cyber security: they deal with the protection of the system from cyber world, many of the cloud computing services are being affected by the cyber attacks, during these attacks large amount of computing resources are utilized due to which consumer is disabled from the computing services. Many of the commonly found attacks are discussed

Insider attack: entrepreneur, employee and associates who accesses the cloud and the whole information system are termed to be insiders; they are organized and run by these individuals to harm or damage knowledge about consumers.

Flooding attack: here the attacker sends very large amounts of packets from exploited information resources, which are termed as zombies.

User to root attacks: in this kind of attack an intruder steals the password and gains the access of the authorized user and gets access to the whole system [8]

Port scanning: in this kind of attack first open and closed filtered ports are identified on the system. With the help of port scanning intruders can stop information with the help of open ports like MAC and IP addresses which belong to a connection, various which run on the system

Virtualization attacks: in virtual environment virtual machines will be captured after the compromisation of hypervisor.

Backdoor channel attacks: here the intruders get in contact with the node in the cloud and they use this node as zombie resource to execute a DDoS attack

Storage allocation and multitenancy: processing of data in the cloud is related to certain issues [9], isolation of data and service level agreement should be realized by the providers.

Authorization and authentication: deployment of virtual machines, resources, and IP addresses are dynamic in cloud computing compared to conventional information technologies. Along with synchronization, authorization, authentication and identity management have to be configured, while achieving this data privacy is also indispensable.

Data modification, forgery and integrity: to gain their own benefit some untrusted providers and system administrators can manipulate data related to authorized

users and consumers [10], due to these real users has to face a lot of problems, with the help certain kinds of encryption techniques these kinds of attacks can be overcome.[11][12].

Table 1 shows various threats that are observed at various levels and there effects

level	Service level	Users	Security requirements	threats
Application level	Software as a Service (SaaS)	End client applies to a person organization who subscribes to a service offered by a cloud provider and is accountable for its use	• Privacy in multitenant environment • Interception • Data protection from exposure (remnants) • Modification of data at rest and in transit • Access control • Data interruption (deletion) • Communication protection • Privacy breach • Software security • Impersonation • Service availability	Interception Modification of data at rest and in transit. Data interruption Privacy breach Impersonation Session hijacking Traffic flow analysis Exposure in network
Virtual level	Platform as a service Infrastructure as a service	Developer moderator applies to a person or organization that deploys software on a cloud infrastructure.	• Access control • Application security • Data security • Cloud management control security • Secure images • Virtual cloud protection	Programming flaws Software modification Software interruption Impersonation Session hijacking Traffic flow analysis Exposure in network Connection flooding
Physical level	Physical data center	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed.	• Legal not abusive use of cloud computing. • Hardware security • Network protection • Network resources protection.	Network attacks Connection flooding DDOS Hardware interruption Hardware theft

VARIOUS IDS/IPS IN CLOUD : As there are different kind of attacks in the cloud to overcome them, Intrusion Detection Systems (IDS) are considered to the practical solution to resists these attacks. These intrusion detection systems may be either hardware or software including the computing entities, These systems realize intrusion detection, log detected information, either they alert or perform predefined procedures [13,14]. Every suspicious detected entity cannot be termed as an intrusion, sometimes unexpected events may also occur so it is important to decide whether they are intruders or not. There exist mainly three types of IDS, which are given as Network based IDS, Host based IDS and Distributed based IDS.

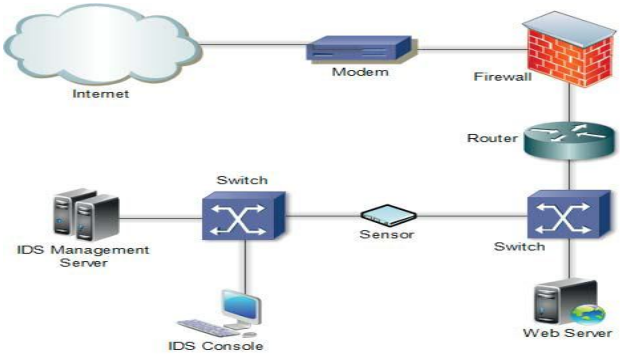

Fig5 shows network based intrusion detection system

A. *Network Based Intrusion Detection System :*An NIDS is an intrusion detection system where unauthorized access of a network is detected by analyzing the network traffic for signs of malicious activities and events. Network traffic is collected on different layers where each layer delivers the data coming from a layer to another layer. With the help of OSI reference model and TCP/IP model one can define the working of these layers, an example of NIDS is shown above.

***B. Host based intrusion detection system*:** In these systems sensors are located on servers and workstations in order to protect the attacks on the host, these systems to protect private and valuable information on server systems. These systems analyze suspicious activities like system call, processes or thread, asset and configuration access with the help of observation of situation of the host. It not only monitors traffic but also traces out more and settles with local settings of an OS and log records, its representation is shown as below.

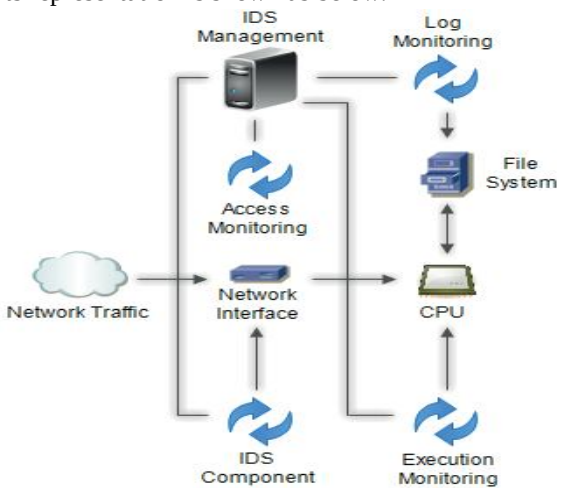

Fig 6 shows host based intrusion detection system

c. Distributed Intrusion Detection systems : It is a way of intrusion detection in a distributed environment such as grid or cloud computing [15]. The components in the distributed area establish communication between them with an agent based approach. DIDS deals the whole system like a traditional network or host [16]. DIDS representation is shown in the diagram.

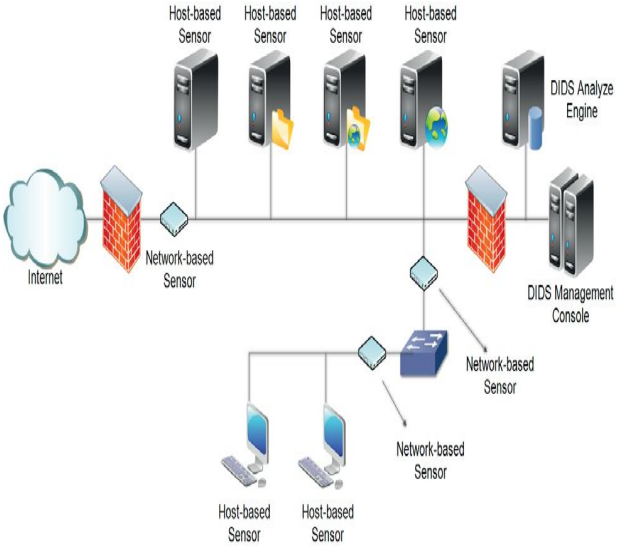

Fig 7shows Distributed Intrusion Detection system

Table 2 shows summary of IDS/IPS Techniques

IDS/IPS Technique	Characteristics / Advantages	Limitations / Challenges
Misuse detection	• Identifies intrusion by matching captured patterns with Preconfigured knowledge base. • High detection accuracy for previously known attacks. • Low computational cost.	• Cannot detect new or variant of known attacks. • Knowledge base for matching should be crafted carefully. • High false alarm rate for unknown attacks.
Anomaly detection	• Uses statistical test on collected behaviour to identify intrusion. • Can lower the false alarm rate for unknown attacks.	• Lot of time required to identify attacks. • Detection accuracy is based on amount of collected behaviour or features.
ANN based IDS	• Classifies unstructured network packet efficiently. • Multiple hidden layers in ANN increase efficiency of classification.	• It requires lot of time at training phase. • Large number of samples required for training effectively. • Has lesser flexibility.
Fuzzy Logic based IDS	• Used for quantitative features. • Provides better flexibility to some uncertain problems.	• Detection accuracy is lower than ANN.
Association rules	• Used to detect known attack	• It cannot be used for totally unknown

based IDS	signature or relevant attacks in misuse detection.	attacks. • It requires more number of database scans to generate rules. • Used only for misuse detection.
Hybrid Techniques	• It is an efficient approach to classify rules accurately.	• Computational cost is high.
SVM based IDS	• It can correctly classify intrusions, if limited sample data are given. • Can handle massive number of features.	• It can classify only discrete features. So , preprocessing of those features is required before applying.

INTRUSION PREVENSTION SYSTEMS

IPS holds all capabilities of IDS and also prevention characteristics along with them, in a nutshell security of a system has some traditional steps, there will be a firewall IDS, IPS and guard the system from behind modem, router or switches where ever it is needed. or a virtual machine can be isolated among security procedures On the detection of an intrusion a firewall rule is applied, routing configuration can be changed

CONCLUSION

Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues The main objective of our study is to provide the cloud computing users aware of the various commonly occurring threats and there effects and possible Measures in order to overcome these threats and at the same time introducing various IDS/IPS they play an important role in order to find the threats and methods in order to unable the effects of these threats at least to certain minimal level . We hope that our work would be useful for better understanding of the challenges and pave a way for further research in this area.

REFERENCES

[1]. NIST Definition of Cloud Computing v15, rc.nist.gov /groups/ SNS/cloud-computing/cloud-def-v15.doc.
[2] Amazon Elastic Computing Cloud, aws.amazon.com/ec2
[3] Cloud Hosting, CLoud Computing and Hybrid Infrastructure from GoGrid, http://www.gogrid.com
[4] FlexiScale Cloud Comp and Hosting, www.flexiscale.com
[5]Google App Engine, URL http://code.google.com/appengine
[6] Dedicated Server, Managed Hosting, Web Hosting by Rackspace Hosting, http://www.rackspace.com.
[7] S. Meena, E. Daniel and N. A. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," *Proc. International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2013, pp. 1076-1081.
[8] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud,"Journal of Network and Computer Applications, vol. 36, no. 1, pp.42–57, January 2013
[9] M. K. Srinivasan and P. Rodrigues, "State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud," *Proc. 2nd International Conference on Advances in Computing, Communications and Informatics,"*Mysore, 2012, pp. 470-476
[10] S. Meena, E. Daniel and N. A. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," *Proc.International Conference on Circuits, Power and ComputingTechnologies (ICCPCT)*, Nagercoil, 2013, pp. 1076-1081
[11] J Kong, " Adjoint VM: a new intrusion detection model for cloud computing", Enerty Procedia vol 13, PP.7902-7911,2011
[12] U. Oktay, M. A. Aydin and O. K. Sahingoz, "Circular Chain VMProtection in AdjointVM", *Proc. The International Conference on Technological Advances in Electrical, Electronics and ComputerEngineering (TAEECE2013)*, Konya, 2013, pp. 94-98
[13] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94 (SP800-94)," Gaithersburg, February 2007.
[14] G. Tyler, "Information Assurance Tools Report Intrusion DetectionSystems," Information Assurance Technology Analysis Center (IATAC), September 2009.
[15]] R. Robbins, "Distributed Intrusion Detection Systems: An Introduction and review SANS institute information security Reading Room, GSEC Practical Assignment, version 1.4b, Option 1, January 2002
[16]] X. Qing, " The Structure Design of A new Distributed Intrusion Detection System"Detection System," *Proc. 2nd International Conference on ComputerEngineering and Technology (ICCET)*, Chengdu, 2010, pp. 100-103
[17] C. B. W. C. M. W. K. M. VIEIRA, A. SCHULTER, "Intrusion detection techniques in grid and cloud computing environment," *IEEE IT Professional Magazine*, 2010
[18] S. Roschke, C. Feng, and C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," *Fifth InternationalConference on Information Assurance and Security*, vol. 2, 2009, pp.130-134
[19] A.bakshi, and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *Second International Conference on Communication Software and Networks*, 2010, pp. 260- 264
[20] C. Mazzariello, R. Bifulco, and R. Canonoco, "Integrating a networkIDS into an Open source Cloud computing," *Sixth Internationalconference on Information Assurance and Security (IAS)*, 2010, pp. 265-270.
[21] C. C. Lo, C. C. Huang, and J. Ku, "Cooperative Intrusion Detection System Framework for Cloud Computing Networks," *First IEEEInternational Conference on Ubi-Media Computing*, 2008, pp. 280-284.
[22] K. A. B. A. V. Dastjerdi, and S. G. H. Tabatabaei, "Distributed intrusiondetection in clouds using mobile agents," *in Third InternationalConference on Advanced Engineering Computing and Applications inSciences*, 2009. ADVCOMP '09, 2009, pp. 175 – 180
[23] L. Fagui Liu, S. Xiang Su, and L. Wenqianl, "The Design and Application of Xen-based Host System Firewall and its Extension," *in The 2009 International Conference on Electronic Computer Technology*, 2009, pp. 392-395.