ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 10, December 2012

Securing Cloud from Attacks based on Intrusion Detection System

Soumya Mathew[1], Ann Preetha Jose[2]

M.E Computer Science & Engineering, Adhiyamaan College of Engineering, Tamil Nadu, India[1]

Assistant Professor, Information Technology Department, ViswaJyothi College of Engineering, Kerala, India[2]

ABSTRACT: **Cloud Computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. Because of their distributed nature, cloud computing environments are easy targets for intruders looking for possible vulnerabilities to exploit. However, with the extensive use of cloud computing, security issues came out on a growing scale. It is necessary to solve these security issues to promote the wider applications of cloud computing. To provide secure and reliable services in cloud computing environment is an important issue. Therefore, a Cloud computing system needs to contain some Intrusion Detection Systems (IDSs) for protecting each virtual machine against threats. In this case there exists a trade-off between the security level of IDS and the system performance. If the IDS provide stronger security services using more rules or patterns, then it needs much more computational resources in proportion to the strength of security. Another problem in Cloud Computing is that, it is hard to analyse huge amount of logs by system administrators. The objective of the paper is to propose a method that enables Cloud Computing System to achieve both effectiveness of using the system resources and strength of the security service without trade-off between them.**

Keywords: **Cloud Computing, Layered Intrusion Detection System, Knowledge Analysis, Behavior Analysis, Security**

I. INTRODUCTION

As Green IT has been issued, many companies have started to find ways to decrease IT cost and overcome economic recession. Cloud Computing service is a new computing paradigm in which people only need to pay for use of services without cost of purchasing physical hardware. For this reason, Cloud Computing has been rapidly developed along with the trend of IT services. Cloud Computing can be defined as internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand.

It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider. Especially, Cloud Computing has been recently more spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility. Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers. Especially, System administrators potentially can become attackers.

Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders.

IDSs are the most popular devices for protecting Cloud Computing systems from various types of attack. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally. Another important problem is log management. Cloud Computing systems are used by many people, therefore, they generate huge amount of logs. So, system administrators should decide, which log should be analyzed first.

In this paper, we propose a Multi-level IDS and log management method based on consumer behaviour and importance of service for applying IDS effectively to Cloud Computing system. The rest of this paper is organized as follows. Section II provides the background and related works about Cloud computing and IDS. Section III analyses the shortcomings of current technology, Section IV analyse requirements need to be satisfied, and describes a method proposed to solve the current problem. Section V estimates the method. Section VI with future enhancements. The paper concludes with Section 7.

II.BACKGROUND

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer.

A. Cloud Computing

Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than an entirely new type of computing technique. Cloud computing has evolved through a number of implementations. Moving data into the cloud provides great convenience to users. Cloud computing is a collection of all resources to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications. The characteristics of cloud computing includes: virtual, scalable, efficient, and flexible. In cloud computing, three kinds of services are provided: Software as a Service (SaaS) systems, Infrastructure as a Service (IaaS) providers, and Platform as a Service (PaaS). In SaaS, systems offer complete online applications that can be directly executed by their users; In IaaS, providers allow their customers to have access to entire virtual machines; and in SaaS, it offers development and deployment tools, languages and APIs used to build, deploy and run applications in the cloud.

B. Threats in Cloud

A cloud is subject to several accidental and intentional security threats, including threats to the integrity, confidentiality and availability of its resources, data and infrastructure. Also, when a cloud with large computing power and storage capacity is misused by an ill-intentioned party for malicious purposes, the cloud itself is a threat against society. Intentional threats are imposed by insiders and external intruders. Insiders are legitimate cloud users who abuse their privileges by using the cloud for unintended purposes and we consider this intrusive behaviour to be detected. An intrusion consists of an attack exploiting a security flaw and a consequent breach which is the resulting violation of the explicit or implicit security policy of the system. Although an intrusion connotes a successful attack, IDSs also try to identify attacks that don't lead to compromises. “Attacks” and “intrusions” are commonly considered synonyms in the intrusion detection context. The underlying network infrastructure of a cloud, being an important component of the computing environment, can be the object of an attack. Grid and cloud applications running on compromised hosts are also a security concern. We consider attacks against any network or host participating in a cloud as attacks against that, since they may directly or indirectly affect its security aspects. Cloud systems are susceptible to all typical network and computer security attacks, plus specific means of attack because of their new protocols and services. The targets that are possibly vulnerable are the protocol stack; network devices; processes running in kernel space, such as operating system daemons; and processes running outside kernel space, such as cloud middleware, cloud applications, and any non-cloud applications running with either root or user privileges. Classification of cloud intrusions is given as follows:

1) Unauthorized Access: A break-in committed by an intruder that masquerades as a legitimate cloud user. It is made possible by obtaining the user’s password through stealing, brute-force cracking, guessing, or the careless exposure by the user himself. Attacking the authentication service is another possibility, and this may result in attack trails left at the service location.

2) Misuse: This may be a consequence of an unauthorized access or the abuse of privileges by a legitimate user (insider) and generally results in an observable user behaviour anomaly. The misuse of cloud resources depends on the defined policies, and those should consider aggressive utilization, user mistakes and malicious usage.

3) Cloud Attack: Attacks performed with the help of tools or exploit scripts that target vulnerabilities existent in cloud protocols, services and applications. They may appear in the form of denial-of-service attacks, probes, and worms, and may leave their trails at several locations of cloud’s infrastructure.

4) Data Security: Data of "Cloud" is stored in different physical locations, in various parts of the Earth, in the absence of corresponding technical and regulatory constraints; data security is difficult to get protection. First of all, different places have different levels of technology, some advanced and some behind. Data is safe somewhere, but there may be some risk in another place. Secondly, there are different regulations in different places.

5) Flash Crowds: Sudden increase in the number of (legitimate) clients. Cloud computing systems are used by many people, therefore, they generates huge amount of logs. Huge amount of log makes IDS hard to analyse them and also time consuming. This in turn reduces system effectiveness. Intrusions in cloud distributed systems are potentially greater in speed, consequences, and damages.

C. Intrusion Detection System

IDSs are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analysing them for signs of security problems. IDSs are one of widely used security technologies. An IDS alerts to system administrators, generate log about attack when it detects signature of accident according to host or network security policy. IDS can be installed in a host or a network according to purpose. Thus, the aim of the IDS is to alert or notify the system that some malicious activities have taken place and try to eliminate it.

According to the method of the collection of intrusion data, all the intrusion detection systems can be classified into two types: host-based and network-based IDSs. Host-based intrusion detection systems (HIDSs) analyse audit data collected by an operating system about the actions performed by users and applications; while network-based intrusion detection systems (NIDSs) analyse data collected from network packets.

IDSs analyse one or more events gotten from the collected data. According to analysis techniques, IDS system is classified into two different parts: misuse detection and anomaly detection. Misuse detection systems use signature patterns of exited well-known attacks of the system to match and identify known intrusions. Misuse detection techniques, in general, are not effective against the latest attacks that have no matched rules or pattern yet. Anomaly detection systems identify those activities which deviate significantly from the established normal behaviors as anomalies. These anomalies are most likely regarded as intrusions. Anomaly detection techniques can be effective against unknown or the latest attacks. However, anomaly detection systems tend to generate more false alarms than misuse detection systems because an anomaly may be a new normal behavior or an ordinary activity.

While IDS detects an intrusion attempt, IDS should report to the system administrator. There are three ways to report the detection results. They are notification, manual response, and automatic response. In notification response system, IDS only generates reports and alerts. In manual response system, IDS provides additional capability for the system administrator to initiate a manual response. In automatic response system, IDS immediately respond to an intrusion through auto response system.

III. RELATED WORKS

In the previous section we described five kinds of intrusions that may violate cloud security: (a) unauthorized access, (b) misuse, (c) cloud attack (d) data security, and (e) flash crowds. To avoid unwanted consequences of these intrusions, typical host-based and network-based IDSs can be deployed in a cloud environment and provide protection against attacks that explore vulnerabilities in its nodes (hosts) and networks. This solution is not complete, as it provides protection against host and network-specific intrusions but not against cloud specific intrusions. The signature database of typical IDS scan be updated to identify trails of (a) unauthorized accesses and (c) cloud attacks left at hosts and network packets. This is not a complete solution either, because (c) cloud attacks may leave trails at more than one location and they may become evident only by correlating the trails identified by the IDSs. Furthermore, a HIDS is unable to properly detect grid and cloud users committing (b) misuse, because they analyse the behavior of users in their local contexts and since grid and cloud users are allowed to use multiple resources from different domains at the same time or consecutively, the analysis must be done in the scope of the cloud as a hole. Therefore, a different approach to the problem is needed to overcome the deficiencies. The need for grid-based intrusion detection systems was first mentioned in although solutions to the problem were not described. An efficient and scalable solution for storing and accessing audit data collected from cloud nodes was proposed [3], but there was no mention on how to use the data to identify intrusions. It describe a cloud based IDS architecture that consists of agents located at nodes responsible for collecting and sending host audit data to storage and analysis servers, but since IDSs are known to consume considerable processing time and storage space, their centralized solution is not scalable with the number of nodes under analysis.

The Intrusion Detection Architecture proposed in [4] solves the scalability problem by distributing the intrusion detection problem among several analysis servers. Both [3] and [4] concentrate on the detection of anomalies in the interaction of cloud users with resources, which is the result of (b) misuse. But they lack proper detection of (a) unauthorized accesses and (c) cloud attacks, and (e) flash crowds. Furthermore, none of the architectures aim to provide protection against (e) flash crowds. In [5], they proposed an IDS called Performance-based Intrusion Detection System in which nodes are allocated through load balancing to analyse collected network traffic and search for network denial-of service attacks. The system uses a cloud's abundant resources to detect intrusion packets, but it does not detect attacks to the cloud itself and it only looks for network attacks, therefore it acts as a NIDS, rather than. The shortcomings of the available solutions motivate to propose new approach .The problem is further analysed in the next section.

IV. PROPOSED APPROACH

A. Problem Analysis

Cloud intrusion detection is a process that involves the gathering of information available at its networks and nodes (host computers), and the identification, based on the evaluation and correlation of the gathered data, of attacks against all the possible vulnerable targets, as well as anomalies in the interaction of cloud users with resources. Some considerations when deploying IDS for protecting each individual VM in Cloud Computing system are as follows. First, the security problems bring much more economic loss in Cloud Computing than in the other kind of systems. Second, in Cloud Computing systems, it is difficult to analyse logs because communication between many system and many consumers generate large amount of logs. Finally, Cloud Computing services are to provide their resource to consumers, therefore effective resource management is greatly desirable. As discussed in the Section III, current intrusion detection technology fails to provide protection against all the intrusions that may violate cloud security. We believe the following three basic requirements need to be satisfied by a cloud based intrusion detection system: They are (i) Coverage: must provide detection of (a) unauthorized access, (b) misuse, (c) cloud attack, (d) data security and (e) flash crowds (Section II); (ii) Scalability: must be scalable with the number of cloud resources and users; (iii) Cloud compatibility: must suit and benefit from the cloud environment. While current solutions to the cloud intrusion detection problem aim to satisfy the requirements of (y) scalability [3][4]; and (z) cloud compatibility [3][4], they lack in (x) coverage. Next sub-section describes the proposed solution which aims to satisfy these three requirements.

B. Integrated Intrusion Detection System

The proposed solution is a Multi-layer integrated IDS for implementing effective IDS in cloud computing system. This IDS service increases a cloud's security level by applying two methods of intrusion detection. This IDS integrates knowledge and behavior analysis to detect cloud specific intrusions. The behavior-based method dictates how to compare recent user actions to the usual behavior. It also uses a multi-layer IDS method lead to efficient system performance by a method that binds each user to different security group. The knowledge-based method detects known trails left by attacks or certain sequences of actions from a user who might represent an attack. The two intrusion detection techniques are distinct. The knowledge-based intrusion detection is characterized by a high hit rate of known attacks, but it's deficient in detecting new attacks. Therefore it is complemented it with the behavior based technique, which can discover deviations from acceptable use and thus help identify privilege abuse.

1) Behavior Analysis: Numerous methods exist for behavior-based intrusion detection, such as data mining, artificial neural networks, and artificial immunological systems. We use a feed-forward artificial neural network, because—in contrast to traditional methods—this type of network can quickly process information, has self-learning capabilities, and can tolerate small behavior deviations. These features help overcome some IDS limitations. Using this method, we need to recognize expected behavior (legitimate use) or a severe behavior deviation. Training plays a key role in the pattern recognition that feed-forward networks perform. The network must be correctly trained to efficiently detect intrusions. For a given intrusion sample set, the network learns to identify the intrusions using its back propagation algorithm. However, we focus on identifying user behavioural patterns and deviations from such patterns. With this strategy, we can cover a wider range of unknown attacks.

2) Knowledge Analysis: Knowledge-based intrusion detection is the most often applied technique in the field because it results in a low false-alarm rate and high positive rates, although it can't detect unknown attack patterns. It uses rules (also called signatures) and monitors a stream of events to find malicious characteristics. Using an expert system, we can describe a malicious behavior with a rule. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones. In contrast, behavior-based analysis is performed on learned behavior that can't be modified without losing the previous learning. Generating rules is the key element in this technique. It helps the expert system to recognize newly discovered attacks.

C. Layered IDS

Although the integrated method provides completeness to the intrusion detection system, there exists a trade-off between security level of IDS and system performance. The volume of users in a cloud computing environment can be high so applying integrated approach to all users leads to performance degradation. So a layered IDS mechanism is proposed. In our paper, we divide security level into three, such as High, Medium and Low for effective IDS construction.

High level is a group which applies patterns of all known attacks and a portion of anomaly detection method when it needs, for providing strong security services. Medium-level is a group of middle grade which apply patterns of all known attacks to rules for providing comparatively strong security service. Finally, Low-level is a group for flexible resource management which applies patterns of chosen malicious attacks that occur with high frequency and that affect fatally to the system. In Multi-Layer IDS scheme [8], an IDS consumes more resource when providing higher level security, because higher level security applies more rules than lower level.

Anomaly levels of users are estimated by their behaviors during the usage of service based on saved user anomaly level in the system. Cloud Computing security system evaluates user anomaly level according to assessment criteria in table 1.

TABLE I
EVALUATION OF USER ANOMALY LEVEL

Attempt to administrator account without working time	8
Guest OS attempt to authorized memory space	7
The traffic of guest OS increases up to 500% than usual traffic	6
IP address of user terminal is changed during the usage Cloud service	6
Host OS manager attempts to access some guest OS	5
An guest OS attempts to other guest OS	5
Traffic of guest OS increases up to 300% than usual traffic	4
Administrator access some guest OS without notice	4
Login failure for 5times	3
Unlicensed IP coverage	3
Known – vulnerable port number	2
Abnormal guest OS power-off	2
Non –updated Guest OS	1

Multi-layer IDS accumulates risk point to each user when they are against more than one rule in assessment rules. Cloud Computing system deploys each VM to one of three security group. When a user is assigned a VM by the system first time, there is no data for determining which security layer of IDS is suitable for the user, so a high-layer IDS should be assigned to the user. Since first provisioning, the decision of which VM is to be assigned to the user may change according to anomaly level of the user, and a migration may occur. Migration is a technique to move VM to other VM space. In the case of existing users, they are judged by previous personal usage history, and assigned VMs with the security layer derived by the judgment. Cloud Computing system checks users' behaviors every day and decreases 1 risk point if a user uses Cloud Computing service more than one hour and increases less than 3 risk points a day. So many people would use Cloud Computing service, so the huge logs arise from transaction between systems, user information update, and mass data processing and so on. Therefore, it is very difficult to analyze using the logs in emergency. To make analyzing log better, we propose the method that divides log priority according to security level [8]. The criteria of anomaly level for deciding security group with risk point is shown in table 2.

TABLE II
CRITERIA OF ANOMALY LEVEL

IDS Group	**Risk Point**
High Layer IDS	More than 6
Medium Layer IDS	3-5
Low Layer IDS	0-2

In proposed solution, approach to the problem is in a different way, especially in regards to the threats system try to defend against by combining two distinct auditing techniques. They are behavior-based method and knowledge-based method. It also uses a multi-layer IDS method lead to effective resource usage by a method that binds users to different security groups in accordance with degree of anomaly, called anomaly level. Thus in proposed solution (i) Layered Intrusion Detection is introduced for efficient log management and (ii) Integrates Knowledge and Behavior analysis to improve Intrusion detection in cloud.

Initially the data is analyzed by performing risk assessment. The analyzed data is sent to the IDS service core, which analyzes the behavior using artificial intelligence to detect deviations. Based on the risk assessment performed, it is easy to identify in which layer the user belongs to. This is done by checking the criteria of user's anomaly level. The proposed system uses a feed-forward artificial neural network, because in contrast to traditional methods this type of network can quickly process information, has self-learning capabilities, and can tolerate small behaviour deviations.The analyzer uses a profile history database to determine the distance between a typical user behavior and the suspect behavior and communicates this to the IDS service. The rules analyzer receives audit packages and determines whether a rule in the database is being broken. It returns the result to the IDS service core.

With these responses, the IDS calculate the probability that the action represents an attack and alerts the other nodes if the probability is sufficiently high. Behavior-based method can cover a wider range of known and unknown attacks. In Knowledge based intrusion detection we can add new rules without losing or modifying the existing ones. Thus proposed system offers complete layered and integrated IDS. The workflow of the proposed System is shown in the figure1.

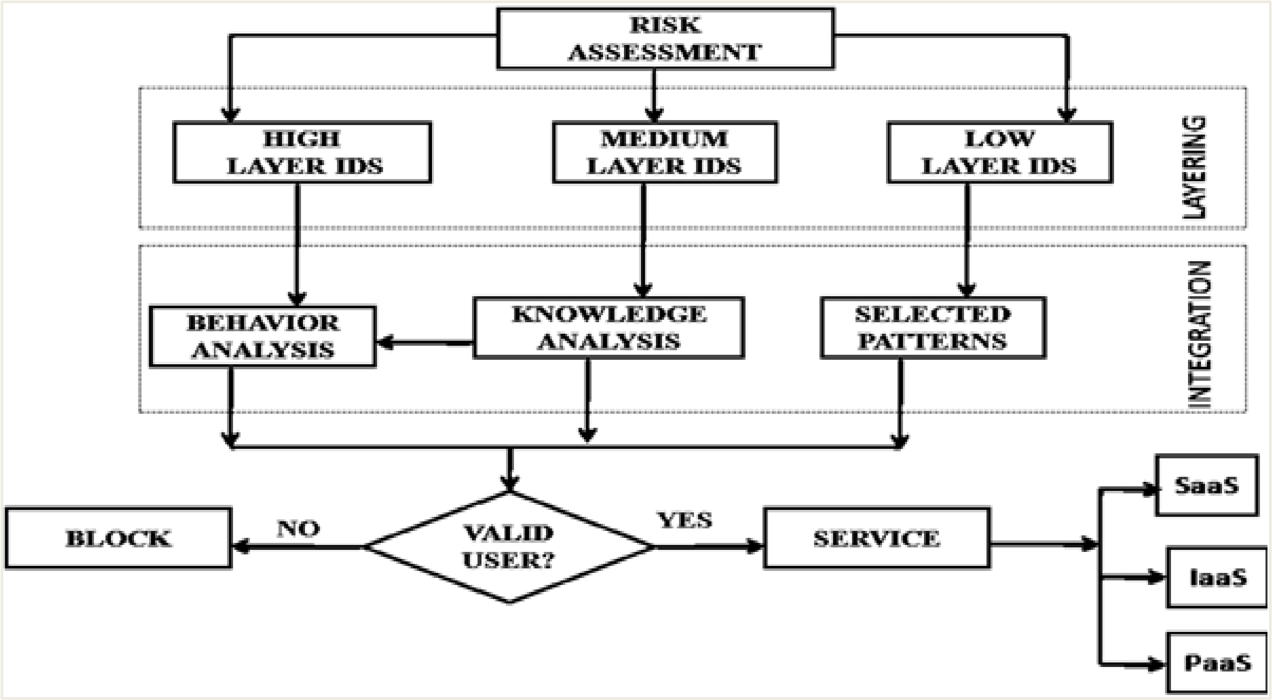

Fig. 1 Workflow of the proposed system

V. ESTIMATION

In this paper, we created a series of rules to illustrate security policies that IDS can monitor. The method increases resource availability of Cloud Computing system and handle the potential threats by deploying Multi-layer IDS and managing user logs per group according to anomaly level. We can suppose that VMs have equal quantity of resource, then host OS can assign less guest OS with IDS, because IDS use much resource.

On the other hands, we can assign more guest OS with Multi-layer IDS, because medium layer and low-layer IDS use less resource. The users classified as high-layer group are potentially dangerous user, therefore a high-layer IDS consumes much resource to detect all of anomalous behaviours. However, a low layer IDS consumes less resource, because the user classified as low-layer group are judged that they are normal user. As a result, low-layer IDSs maintain little rules for managing effective resource, so it can assign more guest OS than high and medium-layer. Our method also supports classifying the logs by anomaly level, so it makes system administrator to analyse logs of the most suspected users first. Therefore our method provides high speed of detecting attacks.

VI. FUTURE ENHANCEMENTS

In the future, we'll implement our IDS, helping to improve green (energy-efficient), white (using wireless networks), and cognitive (using cognitive networks) cloud computing environments. We also intend to research and improve the security features in cloud computing environment.

VII.CONCLUSION

Facing the complexity of Cloud architecture, this paper focuses on proposing deployment architecture of Intrusion Detection Systems in the Cloud. We discuss and list several existing threats for a Cloud infrastructure and are motivated to use Intrusion Detection Systems (IDS) and its management in the Cloud. We propose the deployment of integrated and layered IDS on cloud that designed to cover various attacks. This IDS integrates knowledge and behavior analysis to increases a cloud's security. The two intrusion detection techniques are distinct. But the deficiency of one technique will be complimented by other one. Layered IDS offers effective resource and log management.

ACKNOWLEDGMENT

At the outset I whole heartedly thank the Almighty, who has been my strength in times of weakness and hope in time of despair, the sole creator of all the creations in this world and hence this paper. I thank my parents and guardian who have encouraged me with good spirit by their incessant prayers to complete this paper. I would like to express my sincere thanks to our department for providing me various formalities needed for successful completion of my project. It is my deep sense of gratitude and honor to acknowledge sincere thanks to my internal guide Prof. E. Saravanakumar, for his valuable directions, suggestions and exquisite guidance with enthusiastic encouragement ever since the commencement of the project. I am indebted to my external guide Mrs.Ann Preetha Jose, Asst.Professsor of IT Department, VJCET for her keen interest shown by her in my project and comforting words of encouragement offered by her from time to time.

REFERENCES

[1] H. Debar, M. Dacier, and A. Wespi, "Towards a Taxonomy of Intrusion Detection Systems," Int'l J.Computer and Telecommunications Networking, vol. 31, no. 9, pp. 805–822, 1999.

[2] S. Axelsson, Research in Intrusion-Detection Systems: A Survey, tech. report TR-98-17, Dept. Computer Eng.,Chalmers Univ. of Technology, 1999.

[3] S. Kenny and B. Coghlan, "Towards a Grid-Wide Intrusion Detection System," Proc. European Grid Conf. (EGC 05), Springer, pp. 275–284,2005.

[4] M. Tolba et al., "Distributed Intrusion Detection System for Computational Grids," Proc. 2nd Int'l Conf. Intelligent Computing and Information Systems (ICICIS 05), 2005.

[5] F-Y. Leu et al., "Integrating Grid with Intrusion Detection," Proc. Int'l Conf. Advanced Information Networking and Applications (AINA 05), IEEE CS Press, vol. 1, pp. 304–309,2005.

[6] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud".

[7] Vieira, K. Schulter, A. Westphall, C.B. Westphall, C.M. "Intrusion Detection for Grid and Cloud Computing" IEEE computer society, vol 12, issue 4, pp. 38 – 43,2010.

[8] Jun Ho Lee, Min Woo Park, Jung Ho Ecom"Multi-level Itrusion Detection and Log Management in Cloud Computing" IEEE computer society, pp 552-555, Feb.2011.

[9] Gruschka N, Iancono LL, Jensen M and Schwenk J, 'On Technical Security Issues in Cloud Computing', '09 IEEE International Conference on Cloud Computing, pp 110-112, 2009.

[10] Ramgovind S.Eloff MM,Smith E,"The Management of Security in Cloud Computing",School of Computing,university of South Africa,Published in the IEEE international conference on 2010.

[11] H. Takabi, J. B. D. Joshi and G. Ahn, Security and Privacy Challenges in Cloud Computing Environments, Security & Privacy, IEEE, 8 , pp. 24-31,2010.

[12] Wang xin,Huang ting-lei,Liu Xiao-yu,"Research on the Intrusion Detection Mechanism based on Cloud Computing",published in International journal on Infrastructures for Collaborative Enterprises.on 2010.

[13] Chi-Chun Lo,Chun-Chieh Huang,"A Cooperative Intrusion Detection System Framework for cloud Computing Networks" on 39th International Conference on Parallel Processing,2010.