International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012
Proceedings published by International Journal of Computer Applications® (IJCA)

Intrusion Detection System in Cloud Computing Environment

S.V. Narwane
Department of Computer Engineering.
Mumbai University
Mumbai, Airoli(Navi Mumbai)

S. L. Vaikol
Department of Computer Engineering
Mumbai University
Mumbai, Airoli(Navi Mumbai)

ABSTRACT

The Cloud computing system can be easily threatened by various attacks, because most of the cloud computing systems provide service to so many people who are not proven to be trustworthy. Due to their distributed nature, cloud computing environment are easy targets for intruders[1]. There are various Intrusion Detection Systems having various specifications to each. Cloud computing have two approaches i.e. Knowledge-based IDS and Behavior-Based IDS to detect intrusions in cloud computing. Behavior-Based IDS assumes that an intrusion can be detected by observing a deviation from normal to expected behavior of the system or user[2]s. Knowledge-based IDS techniques apply knowledge accumulated about specific attack . Knowledge-based IDS can't detect unknown attacks, but it uses rules and monitors a stream of event s to find malicious characteristics and set the new rules for unknown attacks. In this paper we proposed a system is to detect intrusions in the cloud computing using Behavior-based approach and knowledge-based approach. If first approach unable to detect the data, second approach again verifies the data and compare it with the signatures within the database. In the proposed system definitely we will have very low false positive alarm.

Keywords

Behavior –based intrusion detection, Cloud computing, Intrusion detection system (IDS),
Knowledge-based intrusion detection, Eucalyptus .

1. INTRODUCTION

Cloud Computing is becoming one of the next industry buzz words. Cloud computing builds upon advance of research in virtualization, distributed computing, grid computing and utility computing. Cloud computing is a collection of all sources to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications. In past three decades, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Location of data and IDSs are auditing engines, so models of auditing system can describe their architecture[7]. The director or analysis engine, may be centralised or distributed or may be hierarchical or fragmented. Information may be gathered from hosts, from network, from both or from other directors. When an intrusion occurs some response is appropriate. If the intrusion attempt is detected before the attack is successful, the system can take the action to prevent the attack from succeeding.

An IDS inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attacks from someone attempting to break into or compromise a system[7].

Processes makes the difference in the realm of computation. On one hand, an individual has full control on data and processes in his/her computer. On the other hand, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. The Cloud computing system can be easily threatened by various attacks, because most of the cloud computing systems provide service to so many people who are not proven to be trustworthy. Due to their distributed nature, cloud computing environment are easy targets for intruders looking for possible vulnerabilities to exploit. Cloud computing have two approaches i.e. Knowledge-based IDS and Behavior-Based IDS to detect intrusions in cloud computing.

Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion detection system might be

complete (i.e. all attacks should be caught), but its accuracy is a difficult issue (i.e. you get a lot of false alarms)[6].

Knowledge-based intrusion detection techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. The intrusion detection system contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities. When such an attempt is detected, an alarm is triggered. In other words, any action that is not explicitly recognized as an attack is considered acceptable [6].

In this paper we proposed a system to detect intrusions in cloud computing environment. Intrusions are detected with the help of Knowledge-based and behavior-based approaches where knowledge-based approach uses signatures (evidences of attacks) and behavior-base approach uses set of normal activities to check abnormality.

The rest of the paper organized as follows. Section 2 describes various attacks in cloud computing. In section 3, Eucalyptus (software tool for cloud computing) is described. Section 4 described the proposed IDS and section 5 gives a short summary.

2. CLOUD COMPUTING ATTACKS

We will focus on specific problems for various kinds of attacks in the cloud [5]:

a) Wrapping attack
b) Malware Injection attack
c) Flooding attack
d) Data stealing problem
e) Accountability checking.

Some details of above attacks are as follows –

2.1 Wrapping Attack Problem:

When a user makes a request from his VM through the browser, the request is first directed to the web server. In this server, a SOAP message is generated. This message contains the structural information that will be exchanged between the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed and canonicalization has to be done. Also, the signature values should be appended with the document. Finally, the SOAP header should contain all the necessary information for the destination after computation is done [5]. For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is duplicated and sent to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers [5].

2.2 Malware-Injection Attack Problem:

In a malware injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. This can be accomplished via subtle data modifications to change the functionality, or causing deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. Here the attacker takes his first step by implementing his malicious service in such a way that it will run in Iaas or SaaS of the cloud servers, for example as mentioned in Section I, with deleteUser and setAdminRights. This type of attack is also known as a meta-data spoofing attack [5].When an instance of a legitimate user is ready to run in the cloud server, then the respective service accepts the instance for computation in the cloud. The only checking done is to determine if the instance matches a legitimate existing service. However, the integrity of the instance is not checked. By penetrating the instance and duplicating it as if it is a valid service, the malware activity succeeds in the cloud [5].

2.3 Flooding Attack Problem:

In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar servicespecific server to offload itself. This sharing approach makes the cloud more efficient and faster executing requests [5]. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Because non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to a great extent. While processing these requests, legitimate services can starve, and as a result the server will offload its services to another server. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system [5].

2.4 Data Stealing Problem:

This is the most traditional and common approach to breach a user account. The user account and password are stolen by any means. As a result, the subsequent stealing of confidential data or even the destroying of data can hamper

the storage integrity and security of the cloud. The providers face the first strike of such kind of problem [5].

2.5 Accountability Check Problem:

The payment method in a cloud System is "No use No bill". When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. So, when an attacker has engaged the cloud with a malicious service or runs malicious code, which consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation. Though the customer is not aware of the attack and until the main cause of the CPU usage is detected, the providers will charge the customers first. As a result, a dispute arises and business reputations are hampered. All the focus for charging is based on the recorded parameters [5].

3. CLOUD COMPUTING PLATFORM

3.1 Eucalyptus

For cloud computing platform we have software tool named as Eucalyptus. Eucalyptus is open source software for cloud environment. Ubuntu community released Eucalyptus for Cloud Computing. Since version 1.5 Eucalyptus has been included in Ubuntu and is now the core element of the Ubuntu Enterprise Cloud (UEC). Since version 1.6.2 Eucalyptus has been included in Debian. In May 2011 Canonical decided to switch from Eucalyptus to OpenStack starting from Ubuntu 11.10. Support for Eucalyptus will be available, but OpenStack will be the default [6].

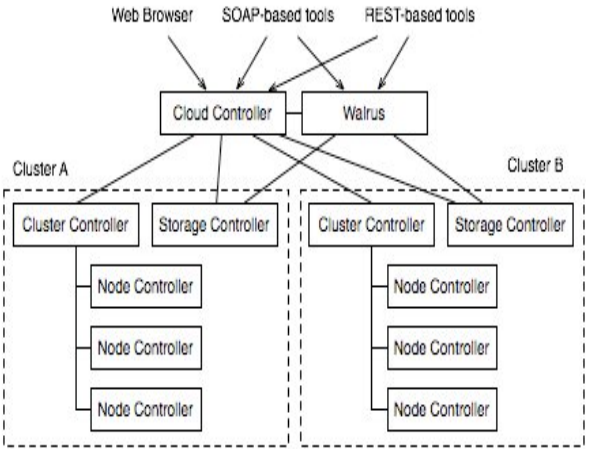

Fig. 3.1: Eucalyptus software architecture

The Eucalyptus cloud computing platform has five high-level components: Cloud Controller (CLC), Cluster Controller (CC), Walrus, Storage Controller (SC) and Node Controller (NC). Each high-level system component has its own Web interface and is implemented as a stand-alone

Web service. This has two major advantages: First, each Web service exposes a well-defined language-agnostic API in the form of a WSDL document containing both the operations that the service can perform and the input/output data structures. Second, Eucalyptus leverages existing Web-service features such as security policies (WSS) for secure communication between components and relies on industry- standard web-services software packages [6].

3.2 Eucalyptus Components [6]:

- Cloud Controller (CLC) - The CLC is responsible for exposing and managing the underlying virtualized resources (machines (servers), network, and storage) via user-facing APIs. Currently, the CLC exports a well-defined industry standard API (Amazon EC2) and via a Web-based user interface.
- Walrus - Walrus implements scalable "put-get bucket storage." The current implementation of Walrus is interface compatible with Amazon's S3 (a get/put interface for buckets and objects), providing a mechanism for persistent storage and access control of virtual machine images and user data.
- Cluster Controller (CC) - The CC controls the execution of virtual machines (VMs) running on the nodes and manages the virtual networking between VMs and between VMs and external users.
- Storage Controller (SC) - The SC provides block-level network storage that can be dynamically attached by VMs. The current implementation of the SC supports the Amazon Elastic Block Storage (EBS) semantics.
- Node Controller (NC) - The NC (through the functionality of a hypervisor) controls VM activities, including the execution, inspection, and termination of VM instances.

4. PROPOSED INTRUSION DETECTION SYSTEM

In the cloud computing every user is unknown and detection of the authorized and unauthorized user is also very difficult, as cloud computing is virtual centralization. We can also say that detection of user's behavior is also difficult. Due to this cloud computing provide services along with some terms and conditions. While user will request for the service Cloud Service Provider (CSP) provides authentication for the user. i.e. CSP provide username and password to the user for accessing services of the cloud. It may possible that any authorized user can also misuse the

service. To track such type of users CSP administrator. Administrators have all the information of the users and it can avoid unauthorized actions in the cloud computing environment.

In proposed IDS we will try to detect various web services attacks such as wrapping attack , malware injection attack as well as some system vulnerabilities. System vulnerabilities includes session riding and hijacking or insecure cryptography etc.

4.1 General View of Intrusion Detection System

Figure 4.1 shows general view of proposed system. Client or user can access various services which is provided by Cloud service Provider(CSP) through internet. An IDS agent will track all the activities of user. Log of all activates are provided to the IDS.

Users: Any authorized client or user. Users are authorized by Cloud Server Provider (CSP) or any organization's users. That organization is authorized by CSP .

Deployment Server: Deployment Server contains our proposed system that is Intrusion Detection System (IDS). Intrusion is detected using Knowledge-based database or behavior based database . In our system we have IDS agent. IDS agent tracks users and provide log to the IDS. Using this log information and the database stored in the system intrusion is detected.

Figure 4.2 shows flow of the proposed system. The proposed system is deployed on server side in the cloud end. System can verify the data with the help of normal behaviour of the client using the service and signatures of the attacks. Our system can track all the activities of users, but user is unaware of he being tracked. Once the attack is detected, information about the attack is forwarded to the appropriate administrative profile. This system will reduce impact of various attacks and system vulnerabilities.

The processing of the system is as follows:

1. The systems have an **Agent.** This agent tracks all the activities of the users. The agent is creating a log of these activities.

2. Whenever any authorized user requests for the service, agent . The agent will collect the information from various activities of the user and provide necessary information for further verification.

3. Collected information is first filtered with the help of various signatures. Signatures are the evidences of the various attacks. If information will match with any of the information, system will detect intrusion and it is verified with the behavioral pattern. If it goes in line with the normal pattern the behavior is updated. If there is mismatch the system will detects intrusion.

From the users' perspective, the application is no different from any other network/Web-based application they would use within the enterprise there is nothing special about the fact that it's running on a cloud platform as far as they are concerned. Finally, there is of course ongoing administration of the platform as well as the applications, which is carried out by the central IT function.

4.2 Flow of the system is as follows

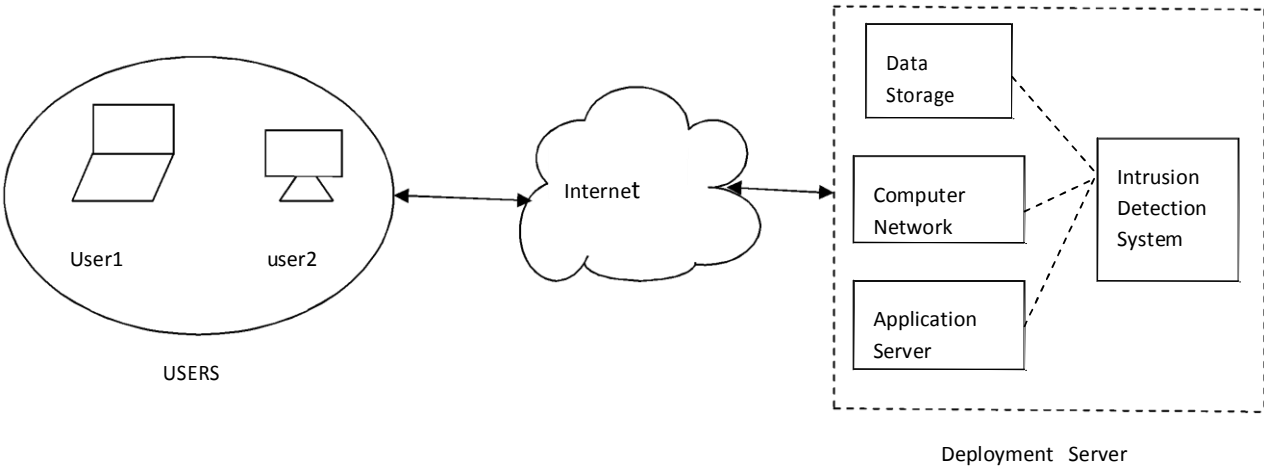

Fig.4.1: General View of the System

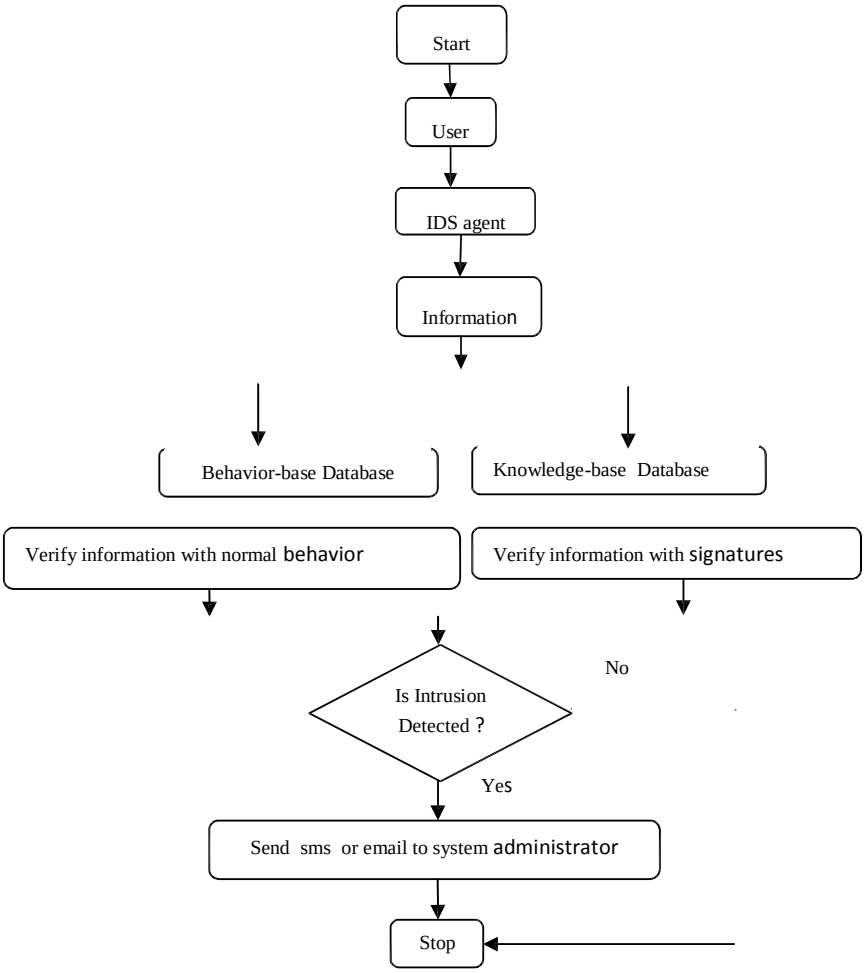

Fig.4.2 : Flow Diagram for System

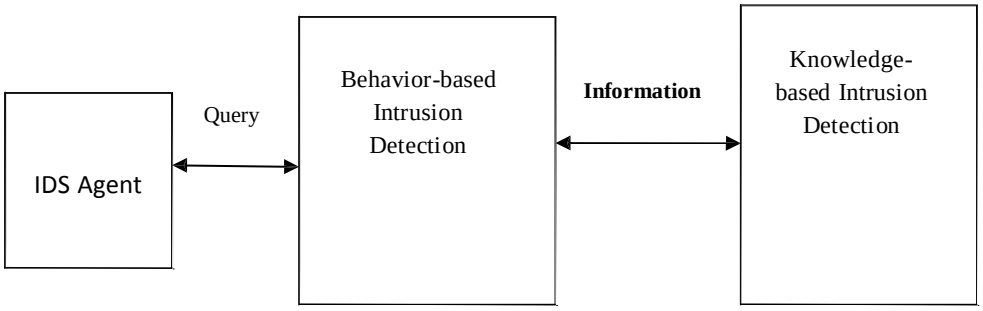

Fig.4.3 : Component at CLOUD side

4.3 Components at Cloud side

There are three main components at Cloud side. Components are as follows:

a) IDS agent

b) Behavior-based IDS

c) Knowledge-based IDS

4.3.1 IDS Agent:

IDS agent collect information about users and track all activities of the users. Log of these activates are analyzes and the information which is important for intrusion detection is forwarded to the IDS system.

4.3.2 Behavior-based IDS

Figure 4.3.2 shows Behavior-based IDS . The Behavior-Based method dictates how to compare resent user action tothe usual behavior. Numerous method exits for Behavior-based intrusion detection, such as data mining, artificial neural networks etc. Behavior –based IDS collect information from IDS agent. Director of the Behavior-based IDS analyzes all this information. The necessary information for intrusion detection is forwarded to the notifier. Notifier compare this information with set of instructions (i.e. set of normal behavior instruction) and take appropriate action.

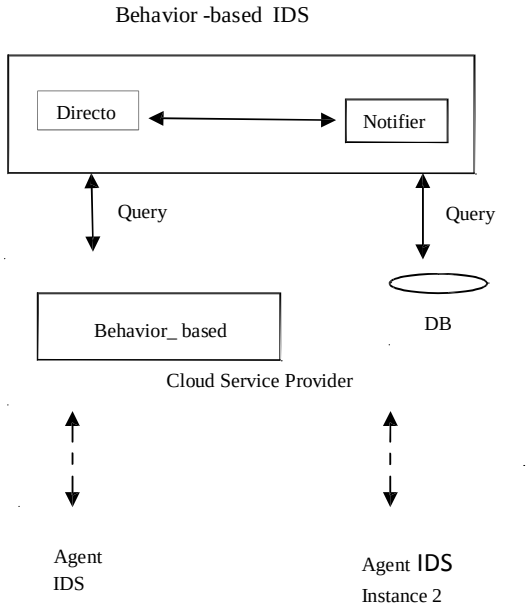

Fig.4.3.2: Behavior-based IDS

4.3.3 Knowledge-based IDS

Figure 4.3.3 shows Behavior-based to Knowledge-based IDS . Knowledge-based intrusion detection is the most often applied technique in the field because it results in low false-alarm rate and high positive rates, although it can't detect unknown attacks patterns. It use rules and monitors a stream of events to find malicious characteristics. One advantage of using this kind of intrusion detection is that we can add new rules without existing ones. Knowledge-based collect information from Behavior-based IDS and again analyzes that information by director of the knowledge-based IDS. Notifier of the knowledge-based IDS compare this information with signatures (evidences of attacks) which are stored database of the knowledge-base IDS. If any match is found it will detect Intrusion.

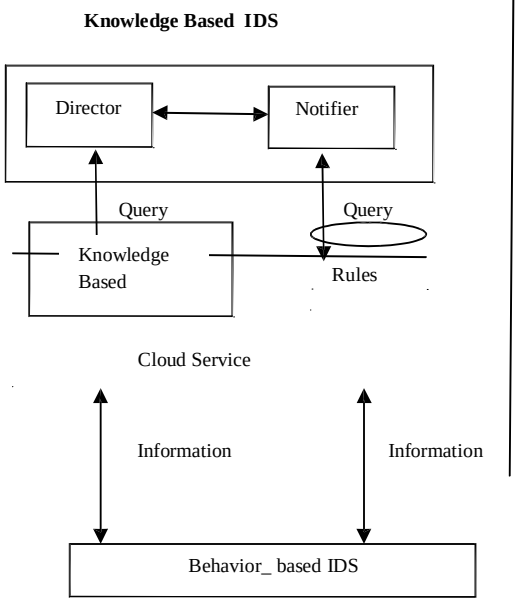

Fig.4.3.2 Behavioral to Knowledge Based IDS

In the proposed system we will use Behavior-based IDS and Knowledge-based IDS which gives us two level of security. The main advantage of our system is that here the data is verified by two systems. If first system unable to detect the data , second system again verifies the data and compare it with the signatures within the database. If it is not matching then it create a new signature for such type of data as well as it will update the database. With the help of proposed IDS
we will try to detect various web services attacks as well as
system vulnerabilities. Initially we will focus on wrapping attack and malware injection attack.

5. CONCLUSION

We proposed a Intrusion Detection System for cloud computing environment to reduce the impact of cyber attacks , virus attacks as well as to detect system vulnerabilities. This System also allow to set new signatures without disturbing previous signatures. We will try to set new set of signatures for new attacks or unknown attacks and forward it to the Behavior-based IDS , so that in future same type of attack is knows by Behavior-based IDS and it is detected by Behavior-based IDS only. With the help of IDS definitely we will reduce false alarm rates. At the same time we can say that it will also detect unknown attacks also. In the proposed system we will use normal behavior of the system and signatures of various attacks to detect intrusions which is a hybrid IDS. The main advantage of our system is that here the data is verified by two approaches. If first approach unable to detect the data, second approach again verifies the data and compare it with the signatures within the database. In the proposed

system definitely we will have very low false positive alarm. With help of proposed system we will try to reduce impact of various attacks in the cloud computing. Finally we can say that we the help of proposed system we will try to improve the security in cloud computing environment.

REFERENCES

[1].Kleber Vieira, Alexander Schulter,CarlosBecker Westphall, and Carla Merkle Westphall "Intrusion Detection for Grid and Cloud Computing" *(IT Professionals, Vol. 12, no. 4, 2010 pp 38-43)*

[2]. S N Dhage, B B Meshram, R Rwat, S Pawawe, M Paingaonkar, A Misra "Intrusion Detection System in Cloud Computing Environment," International Conf. And Workshop on Emerging Trends in Technology" *(ICWET 2011, ACM Press, pp. 235-239).*

[3]. Farzad Sabahi "Cloud Computing Security Threats and Responses" *(IEEE Press (2011), pp. 245-249).*

[4]. Michael R. Hines "Going Beyond Behavior-Based Intrusion Detection" *(IEEE Press 2011)*

[5]. Kazi Zunnurhain, Susan Vrbsky "Security Attacks and Solutions in Cloud"

[6] Wikipedia. http://www.wikipdea.com.

[7] Book- Matt Bishop "Computer Security"