International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 1 (January '2016)

A STUDY ON INTRUSION DETECTION SYSTEMS IN CLOUD COMPUTING

P.Kaladevi,
M.Phil Scholar,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women (Autonomous),
Elayampalayam, Namakkal, Tamilnadu

Dr.P.Sumitra,
Assistant Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women (Autonomous),
Elayampalayam, Namakkal, Tamilnadu

Abstract : Cloud Computing is an attractive and cost-saving service for buyers as it provides accessibility and reliability options for users and scalable sales for providers. In spite of being attractive, Cloud feature poses various new security threats and challenges when it comes to deploying Intrusion Detection System (IDS) in Cloud environments. In this paper, we start by providing an overview of the Cloud Computing classifications, providers, models, and main features. We present a general view of intrusion detection systems. This paper also describes the IDS main components and classifications. After that, we review the requirements and the customer needs for deploying IDS to the cloud.

Keywords: Cloud computing, security, cloud providers, intrusion detection system

I.INTRODUCTION

Cloud computing is a large-scale distributed computing paradigm [1]. It is a collection of sources in order to enable resource sharing in terms of scalability, managed computing services that are delivered on demand over the network. Its users need not to buy infrastructure, software, resources, as a result saving a large amount of expenditure. Cloud basically provides services through a third party. The Cloud Computing model can be classified into many types based on its architectural layout.

Public Clouds are the most popular type among end-users due to their rapid setup time and low capital expenditure. The providers of this type of a cloud usually partition their physical servers and lease these portions to the cloud consumers. Therefore, the end-users have the illusion of managing an infinite computational power and storage capacity. However, public clouds suffer from a lack of infrastructure transparency, which make them less attractive for large organizations [2]. On the other hand,

Private Clouds are not open to the public users in a sense that their infrastructure is controlled by private organizations. Large organizations who wish to take advantage of scalability, availability and structural transparency with a strict enforcement of data security can use such a model. Nevertheless, the private model requires some customization for the owners of existing legacy systems to fit in the cloud environment.

The **Hybrid Cloud** model combines the features of the public and private models. This mixed environment is suitable for organizations that have software or hardware compatibility issues with the external cloud providers, but still want to take advantage of the vast storage space and other cloud resources provided by public clouds. Another reason to choose hybrid clouds is the exibility in exposing corporation's assets for a limited time to the public users. Therefore, a corporation's resources can be partially exposed in public side of the cloud rather than jeopardizing everything on the public cloud. Figure 1 on the next page gives an overview of the main three cloud models discussed.

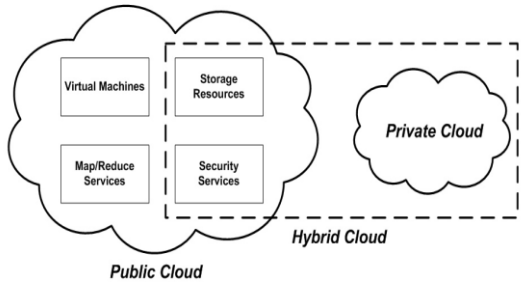

Figure 1: Cloud Deployment Models

II. CLOUD SERVICE MODELS

There are a number of service models provided by the Cloud Computing architecture to satisfy different cloud consumers requirements. Each of these models targets a specific type of application or system deployment. These service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software as a Service (SaaS)
SaaS has the ability to provide the end user with an interface, such as a web browser or a mobile app, to run applications on the cloud provider's premises. These applications are built and located on the clouds assets. Therefore, SaaS users can access the application from anywhere without concerns about the application's underlying installation and management issues.

Services in this layer can include data store-age buckets, database management applications, and security tools. CareCloud [3] and Host Analytics [4] are examples of SaaS services, which are used for business performance analysis.

Platform as a Service (PaaS)
PaaS is an environment to develop SaaS applications. This type of service can be beneficial to the developers for creating the needed software stacks or hardware structure to deploy their application to the cloud. PaaS cloud providers offer pre-installed developing environments like programming languages, IDE tools, and testing bench- marks. For example, platforms to develop cloud-based databases are SQL Azure [5] and Couchbase [6].

Infrastructure as a Service (IaaS)
IaaS provides on-demand infrastructure resources such as virtual machines, virtual network settings, and storage devices. These types of resources are targeting the expert cloud consumers to build and customize their cloud applications from the early stages. Some of the main IaaS providers on the cloud are Amazon EC2 and EMC [7]. The major advantages of these types of cloud-based services are the low initial cost of application deployment, the exibility in scaling the service based on users demand, and the availability of the service based on the cloud providers reputation. The cloud service models are displayed in Figure 2.

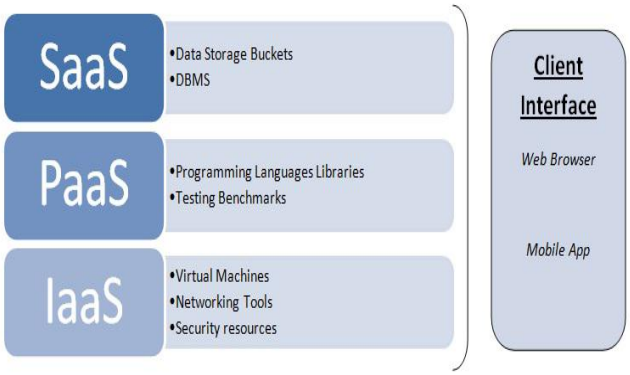

Figure 2: Cloud Service Models

III. CLOUD FEATURES

The Cloud Computing model proposes many desirable features to attract organizations to move their existing IT assets toward the cloud. Regardless of the cloud deployment model, clouds provide one or more features to the end-users based on their applications domain. These choices are intended for rapid application development, self-managing workload adjustments, and financial cost savings. The following are some of the features that are promised by the cloud providers.

Elastic Scalability
Cloud users have the ability to modify the number of consumed resources based on their application demands. Thus, users with large data processing loads can divide them into smaller parts and distribute them into multiple tasks operated by on- demand cloud resources.

High-Availability
For a complex environment like the cloud where large numbers of virtual resources are initialized, relocated, and cancelled based on customers' on-demand requirements, the need to have a stable and reachable service is mandatory. The cloud promises accessibility even with failure of some of its assets. Individual services may fail for one or more particular users, but the system continues to survive for other services or different group of users.

Utility-based Service
Clouds offer the financial concept of pay-as-you-go subscription as their main billing system. Customers get the functionality they need on a powerful infrastructure, but only pay for what they consume. The cost of setting up a server, hiring system administrators, and installing all the needed applications is mostly eliminated. Furthermore, cloud providers can alert their customers if they exceeded certain amount of data usage or reach a specified limit on their account [8].

IV. SECURITY IN THE CLOUD

IaaS is the fundamental tier for the other service layers in the cloud. The absence of strong protection measurements in this layer affects the security available in the other cloud layers. For this reason, many IaaS providers implement various security techniques to protect their customers data and applications. The challenges of cloud security have drawn the attention of different types of IT consumers. According to the International Data Corporation (IDC) [9], a survey conducted of top IT executives about the current cloud services and obstacles preventing many organizations from moving to the cloud found that around seventy five percent voted for security as a top priority concern. Furthermore, the demand for security and privacy features on the cloud is requested by many researchers [10]. Features like access control procedures for data protection and intrusion prevention systems need to be provided to the cloud consumers. In addition, shared datasets have to be sheltered from other privileged users and adversaries existing in the same physical medium. Finally, proper user authentication methods and secure connections from and to cloud assets need to be enforced.

There are several security mechanisms implemented by the cloud providers. First, physical security procedures to protect their datacenters from external intruders are enforced. Network security is also implemented by providing access to firewall ser- vices, SSL-protected APIs, and accounts access management utilities. Hypervisor security is also used to guarantee customer instances isolation and, multiple copies of customer's data are backed up in different physical locations.

Cloud-Specific Attacks

The Cloud Computing paradigm introduces particular challenges when it comes to the nature of observed cyber attacks. Because of data access exibility and various on-demand resources for the cloud, there are different emerged types of attacks that need to be carefully addressed. For example, attacks that camouage the authentication process for certain cloud services. Also, attacks that allow distinct users residing in the same physical server to glimpse others VMs information.

Masquerade Attacks

This type of attacks allow the intruders to hide their original identity by using forged network identity. Typically, attackers use this type of unauthorized access method to bypass the usual authentication process. Vulnerable login procedures, security holes in software packages, or abused privileged-users rights are some of the reasons that facilitate the masquerade attacks. As a result, intrusion detection systems can be used to prevent masquerade attacks in cloud environments by comparing users' behavior based on previous actions [11].

VM Escape Attacks

This vulnerability in the host system virtual environment , the hypervisor, allow the intruder to eavesdrop on other users' information, which are residing in different virtual machine. This attack, also known as side-channel attack, can be performed with very few log trails, which makes it difficult to trace as feature prevention mechanism [12]. IaaS cloud providers implement machine virtualization techniques in order to distribute physical server resource among different VMs. This type of assets multiplexing can result in major security threats due to shared CPU caches or storage devices. Typically, data encryption is an immediate solution for such a public environment. However, encryption is not practical while processing the data in the systems temporary memory. Moreover, the encryption process will add extra overhead on the overall performance especially for remote users. An IDS security system can be tuned to trace the out-going network packets as a prevention of the attack's consequences.

V. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection System (IDS) is a security technology, which can detect, prevent and possibly react to computer attacks. IDSs have proven to be effective tools in conventional local and wide area networks. In a typical network scenario, an IDS generates alerts regarding security threats and logs them for further analysis. Then, a network administrator can decide to rely on the IDS judgment and take an action or let the system react through a predefined plan.

The concept of IDS was first introduced in 1986 by Dorothy Denning [13]. Since then, IDSs have evolved from standalone hardware to a piece of software to a virtual machine (VM) instance which can run on virtual environments like the clouds. Typically, many organizations require an automated process to monitor various events occurring on their network assets. Therefore, it can provide the needed protection against external intruders and internal users who are taking advantage of their privileged accounts. Accordingly, the incorporation of an IDS in any network is vital.

The location of the IDS is an important factor to in achieving efficient monitoring. In a typical network layout, the IDS box can be placed along with other essential security tools like the access control module and anti-virus server just behind the corporate firewall (Figure 3). A major distinction between the IDS and a firewall is that the former will continuously monitor the internal part of the network as well as protecting it from internal and external threats. On the other hand, firewalls act like a conditional barrier that only allow defined services, ports or IP addresses to pass through them. However, once an intruder bypasses the firewall, it is hard to stop or recognize the origin of the attack.

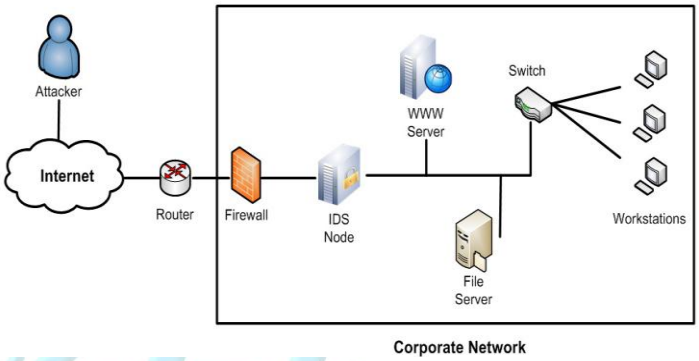

Figure 3: IDS Placement in Typical Network

IDS Components

There are four main components that all IDSs share regardless of their nature: the sensors, the data storage unit, the analysis unit and the knowledge-based unit (KB). Initially, IDS sensors collect data traffic in the network and store them into the storage unit. Next, the analysis unit with the help of the KB correlates the collected data and detects suspicious behavior from the gathered network traffic. The KB usually contains the rules (signatures) that identify different attacking scenarios or the values of thresholds that define the normal behavior of the monitored system. On detecting an attack, the analysis unit informs the security administrator with detailed information about the nature of the event or responds to the incident according to a predefined action plan. Figure 4 on the next page illustrates the intrusion detection process.

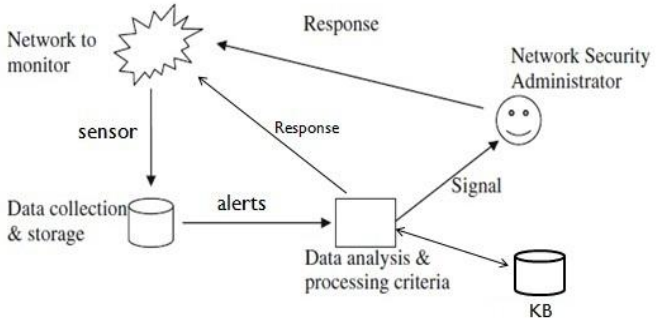

Figure 4: IDS Detection Process

IDS Classifications

In general, IDSs can be classified into different types based on their method of collecting data, their method of analyzing alerts, and their reaction to security threats, as shown in Figure 5 [14]. According to the method they collect data, IDSs can be Host based (HIDS) or Network based (NIDS). A HIDS usually observes a specific host by installing an agent inside the monitored system and examining its system calls, operating system log _les, or application generated events. This type of tight coupling with the monitored target has the advantage of examining system level threats like buffer over flow attacks. However, the need to deploy a sensor to every monitored host can be complicated and unwelcomed by the user in public environments due to privacy concerns. On the other hand, a NIDS collects and examines network packets generated from multiple network nodes. Therefore, a NIDS has the advantages of monitoring all the network activities as well as being independent from the monitored hosts but it can report many harmless legitimate network interactions if it is not properly configured.

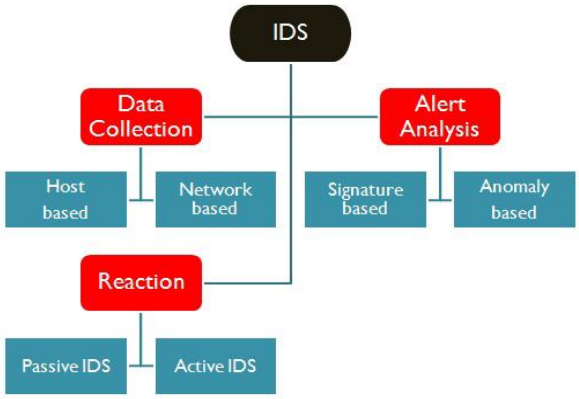

Figure 5: IDS Classifications

IDSs analyze collected data by matching recognized attacking signatures or detecting abnormal behavior. Signature-based or misuse based analysis techniques use pattern recognition procedures to check for well-known attacking scenarios previously defined in the knowledge repository. The use of signatures, which are specified in a grammar-based descriptive language, can be very effective because of their immediate creation and highly customizable nature. Furthermore, they have the benefit of a low number of false-positive alarms, which are alerts from legitimate actions, due to the matching process between the collected data and the stored signatures for the properly configured IDS systems. The security administrator has to tune the quality of the signatures to react the nature of the protected application and signatures have their limitations with respect to detecting zero day attacks [15]. The anomaly or behavior based approach builds a profile of the monitored system and continuously checks for deviations from the defined baseline values of such a profile. This type of approach requires a learning period to decide the different aspects of the system normal behavior. In general, users tend to avoid this type of IDSs because of its latency for acquiring the detailed knowledge of the monitored system's normal state.

IDSs are generally expected to react to the discovered attacks to conclude their protection lifecycle. The passive IDS approach sends alerts to the security administrator regarding suspicious activities. An alert can be in the form of inserting the details of the incident into a database or sending an email to the security administrator. Alternatively, an active IDS takes an action based on a predefined reaction plan. Such an action can involve dropping packets, blacklisting IPs, or diverting network traffic. The action plan is usually defined and maintained by the system security administrator.

IDS in the Cloud

In the Cloud Computing environment, an IDS is still essential. Cloud consumers can not always just depend on the cloud providers security infrastructure. They may need to monitor and protect their virtual existence by implementing IDS with other network security technologies like firewalls, access controls and data encryption within the cloud fabric. Consequently, cloud consumers need to be able to deploy detection systems within their virtual boundaries. IDSs in the cloud has the following requirements:

- The IDS is expected to monitor multiple virtual machines based on application requirements.
- The cloud consumers should be in control of their management.
- Cloud-based IDS must be able to incorporate IDS custom rules (signatures of attacking scenarios). These customized rules will be written by a security administrator based on application requirements.
- Cloud consumers should have the ability to scale the protection coverage of their applications based on the amount and the location of the data being analyzed.

Intrusion Detection for Cloud Computing (IDCC)

The Intrusion Detection based on Cloud Computing (IDCC) architecture [16] was developed to achieve a global monitoring view of the network resources and to help in discovering coordinated attacks on local sites. This architecture consists of two major parts, the local sites and a global site. The global site is called the Cloud Computing Data Center (CCDC). Each part has its own analyzer with database components. Additionally, every local site is composed of multiple sensors to collect network traffic among the local nodes. These sensors produce log les from miscellaneous sources like stand-alone IDSs, firewalls, or any system that can generate logs. In general, Local Controllers (LC) at each site format the logs generated by the sensors and store them in the Local Intrusion Database (LIDB). If multiple LCs exists in a site, a Master Local Controller (M-LC) is used to coordinate between them. In the same way, the Local Analyzer (LA) is used to analyze the collected data from the LIDB and generate alerts based on predefined rules. The LA correlates similar alerts and sends

them to the Global Intrusion Database (GIDB) in the CCDC for further analysis. The GIDB is used as a large database for the alerts generated from local sites. The Global Analyzer (GA) analyzes the collected alerts from the GIDB and searches for complex intrusion attack patterns against all local sites. When a threat is detected by the GA, the local security administrator is informed so a proper action can be taken such as blacklisting the source of the attack.

The proposed architecture is more suitable for private clouds that are designed with this type of infrastructure due its ability to communicate between local and global sites. As a result, cloud users of the local sites will be more dependent on the cloud provider's global IDS administration. Furthermore, the process of administrating the global and local sites raises some serious challenges.

Cooperative Distributed Intrusion Detection System (DIDS)

The main objective of the cooperative distributed intrusion detection system (DIDS) framework is to reduce the impact of Denial of Service (DoS) or Distributed-DoS (DDoS) attacks by sharing alerts between various IDSs in different cloud regions [17]. If a system is under a form of DoS attack, it can spread the news and warn other systems in the cloud before the attacker flood of the network packets can reach them. Consequently, other systems can survive by taking preemptive measures like blocking the source of the reported threat or possibly reallocating virtual or network resources into safer settings. The Intrusion Detection Message Exchange Format (IDMEF) protocol exchanges alerts between IDSs in the form of XML documents. This standard method of communication between IDS nodes can facilitate the integration process of new IDSs into the cooperative DIDS ecosystem. Each IDS has the capability to verify the authenticity of an alert sent by a cooperative agent in other IDS. To achieve this goal, the cooperative agent in each IDS uses the majority voting to judge the legitimacy of the alerts broadcasted from other IDSs and create a new blocking rule to its local rules database in the case of valid warning. If an alert fails to pass the majority voting test, the local IDS ignores the alert.

As seen in Figure 6 on the next page, the cooperative DIDS has five main components; Intrusion Detection, Alert Clustering, Threshold Check, Response & Block, and Cooperative agent. The Intrusion Detection component is implemented using a network-based and rule-based IDS to gather network traffic. The Alert Clustering and Threshold Check components are used to group similar alerts and decide whether to drop suspicious network packets or to apply additional inspections based on predefined threshold values. All packets with the serious alert type are dropped and an entry in the block table is added regarding the source of that packet. The main functionality of the Response & Block component is to prevent the flow of bad packets into the local network as well as to broadcast alerts to other IDSs. The Co- operative agent is responsible for sending and receiving alert messages for other IDSs and applying the majority voting algorithm to verify the alert authenticity.

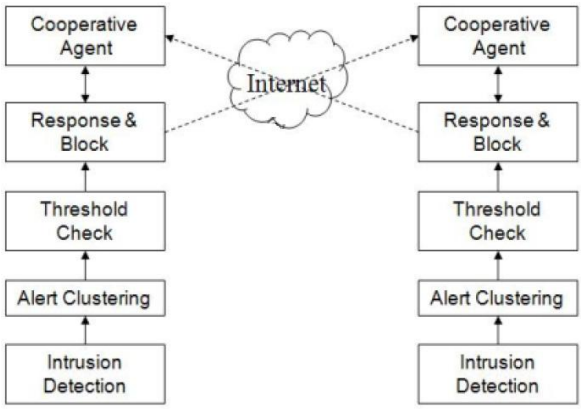

Figure 6: Cooperative DIDS

The main goal of DoS attacks is to suspend access to computer systems by over- loading their resources with unnecessary network requests. This type of sudden strike on the victims networks can cause a significant financial damages compared to other kinds of cyber attacks [17]. The cooperative DIDS is designed specifically to address the DoS problem. However, the implementation of the Cooperative agent and the majority voting system add further complexity to the existing intrusion detection functionality. As a result, the cooperative DIDS can suffer from low performance in terms of computational time and detection rate of other types of attacks. Also, there is need to have special cloud infrastructure to adopt this model.

Integrating a Network IDS into an Open Source Cloud Computing Environment

The work by Mazzariello et al. [34] discusses various deployments of existing IDSs to Eucalyptus [18], which is an open source cloud environment. The suggested model is to deploy multiple IDSs next to every cloud physical controller, which monitors a smaller portion of network traffic for a set of virtual machines. A general layout of the suggested approach is displayed in Figure 7

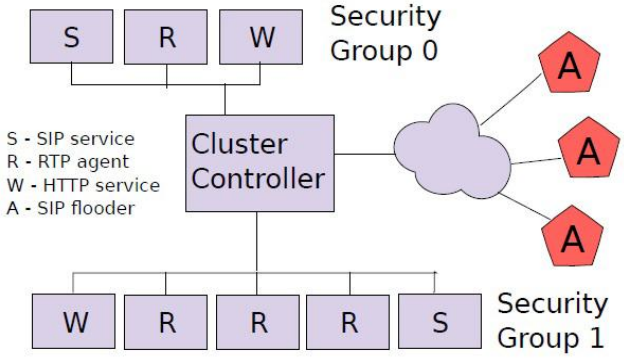

Figure 7: Integrating IDS in the Cloud

The general setup for the approach requires deep alteration of the physical implementation of the cloud assets, which results

in a strong dependency between the IDS components and the cloud provider's infrastructure. Consequently, the IDS administration process by the cloud consumers suffers from service limitations and lack of customization.

VI.CONCLUSION

Cloud computing has motivated the introduction of a new service to the Information Technology (IT) discipline. The use of Cloud computing will reduce the infrastructure maintenance cost, scalability for data and applications, availability of data services and pay as you use features. Since the idea of Cloud computing is well known as a network of networks over the World Wide Web, consequently, the probability of having various types of vulnerabilities causing attacks is high. Analyzing various techniques of intrusion detection and prevention systems has revealed that either using anomaly or signature based techniques stand alone will not provides desired security features. Hence, a hybrid mechanism can be implemented to enhance the detection rate. In this paper we have discussed cloud basics and working on cloud IDS approach administrations.

VII. REFERENCES

[1] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. Elhariri, Ahmed M. Yousof and Sahar A. Shehata. 2012. A Hierarchical Intrusion Detection System For Ckoud: Design and Evaluation. International Journal on Cloud Computing Services and Architecture (IJCSA).

[2] D. McCa_erty, \Cloud Computing: Public Versus Private Options." Base Line Magazine. http://www.baselinemag.com/c/a/Virtualization/Cloud-Computing-Public-Versus-Private- ptions-126667/, Apr 2010. [Accessed: Spet 2012].

[3] Care Cloud. http://www.carecloud.com, May 2012. [Accessed: Spet 2012].

[4] Host Analytics. http://www.hostanalytics.com, May 2012. [Accessed: Spet2012].[17] SQL AZURE, \Windows Azure Environment." http://www.windowsazure.com/en-us/home/features/sql-azure, May 2012. [Accessed: Spet 2012].

[5] Couch-base. http://www.couchbase.com, May 2012. [Accessed: Spet 2012].

[6] EMC. http://www.emc.com, May 2012. [Accessed: Spet 2012].

[7] Amazon Web Services, \Amazon CloudWatch." http://aws.amazon.com/cloudwatch, Jun2012. [Accessed: Spet 2012].

[8] International Data Corporation, \IT Cloud Services User Survey." http://blogs.idc.com/ie/?p=210, Oct 2008. [Accessed: Spet 2012].

[9] K. Hwang, S. Kulkarni, and Y. Hu, \Cloud security with virtualized defense and reputation-based trust mangement," in Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 717{722, Dec.2009.

[10] H. Kholidy and F. Baiardi, \Cidd: A cloud intrusion detection dataset for cloud computing and masquerade attacks," in Information Technology: New Generations (ITNG), 2012 Ninth International Conference on, pp. 397{402, 2012.

[11] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, \Hey, you, get o_ of my cloud: exploring information leakage in third-party compute clouds," in In CCS09: Proceedings of the 16th ACM conference on Computer and communications security, pp. 199{212, 2009.

[12] D. E. Denning, \An intrusion-detection model," IEEE Trans. Softw. Eng., vol. 13, pp. 222{232, Feb. 1987.

[13] S. Axelsson, \Intrusion detection systems: A survey and taxonomy," tech. rep.,2000.

[14] L. Seltzer, \The Zero-Day Attack." PC Magazine Digital Edition. http://www.pcmag.com/article2/0,2817,1879939,00.asp, Oct 2008. [Accessed: Spet2012].

[15] W. Xin, H. Ting-lei, and L. Xiao-yu, \Research on the intrusion detection mechanism based on cloud computing," in Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on, pp. 125{128, Oct. 2010.

[16] C. Lo, C. Huang, and J. Ku, \A cooperative intrusion detection system frame-work for cloud computing networks," in 39th International Conference on Parallel Processing Workshops (ICPPW), pp. 280{284, 2010.

[17] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, \Denial-of-service attack-detection techniques," IEEE Internet Computing, vol. 10, pp. 82{89, 2006.

[18] C. M. R. Bifulco and R. Canonic, \Integrating a network ids into an open source cloud computing environment," in The Sixth International Conference on Information Assurance and Security (IAS), 2010.