International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(1): 32-40
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Secure Model for Virtualization Layer in Cloud Infrastructure

Sina Manavi*, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia, 43400 UPM Serdang, Selangor
Manavi.Sina@gmail.com, Sadra.m.alian@gmail.com, izura@fsktm.upm.edu.my, azizol@fsktm.upm.edu.my

Abstract- *cloud security is one of the buzz words in cloud computing. Since virtualization is the fundamental of the cloud computing, needs to study it more deeply to avoid attacks and system failure. In this research is focused on virtualization vulnerabilities. In addition it is attempted to propose a model to secure and proper mechanism to react reasonable against the detected attack by intrusion detection system. With the secured model (SVM), virtual machines will be resist more efficiency against the attacks in cloud computing.*

Keywords: Cloud computing, security, Virtual Machine, secure virtualication, Virtual Machine Monitor

INTRODUCTION

Cloud computing has been deployed in a variety of data storages and data centers, network communications, data managements. Still there is no universal standard definition of cloud computing. Researchers introduce and define cloud computing in different aspects and terms. The US National Institute of Standards and Technology [1] defined cloud computing as a model for enabling access to a pool of resources such as servers, networks, applications, and services with low cost and minimal management. They characterized cloud model on five characteristics and four deployment models. The characteristics consist of on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured pay-as-you-go services [2]. Meanwhile the deployment models are highlighted with private cloud, community cloud, public cloud, and hybrid cloud [1], [3], [4]. Cloud computing [5] can be defined from different perspectives. From the perspective of a provider, the major cloud components are data centers and data storages for processing and computing. Meanwhile, from another prospective cloud can be divided into two parts, private cloud and public cloud [6], and the combination of the these two parts are hybrid cloud [7]. They signified the integration of hardware and software with application as the main characteristics of cloud.

Service models are classified as the following [2], [8], [9]: Service as a Software (SaaS), i.e. the applications which are running locally on the user's hosts; Platform as a Service (PaaS), i.e. providing the software platform where system runs on; Infrastructure as a Service (IaaS), as it manages large sets of computing resources; and Desktop as a Service and Data as a Service, have the same acronym (DaaS) and different usage.

Even though cloud computing has numerous benefits, since it is still a new technology there are vulnerabilities that need to be addressed. Cloud consumers and providers are investigating on cloud, providing secure communication and services are necessary. Attacks on web-applications (e.g. SQL injection, Cross-Site Scripting, DDOS) and networks shown by the reports, demonstrate that these common attacks have been appeared in cloud computing as well. Usually cloud computing are suffering from following vulnerabilities: accessibility, virtualization, web application, privacy control issue, confidentiality, and integrity, whether they are insider attack or outside ones, and there is no exception for cloud computing [8], [10],[11] [12].

There are several models and tools to enhance security and prevent attacks on applications, data storages, data centers and any hardware or software resources. Firewalls and Antiviruses have been commonly used to protect the servers and clients from attackers and any unauthorized accesses. But unfortunately using these two approaches are

inadequate and it gives rise to the demand for another tool and thus encouraged experts to develop an application which is called an intrusion detection system (IDS).

Intrusion detection systems have been used to detect intruders and attacks. It is classified in categories [13], Host-based Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS), Distributed Intrusion Detection System (DIDS) which is widely used in distributed systems [14], and Hybrid Intrusion Detection System which can be combinations of any of them. NIDS monitors the network traffic and evaluates the input data but one of the negative points of NIDS is poor visibility of the internal network. HIDS investigates and monitors the internal computers behind the firewall unlike NIDS which checks the external data. On the contrary, attacks (e.g. file system changes, system calls and application log) in the host system can be detected by the HIDS. Additionally, another disadvantages of HIDS is that it can be compromised by malwares, and consequently disabling the HIDS from detecting the malicious behaviors [13], [15].

Intrusion detection system has been divided into two techniques [16]: anomaly detection and misuse detection. Misuse detection uses a signature-base which consists of known attacks signatures or patterns to evaluate and match each similarity of the behaviors with the recorded signatures. Meanwhile, it is obvious that zero-day attack signatures or patterns are not included in the knowledge base, and therefore, the signature base needs to be update frequently. To address this weakness, anomaly detection has been proposed to detect unknown attacks using learning techniques. One of the drawbacks of anomaly detection technique is the more significant false positive rate as compared to misuse detection.

Intrusion detection system becomes vital in providing detection of intruders and attacks. Since cloud is widely accessible from all over the network for internal users and external ones, it is urgent to use intrusion detection system to detect possible attacks and contributed to the protection mechanism of the cloud.

The rest part of the paper is organized as follows: Section II explains the definition of the intrusion detection system and the importance of it in cloud environment. Section III, presents the related work of virtualization. Section IV, is a demonstration of virtualization vulnerabilities, finally the last section is the proposed model is a new mechanism to react properly through IDS alarm

1. INTRUSION DETECTION SYSTEM IN CLOUD

In this section we discuss several methods proposed for preventing the cloud from attacks and intruders, focusing on the combination of Virtual Machines (VMs) and intrusion detection system. Different researches have been deployed on available cloud virtualization which gained new approaches as well.

Cloud users and providers have their own set of core security requirements, as shown in Table 1.

TABLE 1. REQUIREMENTS FOR CLOUD SECURITY MONITORING

Requirement	Definition
Effectiveness	The main goal of security in cloud is effectively prevents\detects, vulnerabilities and attacks
Precision	Systems need to enhance its accuracy in terms of detection attacks with minimum false-positive and false-negative rates
Transparency	The security model must have minimum visibility from cloud service provider, developers, and service users and attackers sight
Non-Subvert-ability	The cloud host and physical layer in addition to VMs must be protected against compromised service users with infeasibility to suspending the alarm system
Deployability	The system must be possible to be

	implemented over various available cloud architectures
Dynamic reaction	System must be able to employ impressive techniques to defeat attacks intrusion with minimal effect on legitimate process and functionalities
Accountability	Security system must not affect the cloud's core functionality and applications, while it must log cloud activities to enable accountability

Host tools are efficient and powerful in monitoring host systems for detecting and preventing attacks, even though it is very difficult to detect new attacks (e.g. polymorphism and metamorphism). Meanwhile, it is true that network based tools are not very good for monitoring, detecting and preventing the host system from the attacks, but it is working very positively in resistance against the attacks [17].

Traditional intrusion detection system cannot easily deal with new attacks, such as DDoS, and coordinated attacks. The mechanism proposed in [4] attempts to overcome the shortcomings of traditional IDSs for distributed systems and cloud computing environments in order to speed up the response time, detecting, and capturing of new threats and intrusions, thus decreasing false alarms. Furthermore, it can compact similar alerts and detect more anomaly behaviors in correlating alerts coming from heterogeneous platforms.

By means of classification, training, feature extraction, and meta-learning, a data mining algorithm is utilized to detect and flag malicious attacks with VMM-IDS in virtualized server application to facilitate management and isolation of VMs [18–20]. VMM enhances the invisibility of the intrusion detection system and it can be used as a shield to avoid the intrusion detection systems from being detected and compromised, especially HIDSs. Furthermore, not only developing the VMM-IDS is much easier, but also HIDS and NIDS can be combined to enjoy the advantages both of them. In this case, it is possible to detect unknown and well-known attacks as well. They could increase the accuracy rate with a low percentage of false alarms [15].

1. Virtualization

Via virtualization it is possible to split, allocate, and resize the resources dynamically to build up the ad-hoc systems. A Virtual Machine (VM) is software which runs operating systems and applications as a physical hardware. The operating system which is installed on a VM is called guest OS. Each VM may be able to accommodate multiple operating systems. As it is necessary to manage layers, creating and controlling the virtual machines, this need is addressed by Virtual Machine Monitor (VMM). Hypervisor is one of the techniques which make possible to have multiple operating systems ability.

Several models and frameworks have been developed with the aim to secure the cloud using intrusion detection system and virtualization. Even though intrusion detection systems, virtual machines, virtual machine monitors and hypervisors are being used widely in cloud environment, but there are shortcomings which need to be addressed. One of the limitations of hypervisors is that if an attacker gains control of the hypervisor or if it crashes, then virtual machines are accessible via the attacker [21]. Using the MapReduced algorithm of Hadoop to enhance the calculation speed of intrusion detection system log files and improve the reliability of the system [22] was another proposal for increasing the performances of the intrusion detection system via the Inter-VM. The attack flow which is generated by the malicious activity is identified and isolated by Virtual machine Intrusion deteCTOR (VICTOR). It is integrated into all existing VMMs to monitor the generated packets by VMs that pass through it, to detect intrusions at the first side (i.e. a distant source) or the end side (the destination VM) [17]. Luo et al. [23] propose the combination of the two virtual system security and virtual security management mechanism as

components to cope with current existing vulnerabilities, and a better management and virtualization security. In order to provide new security solution to enhance the protection and monitoring of the hosts in IaaS, the proposed model for this manner provides transparent and real time monitoring for several VMs at the same time in cloud environments [24].

2. Virtulization Vulnerabilities

As long as resources are shared at network level, host level, and application level, on the other side, data centers or processing data might be overseas or even in other country. In this circumstance it is necessary to consider the three items for security terms which are Confidentiality, Integrity, and Availability (CIA). While the technology come up with new phenomena, CIA are one of the most issue must be consider by cloud provider and consumers[3].

Number of methodologies[25], [26] for enhancing user authentication and preventing from unauthorized access offered, but still there are exploits in application vulnerability[27]. Security breaches has been classified[28] by basic security, network level security and application level security. Now days most of the websites are secured at network level but still the vulnerabilities at the application level can be observed. Threats such as XSS, SQL injection, DDOS attack, are resulting from unauthorized access to the applications. Therefore it is necessary to secure the applications and have a suitable implementation for platform level (PaaS) and software level (SaaS). It is vitally needed to secure the infrastructures. since governments and companies intending to migrate to cloud computing, security policies and role of Service Level Agreement (SLA) has been discussed in order to enhancing the security level in IaaS model [29]. Chirag Modi et.al [30] discussed variety of techniques for intrusion detection and prevention for cloud environment to make a secure environment and higher trustworthy in cloud platform to deliver a better service to the customers.

It is known that virtualization playing the significant role in cloud computing. The fundamental of virtualization starts with hypervisors. Hypervisor or Virtual Machine Manager (VMM) allows having multiple Operating System (OS) running on the one physical system, providing resources for each OS without interfering with each other. With virtualization not only flexibility, scalability, security, utilizing resources will be improved in manageability, cost effective cloud computing with virtualization technology takes less power since more than one virtual machines can be run on a single physical machine[31].

It has been a challenge for preventing the hypervisors from being compromised. By running a malicious code on the guest system it is possible to get full access on the hypervisor, therefore hacker may gain access to the guest operating system or even can access to data passing through the hypervisors[23]. Other well-known attack which is common on hypervisor can be named as BLUEPILL[32] , SubVir[33] , DKSM[34]. Isolation is another major key in virtualization.it assurance that one instance of VM cannot affect the other running VMs in one host. But if the implementation is weak, it can bring vulnerabilities as well. while the isolation is applying between the VMs, resources are using the shared resources.VM escape[23] is an exploit that compromise the isolation between VMs and Host whereby the malicious code in a VM can completely bypass the virtual machine monitor layer and gain full access to the host machine. Once attacker has the full access of host machine, controlling the root of virtual network is gained that VM and host can be compromised, which can believe that both the guest and the host are gone. As long as host can control the VM in any circumstance such as starting, shutting down, pausing the VM, with proper rights , it can monitor application running on the VMs as well, furthermore, host can view, copy and even modifying the data stored in the allocated virtual disk of the VM. This all this important roles of the host, shows that securing the host is highly important and needs to find a solution to increase the protection of the host and hypervisor avoiding to be attacked.

If the hacker can get control, he can do the IP spoofing by sending the packets and receiving as trusted party without knowledge of the user, although this weakness can be cover by IPsec and encryption techniques. Sniffing and spoofing are one the vulnerabilities in virtual networks[35]. For instance in Xen hypervisor, there are two mode offered to users, bridge mode and route mode. Bridge applied as a *virtual hub* in the bridge mode; in this mode one VM can sniff the virtual network by sniffing tools such as Wireshark. On the other side, by choosing the route mode, route will be a *virtual switch* which uses a dedicated virtual interface to make connection between each virtual machine. By Address Resolution Protocol (ARP) spoofing, packets can be redirecting and available for sniffing the packets which are passing through the VMs.

Studying the cloud computing security issues, virtualization vulnerabilities are significant problem that needs to be addressed. Attacks on hypervisors and virtualization isolation needs to study more and find proper solution.

3. Secure Model for Virtualization layer in cloud Infrastructure

According to the previous section cloud computing and virtualization vulnerabilities have been studied. The Secure model for Virtualization Layer (SVL) protects cloud environment from threats and attacks. In this research it is attempted to find a way to improve the attack detection and prevention mechanism to avoid system failure and increase the virtualization security.

The Secure model for Virtualization Layer (SVL) uses standard cloud architecture (See Figure 1), which build IaaS on Virtual Machines (VMs) and workload are usually integrated from the guest OS and the user processes. In order to secure these VMs and their transactions with other VMs, Virtual Machine Monitor (VMM) is introduced as an abstract module above virtualization which provides techniques and methods for securing VMs. Methods usually are based on IDS/IPS in combination with Service-Level Agreement (SLA) and Access Control List (ACL). In our general cloud security model (SVL) all seven requirements in Table 1 are met in all level from Host OS up to the guest OS. The main concept is to build a hierarchical isolate-defeat mechanism, to protect the whole virtualization against malicious activities, detecting without preventing legitimate operations from continuing their activities.

To reach this, it is required to have a comprehensive control over virtualization. System resources will be wasted if Host OS methods are applied to control all virtualization in terms of security. Instead of implementing normal model for cloud, we propose a new foundation layer for virtualization, which is called Virtualization Basement (V-Basement). This layer divides virtualization into two separate well-monitored components.

Virtualization takes place inside V-Basement, instead of having a solid virtualization. Hence virtualization could be classified based on services required by end guest machine (VM), regardless of who is going to use this machine as service user (SU). This will increase the feasibility of applying security procedures. It is necessary to specify IDS for each data flow source based on its application (e.g. Web Server, Data Storage, etc.). This specification allows for lightweight IDSs, instead of huge resource-consuming IDS.

3.1 Primary Virtual Mechanism:

A new module is introduced as Primary Virtual Mechanism (PVM). Each PVM contains only specific group of services and applications at the end VMs. Also Inter-PVM Monitor module is added to enable secure communication between PVMs. The idea behind using these modules is providing a semi-VMM service between classified Primary Virtual Machines and a secure channel among PVMs and Host OS. There are four components inside each PVM (see Figure 2).

V-Basement Communicator provides routines and interfaces for PVM to communicate with Host OS. The next module, i.e. the VM-Shadow allows legitimate processes to continue when malicious

activity is detected in a specific End-VM or a group of End-VMs inside a VMM. The mechanism works because all VMs in a specific PVM are similar from the views of applications and implementation. When a new VM is created for SU, VM-shadow starts to take snapshots from the VM (scheduled based on service type and criticality). Therefore, the VM-Shadow has all required information to regenerate a shadow copy to the closest possible state of a selected VM on-demand.

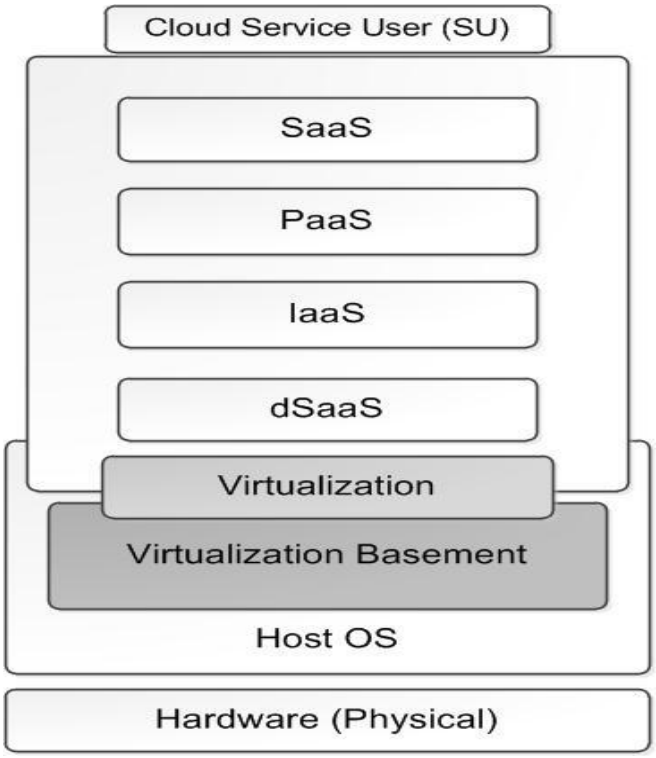

Figure 1. Hirachichal Secure Virtual Model for cloud Security

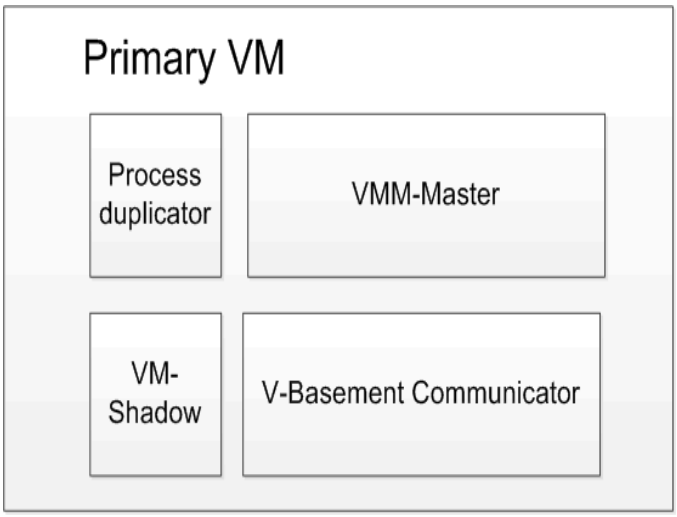

Figure 2. Primary VM-Master

When the VMM-Master detects an anomaly behavior in any VM or VMM group based on the IDS alarm, firstly the suspicious VM will be regenerated by the VM-Shadow and Duplicate processor with the abnormal processes. The shadowed VM gives services to the abnormal or suspicious process to see what does the process is going to do exactly. Furthermore the process in the shadowed VM will be study to examine, is it really abnormal or not. By this means it is possible to decrease the false negative and positive negative of IDS weakness. Meanwhile, the normal processes remains in the main VM and will be responded by the server. The shadowed VM is highly isolated and request responding are not real. In this state, the process behavior is studying by the behavior investigator.

3.2 Virtual Machine Monitor-Master:

The VMM-Master coordinates all VMMs inside the primary VM. This will give another level of abstraction which equips the system with the ability to create a restriction zone for a specific group of VMs without interfering with other VMs by restricting a selected VMM using the firewall module (see Figure 3).

There is an Inter-VM Monitor with the same abilities of VMM but in one outer layer to enable the features described above. It also has a stream buffer, to help its internal IDS to have access to larger

amount of data flow without directly accessing the host OS memory and an Access Control Level (ACL) to control authorized policies.

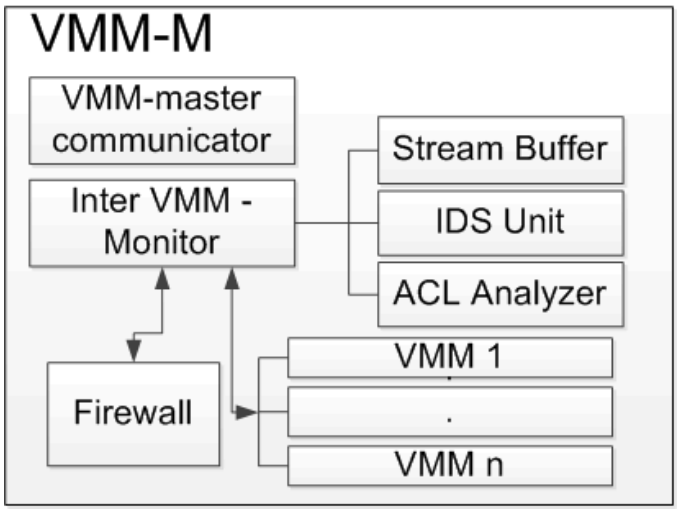

Figure 3. Virtual Machine Monitor-Master

3.3 Virtualization Basement (V-Basement):

V-Basement provides abstracted virtualization by dividing virtualization method hierarchically into primary VMs and the following modules. Inter-PVM Monitor performs VMM roles between PVMs, providing secure communication channels between all the above layers and the actual physical layer (hardware) through Host OS. In this module there is a direct access to the network layer where it is recommended to add a network layer IDS as well (see Figure 4).

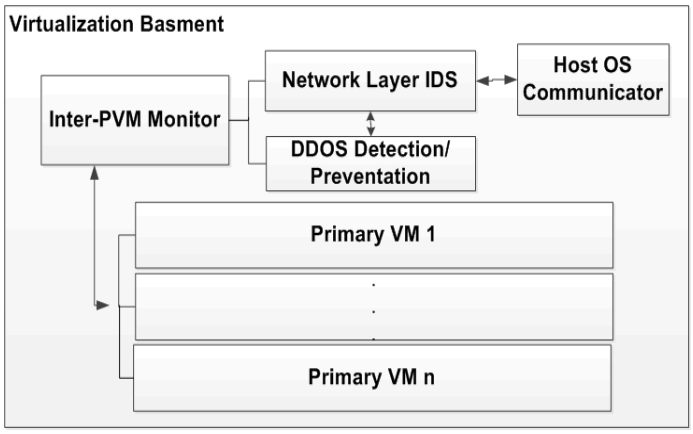

Figure 4. Vrtualization Basement

I. DISCUSSION

In normal virtualization, since the virtualization operations interact directly with VMM on the Host OS, controlling the hierarchical of the VMMs are limited. SVL model provides proper structure to increase the security to the highest possibility for virtualization. In other words, because the allocated resources to the virtualization are self-virtualized, and the possibility of accessing them by unauthorized user is minimized. Furthermore, DDoS attack from internal cloud is restricted, and all the traffics between the VMs are controllable such as controlling traffics in physical layer. Cloud providers have significant controls in IaaS as well. Using suitable reaction mechanism at attack-time, it avoids the possibility of attacks and thus thwarts the distribution of the intrusions. Meanwhile based on the pointed reaction, since all normal processes are duplicated and shadowed using the Duplicate Processor and VM-Shadow, they will not terminate.

Even though SVL model has high complexity especially in implementation, it has the ability to cope against the data leakage, DDoS attack, as well as unauthorized user access.

To the best of our knowledge, there is no similar model implemented; it is assumed that SVL model can address the abovementioned problems.

4. CONCLUSION AND FUTURE WORK

SVL model is introduced to address cloud security drawbacks caused by classic virtualization methods; SVL model proposes a novel hierarchical mechanism which significantly improves vendor control in IaaS. In addition, it provides a practical solution by reacting to intrusions with an isolate-conquer approach. We believe that SVL model, which combines virtualization and intrusion detection system, can increase the detection rate and provide protection against attacks targeting virtualization, and consequently will result in reliable cloud security. Although SVL model is expected to be expensive in terms of implementation cost and performance, we believe that it is worth the higher security it provides. SVL model is proposed based on some assumptions and our best knowledge.

As this is an ongoing work, the proposed model and framework will be implemented in order to compare and evaluate it with the traditional manner.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2009.

[2] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*, 2011, pp. 12:1–12:6.

[3] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[4] W. Xin, H. Ting-iei, and L. I. U. Xiao-yu, "Research on the Intrusion Detection Mechanism based on Cloud Computing," *Computing*, pp. 125–128, 2010.

[5] K. Stanoevska-Slabeva and T. Wozniak, "Cloud Basics – An Introduction to Cloud Computing," in *Grid and Cloud Computing*, K. Stanoevska-Slabeva, T. Wozniak, and S. Ristol, Eds. Springer Berlin Heidelberg, 2010, pp. 47–61.

[6] H. Ghanbari, B. Simmons, M. Litoiu, and G. Iszlai, "Feedback-based optimization of a private cloud," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 104–111, 2012.

[7] C. Vecchiola and R. Calheiros, "Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka," *Future Generation*, vol. 28, no. 1, pp. 58–65, Jan. 2012.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[9] F. Lombardi, R. Lombardi, Flavio;Di Pietro, and R. D. Pietro, "CUDACS: securing the cloud with CUDA-enabled secure virtualization," *Information and Communications Security*, pp. 92–106, 2010.

[10] J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 552–555.

[11] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," *2010 IEEE 3rd International Conference on Cloud Computing*, pp. 276–279, Jul. 2010.

[12] A. Waqar, A. Raza, and H. Abbas, "User Privacy Issues in Eucalyptus: A Private Cloud Computing Environment," *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 927–932, Nov. 2011.

[13] M. Laureano, C. Maziero, and E. Jamhour, "Protecting host-based intrusion detectors through virtual machines," *Computer Networks*, vol. 51, no. 5, pp. 1275–1283, Apr. 2007.

[14] S. Ros, F. Cheng, and C. Meinel, "Intrusion Detection in the Cloud," *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. 729–734, Dec. 2009.

[15] F. Azmandian, M. Moffie, and M. Alshawabkeh, "Virtual machine monitor-based lightweight intrusion detection," *ACM SIGOPS*, vol. 45, no. 2, p. 38, Jul. 2011.

[16] D. Anderson and T. Frivold, "Next-generation intrusion detection expert system (NIDES): A summary," 1995.

[17] U. Tupakula, V. Varadharajan, and N. Akku, "Intrusion Detection Techniques for Infrastructure as a Service Cloud," *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, pp. 744–751, Dec. 2011.

[18] W. Lee, S. J. Stolfo, and K. W. Mok, "A data mining framework for building intrusion detection models," *Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on*. pp. 120–132, 1999.

[19] T.-Y. Wang, C.-H. Wu, and C.-C. Hsieh, "A Virus Prevention Model Based on Static Analysis and Data Mining Methods," *Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on*. pp. 288–293, 2008.

[20] M. G. Schultz, E. Eskin, F. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," in *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, 2001, pp. 38–49.

[21] F. Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology,"

Int. Journal of Machine Learning and Computing, vol. 2, no. 1, 2012.

[22] S.-F. Yang, W.-Y. Chen, and Y.-T. Wang, "ICAS: An inter-VM IDS Log Cloud Analysis System," in *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, 2011, pp. 285–289.

[23] S. L. and Z. L. and X. C. and Z. Y. and J. Chen, S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in *International Conference on Cloud and Service Computing (CSC)*, 2011, pp. 174–179.

[24] M. Ibrahim, A.S. and Hamlyn-Harris, J. and Grundy, J. and Almorsy, "CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model," in *5th International Conference on Network and System Security (NSS)*, 2011, pp. 113–120.

[25] J. Sedayao, S. Su, X. Ma, M. Jiang, and K. Miao, "A Simple Technique for Securing Data at Rest Stored in a Computing Cloud," in *Proceedings of the 1st International Conference on Cloud Computing*, 2009, pp. 553–558.

[26] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th international *conference on Financial cryptograpy and data security*, 2010, pp. 136–149.

[27] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)*. O'reilly Media, 2009.

[28] R. B. and S. S. And, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," *CoRR*, vol. abs/1204.0, 2012.

[29] L. Karadsheh, "Applying security policies and service level agreement to IaaS service model to enhance security and transition," *Computers & Security*, vol. 31, no. 3, pp. 315–326, May 2012.

[30] 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*, pp. 1–16, Jun. 2012.

[31] B. Loganayagi and S. Sujatha, "Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques," *Procedia Engineering*, vol. 30, no. 2011, pp. 654–661, Jan. 2012.

[32] J. Rutkowska, "Subverting VistaTM kernel for fun and profit," 2006.

[33] J. Rutkowska, S. T. King, and P. M. Chen, "SubVirt: implementing malware with virtual machines," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*, 2006, p. 14 pp.–327.

[34] S. Bahram, X. Jiang, Z. Wang, M. Grace, J. Li, D. Srinivasan, J. Rhee, and D. Xu, "DKSM: Subverting Virtual Machine Introspection for Fun and Profit," *Reliable Distributed Systems, 2010 29th IEEE Symposium on*. pp. 82–91, 2010.

[35] H. Wu, C. Winer, Y. Ding, and L. Yao, "Network security for virtual machine in cloud computing," *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, no. 60803057, pp. 18–21, 2010.