OpenStack Cloud Security Vulnerabilities from Inside and Outside

Sasko Ristov, Marjan Gusev and Aleksandar Donevski
Ss. Cyril and Methodius University,
Faculty of Information Sciences and Computer Engineering,
Skopje, Macedonia
Email: sashko.ristov@finki.ukim.mk, marjan.gushev@finki.ukim.mk, aleksandar.donevski@outlook.com

***Abstract*—As usage of cloud computing increases, customers are mainly concerned about choosing cloud infrastructure with sufficient security. Concerns are greater in the multi-tenant environment on a public cloud. This paper addresses the security assessment of OpenStack open source cloud solution and virtual machine instances with different operating systems hosted in the cloud. The methodology and realized experiments target vulnerabilities from both inside and outside the cloud. We tested four different platforms and analyzed the security assessment. The main conclusions of the realized experiments show that multi-tenant environment raises new security challenges, there are more vulnerabilities from inside than outside and that Linux based Ubuntu, CentOS and Fedora are less vulnerable than Windows. We discuss details about these vulnerabilities and show how they can be solved by appropriate patches and other solutions.**

***Keywords-Cloud Computing*; *Security Assessment*; *Virtualization*.**

I. INTRODUCTION

Infrastructure as a Service (IaaS) is the most offered cloud service layer by public cloud service providers and also the most used by customers. There are lots of open source cloud solutions that offer building IaaS framework over Internet. Selecting a proper IaaS framework is a difficult task since the customers have different requirements and all IaaS frameworks offer various advantages [1]. System administrators mostly care about easy deployment, scalability, supporting different operating systems, hypervisors, and licensing. However, the main concern of cloud computing customers is the security. New challenges arise due to multi-tenancy, virtualization, data and application transfer to third party.

Building a private cloud is a good approach that might solve most of the security challenges, since it mitigates the security risks. However, private clouds lack scalability and elasticity [2]. Therefore, most customers will make their decisions in favor of public clouds, since they offer scalability, elasticity and cost reduction. For example, public clouds reduce the cost up to 85% for disaster recovery compared to on-premise resources [3]. It could provide better Recovery Point Objective (RPO) due to layered backup strategy and also Recovery Time Objective (RTO) due to built-in geographic redundancy. Nevertheless, the cloud service provider maybe has not defined these objectives or they do not meet with the customer's one [4]. Most discussions and related papers conclude that the main obstacle for public cloud solutions is the security [2]. Confidentiality, integrity and availability are the biggest security concerns faced by the customers in public cloud solutions [5].

Security evaluation of the cloud architecture and cloud service provider should be realized before migrating the customer virtual machines in public cloud. Traditional security incident handling procedures are applicable for cloud computing with some modification to function optimally [6]. Security assessment and comparison of commercial clouds might be a difficult task because of the limited access rights. Therefore, many public cloud service providers use open source clouds.

In this paper, we are interested in analyzing the security vulnerabilities from private or public networks both on virtual machine instances and OpenStack [7] cloud nodes. We focus on OpenStack open source cloud since it is a scalable solution and more than 60 leading companies participate in its development. The goal of this research is to check the validity of the following hypotheses:

- H1 The cloud solution is more vulnerable from inside than outside. Inside vulnerabilities subsume the outside vulnerabilities;
- H2 The multi-tenant environment raises new security vulnerabilities risks from inside the cloud, both for the tenants and the OpenStack cloud provider; and
- H3 Windows based virtual machine instances are more vulnerable than Linux based CentOS [8], Ubuntu [9] and Fedora [10].

The hypotheses are set since the tenants in the cloud are exposed not only from outside, but also from inside the cloud. That is, there is a threat from other tenants, but also from the cloud provider. The cloud provider has also threats from inside, i.e., the tenants. The systems are more vulnerable if the attacker is in the same LAN [11].

We installed the OpenStack cloud with default installation, where the virtual machine instances are installed with default operating systems. Our goal is to determine all possible risks that arise from inside and outside the OpenStack cloud, the OpenStack cloud architecture vulnerabilities, as well as to propose measures to mitigate the security risks by securing detected vulnerabilities. Our analysis is focused

 ISBN: 978-1-61208-271-4

toward operating system vulnerabilities of virtual machine instance hosted in the cloud and the cloud controller where the OpenStack cloud services are deployed. We assess the OpenStack product weaknesses, possibilities of unauthorized access, ensuring data confidentiality, integrity and availability, risk of DoS (Denial-of-Service) or even Distributed DoS (DDoS) attacks, man-in-the-middle attack, etc.

The rest of the paper is organized as follows. Related work is presented in Section II. Section III briefly describes the OpenStack cloud architecture and its components. The methodology for security assessment is presented in Section IV. In Section V, we present assessment results both for inside and outside vulnerabilities. We discuss and conclude our work, and present future work in Section VI.

II. Related Work

There are a lot of open source cloud solutions to build a private cloud with IaaS cloud service layer. Voras et al. [12] devise a set of criteria to evaluate and compare most common open source IaaS cloud solutions. Mahjoub et al. [13] compare the open source technologies to help customers to choose the best cloud offer of open source technologies. Most common open source cloud computing platforms are scalable, provide IaaS, support dynamic platform, Xen virtualization technology, linux operating system and Java [14]. However, they have different purposes. For example, Eucalyptus [15] fits well to build a public cloud services (IaaS) with homogeneous pool of hypervisors, while OpenNebula [16] fits well for building private/hybrid cloud with heterogeneous virtualization platforms [17].

Many authors have analyzed the cloud security challenges and propose methodologies for security evaluation of the cloud solutions. Cloud Security Alliance (CSA) announce Cloud Control Matrix Version 1.3 [18] which can assist the potential cloud customers to assess the overall security risk of a cloud service providers classifying the security controls according to cloud service layer and architecture. A methodology for security evaluation of on-premise systems and cloud computing based on ISO 27001:2005 [19] is proposed in [20]. The authors in [4] evaluate ISO 27001:2005 control objective importance for on-premise and the three cloud service layers IaaS, PaaS (Platform as a Service) and SaaS (Software as a Service). International Organization for Standardization (ISO) is developing new guidelines ISO/IEC WD TS 27017 [21] that will recommend relevant security controls for information security management system (ISMS) implementation in cloud computing. Eucalyptus and CloudStack [22] have integrated the maximum security level in front of OpenNebula and OpenStack open source cloud solutions [23].

III. The OpenStack Cloud Architecture

Open source clouds have similar architecture [24]. Each open source cloud has, at minimum:

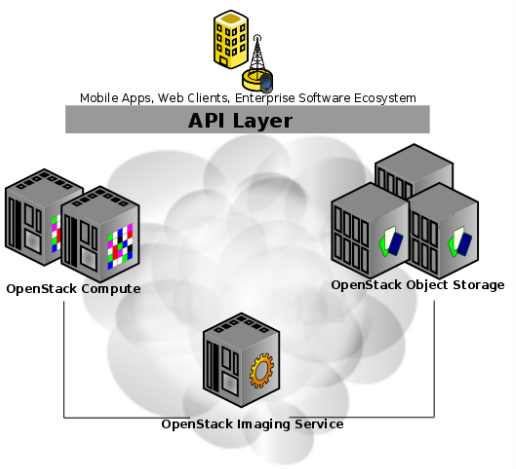

Figure 1. The three components of OpenStack cloud [7]

- *cloud controller* - several services are deployed on this server that control the system, network, schedule the virtual machine instances and act as administrator interface; and
- *cloud node* - this server hosts the virtual machine instances of virtual machines. It communicates with the cloud controller.

This section briefly describes the architecture of the newest Folsom release of OpenStack cloud, its components, networking and features.

A. OpenStack Components

Figure 1 depicts the three main components of OpenStack cloud: Compute, Object Storage, and Image Service.

Compute Infrastructure (Nova) is the core part of the OpenStack cloud that manages instances of virtual machines and networking. *Object Storage* is the subsystem that stores the objects in a massively scalable, large capacity system. It back ups and archives data, stores secondary or tertiary static data, stores data when predicting storage capacity is difficult, and creates the elasticity and flexibility of cloud-based storage for customer web applications. *Image Service* is lookup and retrieval subsystem for virtual machine images.

B. OpenStack Deployment

OpenStack can be deployed and runs on Linux Ubuntu, CentOS and RedHat operating systems. It supports KVM [25], Xen [26], UML [27], and Hyper-V [28] hypervisors. Nova services can be deployed either on the same physical server or they can be installed on separate servers. The OpenStack cloud can be deployed in three different modes:

- Single Node: All nova-services are deployed on only one physical server which hosts also all the virtual machine instances.

 ISBN: 978-1-61208-271-4

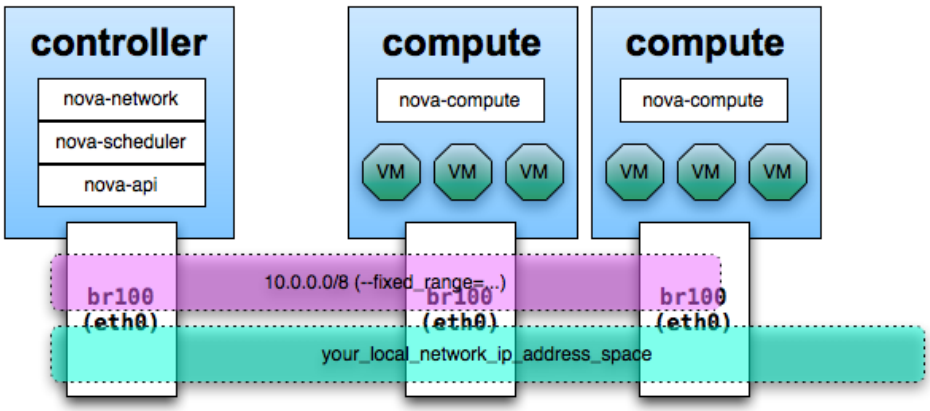

Figure 2. OpenStack networking example [7]

- Dual Node: This deployment consists of two physical servers, i.e., the *Cloud Controller Node* (CCN) and the *Compute Node* (CN). The former is used as cloud controller which runs all the nova-services except for nova-compute. The latter is deployed with nova-compute to instantiate virtual machine instances.
- Multiple Node: Particular number of CNs can be installed resulting in a multiple node installation. Volume controller and a network controller can be added as separate nodes in a more complex, multiple node installation.

We deployed the OpenStack in the Single Node since we are not interested in performance, but for security. The choice for Single Node is based on the fact that the security vulnerabilities of OpenStack services do not depend on the number of physical nodes.

C. OpenStack Networking

OpenStack network consists of two networks, public and private, as depicted in Figure 2. IP addresses from the public network are associated with virtual machines instances to be accessed from the public Internet. The private network is used for internal cloud web service communication.

In this paper, we are interested in analyzing the security vulnerabilities from private or public networks both on virtual machine instances and OpenStack cloud node deployed in Single Node.

IV. Methodology for Security Assessment

This section presents the methodology for security assessment on OpenStack cloud and virtual machine instances. It is based on two assessments with two groups of test cases for different targets. The goal of the assessments is to determine the vulnerabilities of the OpenStack cloud nodes (Compute and Controller deployed in one physical server) and virtual machine instances with different operating systems, both from inside and outside the OpenStack cloud.

A. The Targets

Two different target groups will be assessed. The first target group covers the assessment of physical OpenStack server node which is installed with Ubuntu Server 12.04 64-bit operating system. The second target group covers the assessment of virtual machine instances hosted in the cloud with operating systems:

- Windows 2008 R2 Standard 64 bit;
- CentOS 6 64 bit;
- Ubuntu 10.04 Server Edition 64 bit; and
- Fedora 17 64 bit.

The virtual machine instances are installed with default configuration in order to detect all possible vulnerabilities. We will address which vulnerabilities can be secured after implementing additional patches or reconfigurations.

B. Security Assessment Plan

The security assessment basic goal is to determine the security vulnerabilities of the targets from inside and outside the OpenStack cloud. Therefore, we realize two different assessments using Nessus 5 vulnerability and configuration assessment scanner [29] using External Network Scan policy. Nessus scans all TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports, as well as the vulnerabilities of the services that work on certain opened port.

Each vulnerability is rated as derived from the associated Common Vulnerability Scoring System (CVSS) [30] score:

- *Info* if CVSS score is 0;
- *Low* for CVSS score $\in \{1, 2, 3\}$;
- *Medium* for CVSS score $\in \{4, 5, 6\}$;
- *High* for CVSS score $\in \{7, 8, 9\}$; and
- *Critical* if CVSS score is 10.

Figure 3 depicts the test cases of security assessment from inside and outside the OpenStack cloud, i.e., on private and

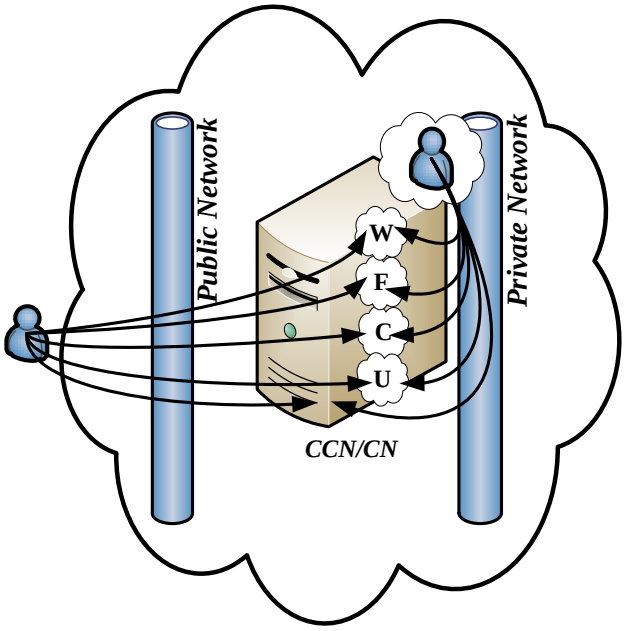

Figure 3. Inside and outside security assessment

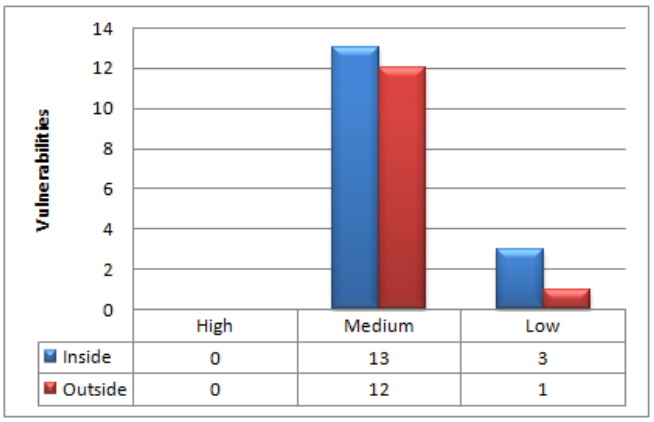

Figure 4. Summary results of OpenStack security assessment

public network. U denotes the Ubuntu operating system, while F, C and W denote the Fedora, CentOS and Windows operating systems, correspondingly.

1) Inside Security Assessment: The Nessus client is deployed on one virtual machine instance. It scans the four virtual machine instances with different operating systems and cloud physical server node (both CCN and CN are the same physical server in our case). This assessment from inside simulates the tenant and its goal is to assess the vulnerabilities that arise from the cloud multi-tenancy. OpenStack private network is used to communicate among the target inside virtual machine instances, the cloud physical node and the virtual machine instance with Nessus client.

2) Outside Security Assessment: The Nessus client is deployed on a workstation outside the OpenStack cloud, i.e., on a public network. It also scans the same four virtual machine instances with different operating systems hosted in the OpenStack cloud and the cloud physical server node. This assessment goal is to assess the vulnerabilities that arise for virtual machine instances and the OpenStack cloud services outside the cloud. OpenStack public network and floating IP addresses are used for communication with virtual machine instances and cloud physical server node.

V. The Results of the Assessment

This section presents the results of both assessments for both target groups defined in previous Section IV. We omit the results of the assessments with CVSS score 0 since they are informative, rather than real vulnerabilities. The values for critical vulnerabilities are also omitted since we have not found any critical vulnerability during the assessments.

A. OpenStack Node Vulnerabilities

Figure 4 depicts the summary results of the security assessment of the cloud node.

The results confirm the hypothesis H1 that there are more inside vulnerabilities which subsume the outside vulnerabilities. 13 medium and 3 low vulnerabilities are detected from inside and only 1 low and 12 medium vulnerabilities are detected from outside. High vulnerabilities are not detected neither from outside, nor from inside.

Let us assess detected vulnerabilities in more detail. 6 Web Server Generic XSS (Cross-site scripting) and 6 Web Server Generic Cookie Injection vulnerabilities (medium) are detected by both assessments on several ports. We conclude that the web server is prone to cross-site scripting and cookie injection attacks. Therefore, new patches must be developed in order to secure two assessed vulnerabilities. Common low vulnerability is the usage of plain text authentication forms which should be transmitted encrypted over secured HTTPS.

Assessment of inside vulnerabilities detected 1 additional medium vulnerability, i.e., the DNS (Domain Name System) server is vulnerable to cache snooping attacks. DNS software vendor should fix it.

Two additional low vulnerabilities are detected, as well. DHCP (Dynamic Host Configuration Protocol) server may expose information about the associated network and applying filtering will keep the information off the network and mitigate the risk of this vulnerability. The web server leaks a private IP address that is usually hidden behind a NAT (Network Address Translation) Firewall or proxy server. However, this is not a real vulnerability since our private IP address will be a public IP in real world scenario.

 ISBN: 978-1-61208-271-4

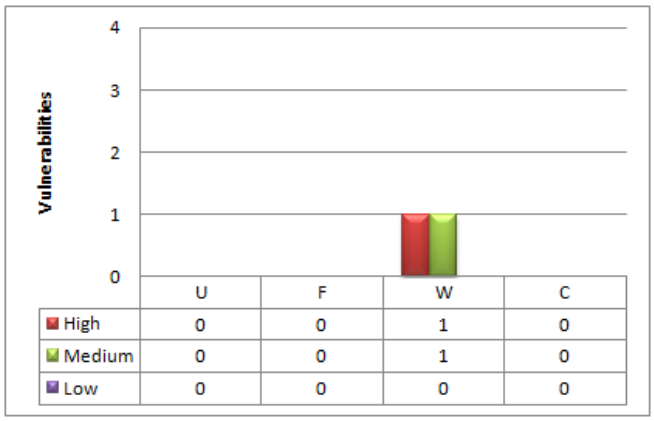

Figure 5. Summary results of outside security assessment on instances

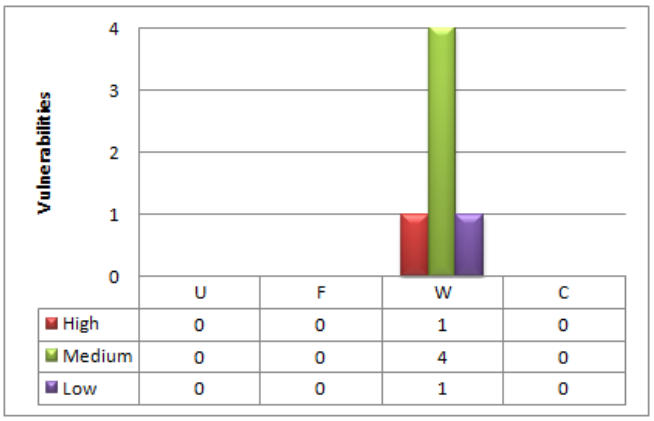

Figure 6. Summary results of inside security assessment on instances

B. Virtual Machine Instance Vulnerabilities

In this section we present and analyze the results of the assessment of the four instances, each with different operating system, both from inside and outside the OpenStack cloud.

1) Vulnerabilities from Outside: Figure 5 depicts the summary results of the outside security assessment on virtual machine instances. U denotes the Ubuntu operating system, while F, C and W denote the Fedora, CentOS and Windows operating systems, correspondingly.

The Nessus client has not detected any vulnerability neither on Ubuntu, nor on Fedora, nor on CentOS operating system. 1 high and 1 medium vulnerabilities are detected on Windows operating system with the assessment from outside the OpenStack. Windows could allow arbitrary code execution (high vulnerability) in the implementation of the Remote Desktop Protocol (RDP). The problem with Windows lies in the requirement to activate remote desktop to connect to Windows, instead of secured SSH (Secure Shell) protocol to connect on Linux based operating systems. However, installing the existing patch will secure the vulnerability. Network Level Authentication (NLA) on the remote RDP server is not configured (Low vulnerability) by default and should be enabled.

2) Vulnerabilities from Inside: Figure 6 depicts the summary results of the inside security assessment on virtual machine instances hosted in OpenStack.

Linux based operating systems are not detected with any security vulnerability from outside the OpenStack cloud, as well. The same 1 high and 1 medium vulnerabilities are detected from inside the virtual machine instance with Windows operating system. However, 3 additional medium vulnerabilities are detected. The first, Windows is using weak cryptography by default for RDP and changing RDP encryption level to ”High” or ”FIPS Compliant” will mitigate this vulnerability. The second, the virtual machine instance is vulnerable to a man-in-the-middle attack. Forcing SSL (Secure Sockets Layer) or RDP with NLA will secure the vulnerability. The last detected medium vulnerability is ”man-in-the-middle attack against the Server Message Block (SMB) server” which can be secured by enforcing message signing.

FIPS-140 incompliance for terminal services encryption level is the additional low vulnerability which can be secured changing RDP encryption level to ”FIPS Compliant”.

VI. Conclusion and Future Work

We have realized security assessments of OpenStack cloud services and four virtual machine instances with different operating systems Fedora, Ubuntu, CentOS and Windows. The experiments addressed the security vulnerabilities both from inside and outside the OpenStack cloud.

The results of the assessments proved hypothesis H2 that cloud multi-tenant environment raises new security vulnerabilities risks from inside the cloud, both for the tenants and the OpenStack cloud provider. Inside vulnerabilities subsume the outside vulnerabilities for the cloud node and each operating system, which proves the hypothesis H1.

Vulnerabilities on Linux operating systems are not detected, neither from outside, nor inside. The assessment of Windows operating system shows additional 1 low and 3 medium security vulnerabilities, which proves the hypothesis H3. All these vulnerabilities are not detected from outside since the OpenStack cloud denies all TCP and UDP ports from outside by default. They still exist because of the Windows default installation (configuration) and the requirements of creating Windows image.

Although Windows based virtual machine instances with default configuration are less secure than Linux based instances, all Windows vulnerabilities can be secured by implementing existing patches or reconfiguration. Only then RDP port 3389 should be opened to outside.

OpenStack cloud is also more vulnerable from inside the cloud with additional 1 medium and 2 low vulnerabilities

 ISBN: 978-1-61208-271-4

which can be secured with reconfiguration. However, we detect that OpenStack cloud has 2 medium vulnerabilities on 6 different ports that can not be secured with reconfiguration, but with new patches that should be developed. All detected OpenStack security vulnerabilities do not depend on creating different virtual machine images, but they exist with default OpenStack deployment.

This paper realizes the security assessment of OpenStack open source cloud and virtual machine instances hosted with different operating systems. We will continue the security assessment on the other open source clouds and bring relevant conclusions about their security vulnerabilities. This will help the customers to select the most appropriate cloud solution regarding the security.

REFERENCES

[1] G. von Laszewski, J. Diaz, F. Wang, and G. Fox, "Comparison of multiple cloud frameworks," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, june 2012, pp. 734 –741.

[2] M. Shtern, B. Simmons, M. Smit, and M. Litoiu, "An architecture for overlaying private clouds on public providers," in 8th Int. Conf. on Network and Service Management, CNSM 2012, Las Vegas, USA, 2012.

[3] T. Wood, E. Cecchet, K. K. Ramakrishnan, P. Shenoy, J. van der Merwe, and A. Venkataramani, "Disaster recovery as a cloud service: economic benefits & deployment challenges," in Proc. of the 2nd USENIX conf. on Hot topics in cloud comp., ser. HotCloud'10, USA, 2010, pp. 8–8.

[4] S. Ristov, M. Gusev, and M. Kostoska, "Cloud computing security in business information systems," International Journal of Network Security & Its Applications (IJNSA), vol. 4, no. 2, March 2012, pp. 75–93.

[5] S. Chaves, C. Westphall, C. Westphall, and G. Geronimo, "Customer security concerns in cloud computing," in Proceedings of the 10-th Int. Conf. on Networks, ser. ICN 2011. IARIA, 2011, pp. 7–11.

[6] A. TaheriMonfared and M. G. Jaatun, "As strong as the weakest link: Handling compromised components in OpenStack," in Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science, ser. CLOUDCOM '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 189–196.

[7] O. C. Software. Openstack cloud. [Retrieved: March, 2013]. [Online]. Available: http://openstack.org

[8] T. C. Enterprise, "Centos," [Retrieved: March, 2013]. [Online]. Available: http://www.centos.org/

[9] Canonical, "Ubuntu," [Retrieved: March, 2013]. [Online]. Available: http://www.canonical.com/

[10] A. R. H.-S. C. Project, "Fedora," [Retrieved: March, 2013]. [Online]. Available: http://fedoraproject.org/

[11] H.-C. Li, P.-H. Liang, J.-M. Yang, and S.-J. Chen, "Analysis on cloud-based security vulnerability assessment," in e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on, Nov. 2010, pp. 490–494.

[12] I. Voras, B. Mihaljevic, and M. Orlic, "Criteria for evaluation of open source cloud computing solutions," in Information Technology Interfaces (ITI), Proceedings of the ITI 2011 33rd International Conference on, june 2011, pp. 137 –142.

[13] M. Mahjoub, A. Mdhaffar, R. B. Halima, and M. Jmaiel, "A comparative study of the current cloud computing technologies and offers," in Proceedings of the 2011 First International Symposium on Network Cloud Computing and Applications, ser. NCCA '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 131–134.

[14] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang, and Q. Li, "Comparison of several cloud computing platforms," in Proceedings of the 2009 Second International Symposium on Information Science and Engineering, ser. ISISE '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 23–27.

[15] Eucalyptus. Eucalyptus cloud. [Retrieved: March, 2013]. [Online]. Available: http://www.eucalyptus.com/

[16] OpenNebula. Opennebula cloud software. [Retrieved: March, 2013]. [Online]. Available: http://Opennebula.org

[17] T. D. Cordeiro, D. B. Damalio, N. C. V. N. Pereira, P. T. Endo, A. V. de Almeida Palhares, G. E. Goncalves, D. F. H. Sadok, J. Kelner, B. Melander, V. Souza, and J.-E. Mangs, "Open source cloud computing platforms," in Proceedings of the 2010 Ninth International Conference on Grid and Cloud Computing, ser. GCC '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 366–371.

[18] CSA, "Cloud security alliance," [Retrieved: March, 2013]. [Online]. Available: http://cloudsecurityalliance.org/

[19] ISO/IEC, "ISO/IEC 27001:2005, Information Security Management Systems - Requirements," [Retrieved: March, 2013]. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[20] S. Ristov, M. Gusev, and M. Kostoska, "A new methodology for security evaluation in cloud computing," in MIPRO, 2012 Proc. of the 35th Int. Convention, IEEE Conference Publications, 2012, pp. 1808–1813.

[21] ISO/IEC, "WD TS 27017, Guidelines on information security controls for the use of cloud computing services," [Retrieved: March, 2013]. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

[22] CloudStack. Cloudstack opens source cloud computing. [Retrieved: March, 2013]. [Online]. Available: http://cloudstack.org

[23] S. Ristov, M. Gusev, and M. Kostoska, "Security assessment of openstack open source cloud solution," in Proceedings of the 7th South East European Doctoral Student Conference (DSC2012), 2012, pp. 577–587.

 ISBN: 978-1-61208-271-4

[24] C.-H. Ng, M. Ma, T.-Y. Wong, P. Lee, and J. Lui, "Live deduplication storage of virtual machine images in an open-source cloud," in Proceedings of the 12th ACM/IFIP/USENIX international conference on Middleware, ser. Middleware'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 81–100.

[25] KVM, "Kernel based virtual machine," [Retrieved: March, 2013]. [Online]. Available: http://www.linux-kvm.org/page/Main_Page

[26] C. Systems, "Xen hypervisor," [Retrieved: March, 2013]. [Online]. Available: http://www.xen.org/

[27] UML, "User-mode linux kernel," [Retrieved: March, 2013]. [Online]. Available: http://user-mode-linux.sourceforge.net/

[28] Microsoft, "Microsoft hyper-v server 2012," [Retrieved: March, 2013]. [Online]. Available: www.microsoft.com/hyper-v-server/

[29] Tenable, "Nessus 5," [Retrieved: March, 2013]. [Online]. Available: http://www.tenable.com/products/nessus

[30] N. V. Database, "Common vulnerability scoring system," [Retrieved: March, 2013]. [Online]. Available: http://nvd.nist.gov/cvss.cfm

 ISBN: 978-1-61208-271-4