

STUDY ON MALWARE ATTACKS OF VIRTUAL MACHINE SNAPSHOTS IN A PRIVATE CLOUD SETUP

Phadtare Tushar Tulsidas

Research Scholar

School of Science & Technology, Glocal University Saharanpur (U.P)

Dr. Praveen Kumar

Research Supervisor

School of Science & Technology, Glocal University Saharanpur (U.P)

Abstract- Cloud computing environment strives to be dynamic, reliable and customizable with a guarantee towards quality service. Virtualization is one of the major backbone components in cloud computing, widely used not only in the infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) but also for software testing, security as a Service, business process as a service and so on. These VM instances are isolated from each other, providing hardware utilization, easier management and migration compared to its physical counterpart. Services are shared among a group of service consumers, partners and vendors. The resources of a single physical machine are shared among the various created VM's giving rise to new architectures and computing paradigms. Thus, security problems pose a major challenge in the virtual machines in the cloud environment. This paper discusses the virtual machine security, the vulnerabilities that are associated with the virtual machines and the security challenges raised by virtualization are presented. Different malwares attacks on the VM s and thereafter their snapshots are analyzed with the help of a Cuckoo Analyzer tool. The average scores are then computed and shown by the tool. An open stack private cloud setup is used for this purpose of study.

Keywords--- *Cloud Computing, Virtualization, Virtual Machines Security, Malwares, VM Snapshots, Open Stack.*

I. Introduction

Virtualization is defined as creating virtual isolated instances of computer hardware platforms, operating systems, storage devices, and network resources by using techniques such as time-sharing, emulation and partitioning. It is the key technology to create a cloud computing platform. The virtualization technologies and the cloud deployment models are adopted in widespread mechanisms, due to their many benefits and advantages. The requirements for such a virtualized environment can be met by four criteria such as (i) Efficiency (ii) Resource control (iii) Equivalence and (iv) Emulation. Virtualization component can enable many possibilities according to the needs of the computing environment. Various kinds of virtualization can be availed namely classified as server, network, storage, memory, software and data virtualization. Also, it can be divided as full virtualization, paravirtualization and partial virtualization based on the architectural considerations. Moreover

hypervisors can be classified as type 1 hypervisors and type 2 hypervisors. Xen and VMware are examples of type1 hypervisors. QEMU, Virtual Box and VMware are some of the examples of type2 hypervisors. Virtualization is considered to be a large and a more enterprising field of research, with utmost new research technologies and new threats figuring out more frequently, with vivid solutions and not fully complete. A VM should be secured from malwares, guest OS root kits, as well as from other co resident VMs on the same underlying physical machine [1]. Threats can affect the virtual machine manager, the virtual machines itself, the operating systems in VM instances, the applications running on those OSs, and the network. Security refers to sensitive data free from disclosure and alteration of data.

Most of the underlying models used in cloud depend on the existing technologies for support; in particular, virtualization component enables on-demand resource provisioning and multi tenancy. Users access software and hardware in cloud environment, through several virtual machines (VM) instances.

1.1. Virtual Machine Security Issues

Virtualization in spite of its increased usage in various deployments of the cloud has the many security concerns and issues namely in the operating system running as a guest (GOS), the hypervisor layer, as well as virtualization itself. Some of the security issues and threats are given.

Mobility of Data

Virtualized environment of cloud consists of workloads, data repositories and sensitive data which are highly mobile and are frequently moved to different virtual and physical resources. Virtual machine data is backed up every time as snapshots and stores those in memory causing backups that result in residing in more locations in different places.

Data Theft

Virtual machine images and so the snapshots from the virtual machines are prone to modification and theft when they are in running or dormant states provoking vulnerability [4]. The remedy is to encrypt these snapshots at all times but can create an overhead on the performance factor. Security of these snapshots must be done in combination with audit trails, log and administrative controls to avoid a snapshot from access by the intruder to access the data in the snapshot image. A solution to this may be the peak valley pair method which is used to maximize the embedding capacity of an image. This method is a reversible lossless data hiding algorithm and helps in hidden data communications [6].

Large Volume Data Destruction

Large volumes of VM snapshots stored have to be completely and permanently deleted from all the potential locations [4]. When the VM's are moved from one physical server to another, it should be such that no trace of

bits should be remnant on the host disk that could be obtained by an intruder or when the host physical disk may be deprovisioned [1].

VM Hardening

VM hardening is the process by which the VM instances are secured and protected by all means, including the firewall. Host Intrusion Prevention Systems or agents protect the virtual machine instances against known and unknown malicious attacks. The file integrity monitoring systems, log monitoring systems, web application protection schemes, and antivirus schemes are some of the guest hardening procedures. VM hardening can be made possible through software in each guest or hypervisor-based APIs such as VMware Vshield APIs [2].

Hypervisor Security

The hypervisor being the important component of virtualization enabling control and monitoring of the VM instances has to be secured and hardened using procedures, protocols and various security schemes. Hypervisor security forms the primary concern for organizations, customers and vendors [4]. It should be able to sustain a complete management, configuration controls and operations, as well as the security of the physical server or any physical machine hosting the hypervisor.

Inter-Communication VM attacks

Virtualization has become imparted to the creation VM instances, such that the network security of the virtual machine instances has to be secured. Inter-VM attacks are made possible when one of the created VM's is attacked and the intruder can compromise or gets access to this guest VM, which can then pass the malicious infection to other guest VMs on the same host [9]. Infected virtual machines now may communicate over each other, making, the already existing network security controls almost invisible to this traffic, hindering monitoring. A complete set of security tools, procedures and protocols can be installed and implemented on each virtual machine.

VM Sprawl

Virtual machine sprawl occurs when there is excess amount of virtual machines instances that are connected to the network which can then exceed the network's capabilities. This is due to the factor with which VMs can be provisioned easily.

This has led to more amount of requests for VM instances and the lack of improper provisioning rules. This can create a larger and more vulnerable attack surfaces and increases security prone. In order to avoid large VM sprawls, virtual machine lifecycle management (VMLM) can be implemented properly [3]. The administrators can be provided with tools to monitor and oversee the complete implementation, operation, delivery and maintenance of all virtual machines during their entire period or existence. In such a way, all VM creations can

be monitored and accountability can be set, and each created VM can be deprovisioned once their purpose has been served [12]. Usage of virtualization management framework and policy based management schemes may be used in these situations.

1.2. VM Vulnerabilities and Attack Examples

Virtualization in cloud computing, despite its emergence as an important part technically, has its own attack layouts. The attacks on the virtual machine instances are similar to that of a physical machine and an attacker or an intruder can attack and take control of it with the same tools, as that of the physical machine counterpart. Also, an attacker can devise new ways to destabilize its target machine in the virtualization layer. As shown in the fig1, the vulnerabilities for a type 2 hypervisor, can be such that attacks could be performed from a VM instance against another VM instance, the hypervisors or the physical host operating systems. Ivan Studnia[11], in his paper discusses some of the attacks by using the properties of virtualization in a virtualized environment targeting virtual machine instances, thus corrupting the created VM instances.

Detection of Virtualized Environment

Virtualization concepts, except the para virtualization technique are designed in such a way that an exact duplication of the physical machine can be provided loaded with the guest OS images. Therefore, in order to detect a virtualized environment, the presence of a hypervisor running underneath the OS has to be determined. An intruder could estimate whether the system under target is in a virtualized mode or not. By this process, he could take any corresponding action pertaining to the current situation of the VMs. The virtual machine can be checked for its integrity by the presence of a hypervisor under his OS or not. [8] gives specific example of hypervisor detection. The presence of the hypervisors could be confirmed by the time taken for the instructions to execute. So, from this time calculated the presence of the machine whether in virtualized environment or not can be found as the hypervisors require more time to execute. These comparisons are precomputed based on the time complexities and their measurements of an identical, safe and secure system. [21] Relates a methodology based on the time calculations needed to access the TLB (Translation Lookaside Buffers).

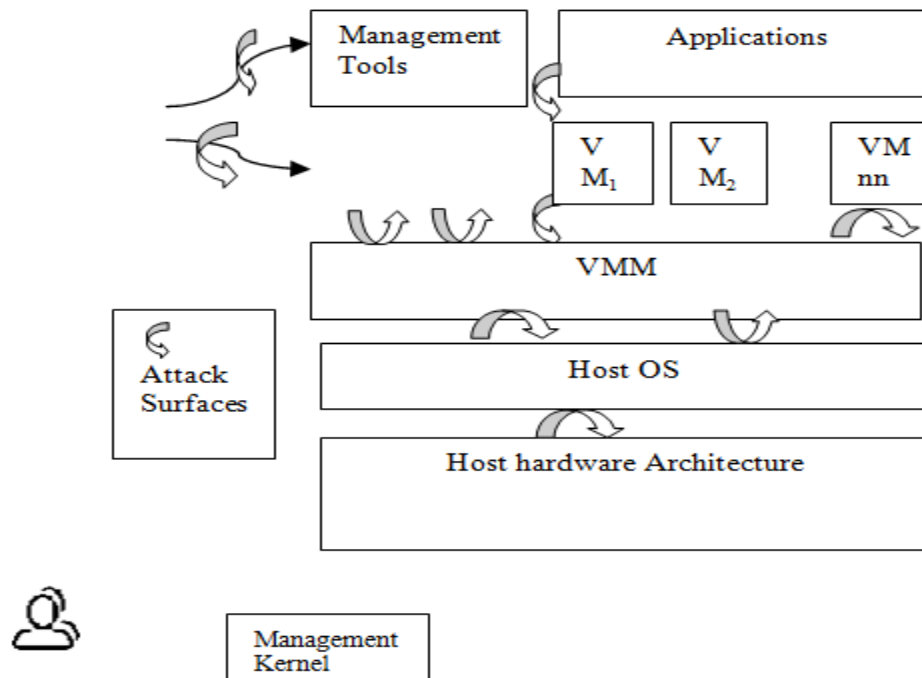


Fig. 1: Attack Surfaces on a Specific Virtual Machine

1.3 Security Methods

Virtualization is one of the huge and active fields of research in cloud computing, with every new research technologies coming up. Also in line with this new threats and vulnerabilities coming out, the whole of it can never be completely overcome. Threats can affect the following agents: the Virtual Machine Monitor (hypervisor) itself, the Virtual machines, the operating systems images(ISO) in VMs, the software running/present on those Operating systems, and the networks. Security has to be applied to data disclosure, alteration of any data whether sensitive or public and the many sensitive transactions associated with data.

Virtual Machine Introspection is a technology of monitoring a Virtual Machine (VM) for analyzing the software which is present/running on the virtual machines and the capability of the hypervisors to ingress the allotted memory space of a victim virtual machine [13]. Kernel and rootkit protection can be provided by making the hypervisor in a more privileged mode. Security could be thus enforced in the operating system by these hypervisors externally. The authors studnia et al in [11] describes three types of hypervisors namely the Scivisor, Hytux and the patagonix. For example, the SecVisor is a type of hypervisor designed and made possible to ensure the integrity of an OS.

2. Methodology

Virtualization has made possible to capture the VM snapshots from each virtual machine. Usually, a particular VM runs from the memory of a physical host and thus a snapshot from a given virtual machine would capture

the complete state, the behavior of the virtual machine pertaining to the configuration and the data associated with it at that particular moment.

It preserves the state of the VM at that moment of time and prevents the GOS (Guest Operating Systems) to write on a snapshot file. Thus, the capture of the VM snapshot is stored as a file on the memory of the physical host. Capturing the state of a VM by a snapshot doesn't take time thus creating no disruptive downtime in the process of the machine at hand. Thus it is much easier to create, retain and manage the snapshots. Broadly, snapshots can be classified as two types, they are

1. Disk Snapshots: These types of snapshots retain the state of a Virtual machine virtual hard disk, at a particular instant of time. For this snapshot to be resumed, it requires to reboot and all the applications to be restarted. This type of snapshot can be taken in two phases: (a) the memory contents of the cache data in the virtual disk. (b) The snapshot itself of the virtual hard disk.
2. System Snapshots: The system snapshot exhibits the complete state information of the virtual hard disk and the RAM [20]. Using these snapshots, users could roll back to the restore state without rebooting and the applications are resumed from the last execution state. When a VM snapshot is captured, the files related to a particular snapshot can be shown as in table 1,

File type	Extension format	Description
Flat file	-flat.vmdk	This file comprises of the data for the base disk, ie the data contents of a VM hard disk drive. This is the first file that is created.
Delta Disk files	-delta.vmdk	The delta disk files represent the difference between the current status of the VM and the snapshot that is taken at a previous time period.
Memory file	.vmsn	The memory state of the virtual machine. It stores the running state of the VM.
Database file	.vmsd	It contains the source information for the snapshot manager. It also defines the relationships between the parent and the child snapshots.

Malware attacks, once penetrated in to the virtual machine can change, modify and alter the kernel code and data, especially the kernel rootkits. In particular there are many types of attacks, namely the virus, the worm, the Trojans, the Adwares, the spywares, the rootkits, the backdoor, the ransomware, the Remote Administration Tools (RAT) and the key loggers. For our purpose of study, the analysis is drawn from a victim VM under a malware attack. The malware for our experiment are the TeslaCrypt (type of ransom ware), the Zeus (botnet), and the CyberGate, DarkComet and Xtreme (RAT). The effect of these malware on the memory of a virtual machine has to be considered. For this purpose, samples of the malware dataset is taken and induced into the

virtual machine with the help of software penetration tool, namely the metasploit. The binary analysis of the memory is obtained and the effect of these malwares is analyzed. Virtual machines are created, with one VM assigned as the attacker and the other VM assigned as the Victim VM. As the created VM's have a property of being in isolation, steps are taken to connect the VM's. Specifically, we try to create an inter-communication attack between the two VM's created. The memory snapshots are obtained for the victim VM and further analysis is made by the Cuckoo Analyzer Sandbox.

2.1. Experimental Setup

Each VM instance in the open stack private cloud setup consists a of the following specifications as given. Samples of the malware dataset are given as input to the victim VM from the attacker VM. In addition to this benign data is also input to the virtual machine. Then start tracing the victim VM for significant changes produced in the snapshot obtained. The severity of the attack is analyzed associated with changes that are occurred in the snapshots. The behavioral analysis is noted and the different malware attacks on the virtual machine have different severity levels. The analysis score is given by the cuckoo analyzer tool, which gives an indication of how severe the

malicious code has affected the VMs. The cuckoo analyzer tool uses a component called signatures to indicate the malicious behavior of the malwares in the victim VM. These signatures are indicated as the scores, which is nothing but the severity of the attack. There are levels of scores with 1 for low which may be an act of performing a query on a virtual machine, 2 for medium which may be an example like creating an .exe file in the virtual machine and 3 for high given to be for an example like removal of any files. The effect of these attacks is thus measured by the cuckoo analyzer tool.

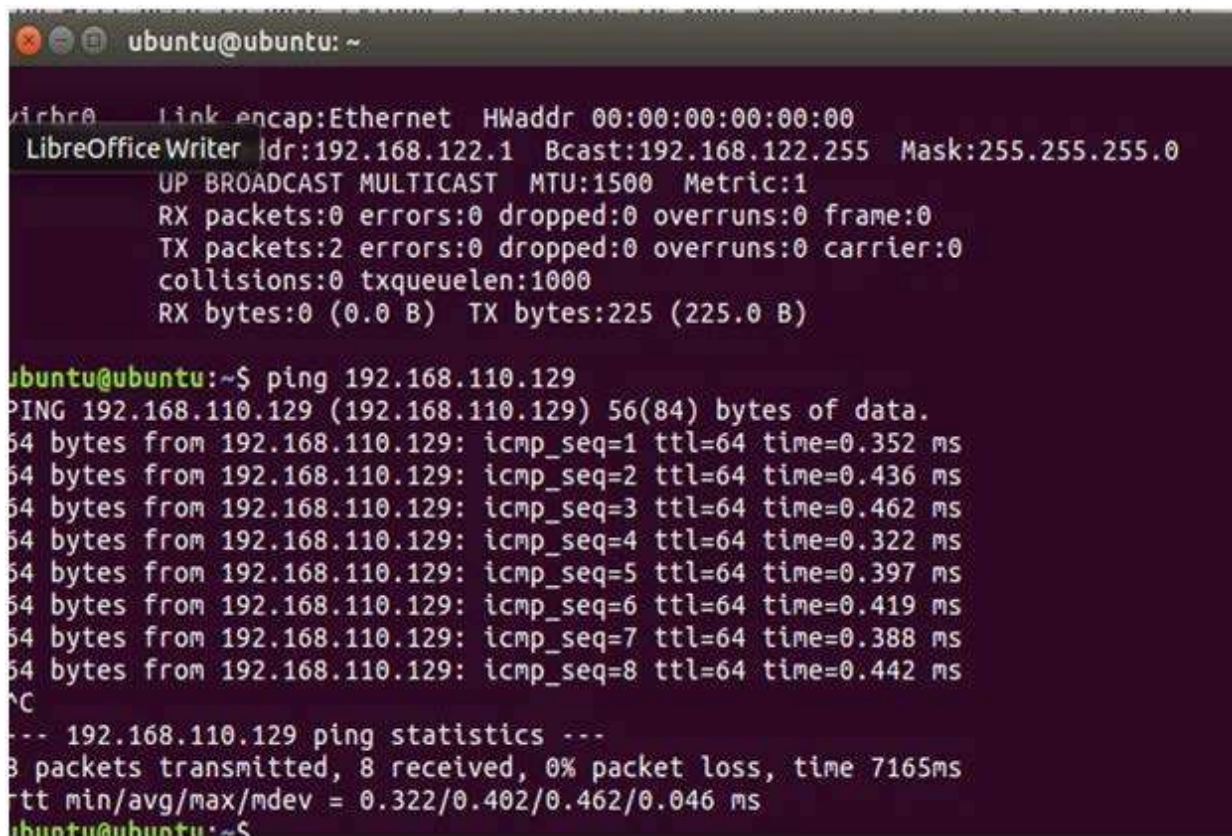
3. Results and Discussion

The average scores by the cuckoo analyzer tool for the different malware samples are given in table 3. All the malwares were computed for the scores by the analyzer.

Table 3: Cuckoo Scores for Malwares

Malware	Average Cuckoo Score
TeslaCrypt	5.46
Zeus	6.04
CyberGate	6.47
Xtreme	5.56
DarkComet	5.03

From the analysis, we find that different malwares have their own severity scores, indicating that the malwares all amount to more or less a similar effect on the VM Snapshots.



```

vibro eth0: Link encap:Ethernet HWaddr 00:00:00:00:00:00
LibreOfficeWriter |dr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:225 (225.0 B)

ubuntu@ubuntu:~$ ping 192.168.110.129
PING 192.168.110.129 (192.168.110.129) 56(84) bytes of data:
64 bytes from 192.168.110.129: icmp_seq=1 ttl=64 time=0.352 ms
64 bytes from 192.168.110.129: icmp_seq=2 ttl=64 time=0.436 ms
64 bytes from 192.168.110.129: icmp_seq=3 ttl=64 time=0.462 ms
64 bytes from 192.168.110.129: icmp_seq=4 ttl=64 time=0.322 ms
64 bytes from 192.168.110.129: icmp_seq=5 ttl=64 time=0.397 ms
64 bytes from 192.168.110.129: icmp_seq=6 ttl=64 time=0.419 ms
64 bytes from 192.168.110.129: icmp_seq=7 ttl=64 time=0.388 ms
64 bytes from 192.168.110.129: icmp_seq=8 ttl=64 time=0.442 ms
^C
--- 192.168.110.129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7165ms
rtt min/avg/max/mdev = 0.322/0.402/0.462/0.046 ms
ubuntu@ubuntu:~$

```

Fig. 3: vm1 Pinging to vm2

An inter communication is made between the two virtual machines. As virtual machines have the property of isolation, they can be communicated by the following steps:

- Create two virtual machine using Ubuntu 16.04 iso image.
- Install required packages.
- Get ip address of virtual machine by typing ifconfig in terminal.
- In terminal, type and ping ip addresses on both vm's.
- Check packets transmitted and received.

In order to transfer a file between two virtual machines

- Create vm1 as server and vm2 as client.
- Install python packages on both the virtual machines.
- Open and Run the server script by typing:
 - python server.py -u username -p password
- Open and Run the client script by typing:

- python client.py -u username -p password
- The username and password has to be matched for both the server and client.
- After the client is connected you need to provide the server's ip address for the connection to complete.
- Once connection is established, you can download any file from vm1 to vm2.
- Command to download is dl<filename>.

The figure 4 shows the comparative analysis of the different malware attacks on the virtual machines. The memory snapshot of the victim VM is obtained and binary analysis on the snapshot is performed and tested with the cuckoo analyzer tool to obtain the expected results.

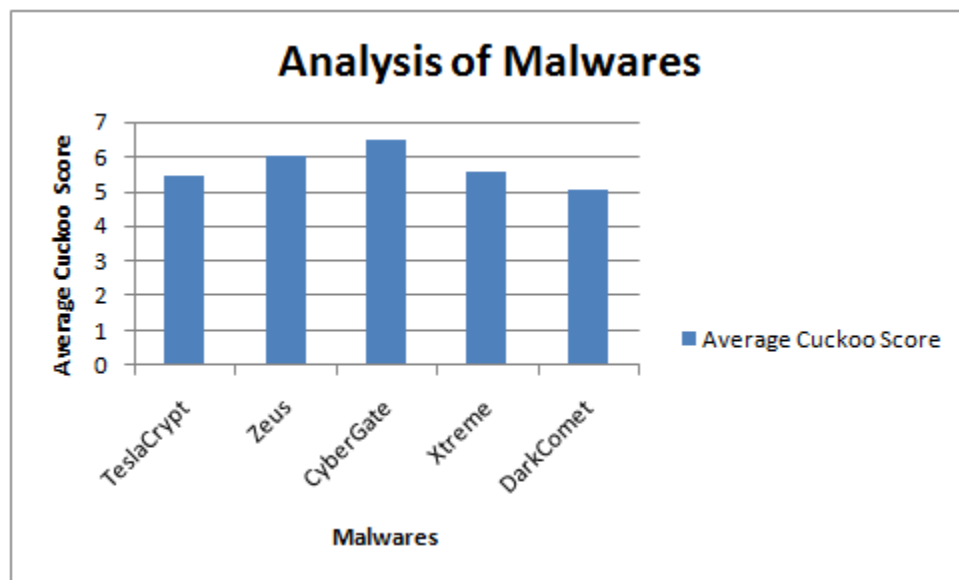


Fig. 4: Comparative Analysis of Malware Attacks of VM's

4. Conclusion

Research on virtual machines in cloud computing is very enormously active nowadays, from developing possibilities to provide security to popular systems like KVM, XEN or VMW are solutions. This paper makes an analysis of the 3 different families of malware attacks namely the families of ransom are, the botnet and the RAT. The severity of the attacks is obtained by the cuckoo analyzer. Further improvements can be made possible by detecting and classifying by using the machine learning algorithms on the attack analysis made on the VM snapshots. The cuckoo analyzer just indicates the severity of the malware attacks but does not give a classification of these malwares. So, in order to give an accurate classification of these malware attacks, we go for identifying machine learning algorithms to classify and possibly to detect the type of malware attacking the

system, thus once a malware makes a breach on the victim VM, it identifies and prevents itself from further attacks. It has also to be seen that no additional overhead is made possible in the implementations and thus make a decrease in the efficiency of the system. Therefore a security system based on anomaly detection with autonomic computing can be proposed to provide a correct balance in the performance and security.

5. References

- [1] More, A. and Tapaswi, S. Virtual machine introspection: towards bridging the semantic gap. *Journal of Cloud Computing* **3** (1) (2014) 1-16.
- [2] Prakash, A., Venkataramani, E., Yin, H. and Lin, Z. On the Trustworthiness of Memory Analysis An Empirical Study from the Perspective of Binary Execution. *IEEE Transactions on Dependable and Secure Computing* **12** (5) (2015) 557-570.
- [3] Sevak, B. Security against side channel attack in cloud computing. *International journal of engineering and advanced technology (IJEAT)* **2** (2) (2013).
- [4] Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M. A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing* **63** (2) (2013) 561-592.
- [5] Los, R., Shackelford, D. and Sullivan, B. The notorious nine cloud computing top threats. *Cloud Security Alliance*, 2013.
- [6] Joseph, L., Renjit, J.A. and Kumar, P.M. Dynamic programming based encrypted reversible data hiding in images. *Journal of Applied Security Research* **8** (4) (2013) 467-476.
- [7] Ferrie, P. Attacks on more virtual machine emulators. *Symantec Technology Exchange*, 2007.
- [8] Obasuyi, G.C. and Sari, A. Security challenges of virtualization hypervisors in virtualized hardware environment. *International Journal of Communications, Network and System Sciences* **8** (7) (2015) 260-273.
- [9] Grobauer, B., Tobias, W. and Elmar, S. Understanding cloud computing vulnerabilities. *IEEE Security & Privacy* **9** (2) (2011) 50-57.
- [10] Ibrahim, A., Hamlyn-Harris, J., Grundy, J. and Almorsy, M, Cloud sec: A security monitoring appliance for virtual machines in the IaaS cloud model. *5th International Conference on Network and System Security(NSS)*, 2011, 113–120.
- [11] Studnia, I., Alata, E., Deswarte, Y., Kaâniche, M. and Nicomette, V. Survey of security problems in cloud computing virtual machines. *Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012). Cloud and security: threat or opportunity*, 2012, p-61-74.

- [12] Jamkhedkar, P., Szefer, J., Perez-Botero, D., Zhang, T., Triolo, G. and Lee, R.B. A framework for realizing security on demand in cloud computing. *IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom)*, 2013, 371-378.
- [13] Popović, K. and Hocenski, Ž. Cloud computing security issues and challenges. *MIPRO 33rd international convention*, 2010, 344-349.
- [14] Vista, S. Kernel for Fun and Profit. *Joanna Rutkowska, Advanced Malware Labs, COESEINC, © SyScan*, 2013.
- [15] Rutkowska, J. and Tereshkin, A. Blue pilling the xen hypervisor. *Black Hat USA*, 2008.
- [16] Subashini, S. and Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications* **34** (1) (2011) 1-11.
- [17] Selvam, L., Kumar, P.M. and Renjith, J.A. Encryption-based secure sharing of data with fine-grained access control in public clouds. *Journal of Applied Security Research* **9** (2) (2014) 172-184.
- [18] Zhang, T. and Lee, R.B. Monitoring and Attestation of Virtual Machine Security Health in Cloud Computing. *IEEE Micro* **36** (5) (2016) 28-37.
- [19] Xie, X. and Wang, W. Rootkit detection on virtual machines through deep information extraction at hypervisor-level. *IEEE Conference on Communications and Network Security (CNS)*, 2013, 498-503.
- [20] Yang, Y., Mao, B., Jiang, H., Yang, Y., Luo, H. and Wu, S. SnapMig: Accelerating VM Live Storage Migration by Leveraging the Existing VM Snapshots in the Cloud. *IEEE Transactions on Parallel and Distributed Systems*, 2018, 437-441.
- [21] Zhang, F., Chen, J., Chen, H. and Zang, B. Cloud Visor: retrofitting protection of virtual machines in multitenant cloud with nested virtualization. *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, 2011, 203-216.
- [22] Xiao, Z. and Xiao, Y. Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials* **15** (2) (2013) 843-859.