ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Cloud Forensic Investigation using VM Snapshots and Log Information

Nilima Mitragotri[1], Prof M.A.Nirgude[2]

P.G. Student, Department of Computer Science and Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India[1]

Assistant Professor, Department of Information Technology, Walchand Institute of Technology, Solapur, Maharashtra, India[2]

ABSTRACT: Cloud computing systems host most of today's commercial business applications which makes it a target of cyber-attacks. This highlights the need for a digital forensic mechanism for the cloud environment. Conventional digital forensics cannot be directly presented as a cloud forensic solution due to the multi-tenancy and virtualization of resources prevalent in the cloud, as it has to address various technical, legal, and organizational challenges typical to the cloud systems. While doing cloud forensics, the data to be inspected are cloud component logs, virtual machine disk images, volatile memory dumps, console logs. The dynamic idea of cloud computing enables abundant chances to empower digital investigation in the cloud platform.

KEYWORDS: Cloud computing, Virtual Machine, Intrusion Detection system, Forensic Investigation, VM Snapshots, Attacks

I. INTRODUCTION

Cloud computing is the rising essential model for conveying information technology (IT) administrations to Internet associated devices. It extracts away the physical compute and communication infrastructure, and allows customers to rent, instead of own and maintain, as much compute capacity as needed [1].

The cloud service model, enabled by a number of technological developments, is primarily a business concept, which changes how businesses use and interacts with it.

Business houses migrate to cloud after verifying the security mechanism of the cloud service provider's infrastructure. Though the security mechanisms employed are good, due to the huge revenue involved in cloud, it is an easy target for hackers, crackers and other unethical online intruders. If the cyber-crime breaches the installed security system, then forensics can be used to find the evidence and prove the guilty before the court of law. Digital forensics is traditional computer forensic science which involves the process of seizure, acquisition, analysis and reporting the evidences in traditional OS images, USB drives and hard disks [2].

Cloud and forensic is interrelated. Traditional analytical model of digital forensics has been client-centric, investigator works with physical evidence devices such as storage media or integrated computer devices (e.g., smartphones). On the client (or standalone) device it is easy to identify where the computations are performed and where the results/traces are stored. Therefore, research has focused on discovering and acquiring every little piece of log and Timestamp information [5].

VMs are rapidly gaining popularity due to their ability to emulate computing environments, isolate users and support remote initialization. Prevention of unauthorized or malicious activities in cloud is a major challenge. So there is need of performing Digital Investigation on the cloud platform which leads to propose a technique that will be able to prevent the unauthorized activities on VM.

We propose an approach to forensic investigation, using Log Information and VM Snapshots of the malicious activities in the cloud environment. To ensure the security of Log files we aim to apply Encryption algorithms to Log information, which will be helpful for further investigation.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

II. LITERATURE SURVEY

A critical assessment of the work has been done so far on Cloud Forensics to show how the current study related to what has already been done. DeeviRadha Rani and Geethakumari G [1] proposed the technique of Forensic investigation of VM using snapshots as evidence that can be shown as a proof in front of court of law. In that mechanism, software stored and maintained snapshots of running VM selected by the user which acted as good evidence.
BKSP Kumar RajuAlluri and Geethakumari G [2] presented a Model for the self-analysis of VM. They split the entire Introspection into three parts as follows. a) Analysing virtual machines by taking into consideration the swap space where the continuous monitoring of swap space is done. It provides the information about current process of the VM. b) A self-analysis method for VM instances. In this three models were used, to collect as much accurate data evidence can be collected and reduce the semantic gap. But later, out of these three methods in-band method was proved to be less useful for live forensic as it modified the data at the time of collection phase. c) A Terminated Process based Introspection for Virtual Machines in Cloud Computing. This work can be useful in current research if incorporated as a part of the investigation process. Saibharath S and Geethakumari G [3] have implemented a data collection and rendering mechanism for cloud through hadoop file system using struts 2.0 MVC framework integrated with hadoop and cloud, a web software tool has been successfully implemented to do cloud forensics. Pre-processing of the evidence files have performed through log and VM disk drives clustering. It helps in minimizing the time of forensic investigation. Curtis Jackson1, Rajeev Agrawal2, Jessie Walker3, William Grosky4 [4] proposed virtual environment for testing utilizing Proxmox, an open source virtualization management tool, and KVM, a virtualized environment. Initially they have captured data from VM. In phase 2 investigation of the Virtual Machine Monitor has been done. Comparing the datasets from the initial attack scenarios to the Virtual Machine Monitor's data, they have identified and verified the activity for threats and normal activities. Ting Sang[5] stated a log-based model which can help to reduce the complexity of forensic for nonrepudiation of behaviours on cloud. However, it is totally no enough for the other kinds of digital forensics. FilipoSharevski [6] presented an initial effort to describe the potential privacy implication that might arise during the cloud forensic investigation. Additionally, he has approached every dimension of the cloud investigation process with a set of preliminary recommendations that can greatly contribute in the formal definition of privacy requirements in the extremely complex cloud environment. The work presented here is generic in nature and can be easily extended to cover privacy aspects in different cloud service or deployment models against various types of cybercrimes, cyber-attacks or incidents that may have potential impact on the cloud entities' privacy.

III. METHODOLOGY OF PROPOSED SYSTEM

There are too many systems which are used for attack detection and forensic IDS in cloud environment. The traditional digital forensic process undergoes the following steps which can be incorporated in cloud forensics considering its different service and deployment models.

- Identification of malicious activity
- Collection of Evidences
- Examination
- Analysis
- Reporting & presentation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

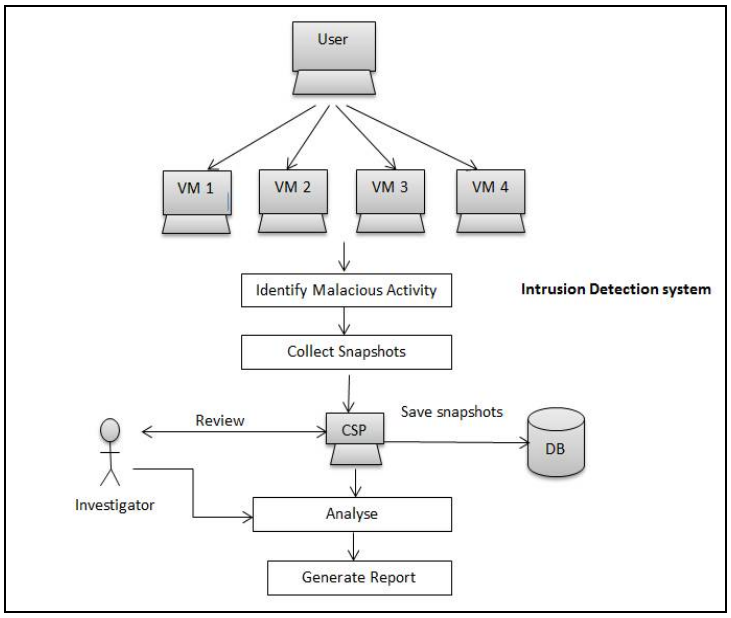

Figure 1: System Architecture

Earlier methodologies of cloud computing has generated too many snapshots to prevent the malicious activities from attackers. Some approaches generate snapshot in very high quantity even when user follows the normal activities, so it leads to high time complexity issues for investigator for manual verification. The challenging work of this system to eliminate the high time complexity using on demand snapshot generation when malicious activity has generated.
We have implemented a system which incorporates Intrusion Detection System on VMs which allows it to monitor itself and on VMM to detect malicious activity between VMs. Intrusion Detection Systems (IDS) are incorporated in all the VMs for monitoring malicious activities as shown in above figure. Deploying, managing and monitoring the Intrusion Detection System are done by cloud service provider.

We have incorporated Intrusion Detection System on multiple VMs which allows it to monitor itself and to detect malicious activity between VMs. We have used Amazon EC2 as cloud service provider to create VMs.
Figure 1 shows architecture diagram of the proposed system.
Users will make a request to create a VM by logging onto the cloud portal after the VM is created and ready to use, the user will gain total control of VM as shown in Figure 1. Malicious activities will be identified by IDS when users of that VM perform any activity like dos attacks, crashing server, cracking passwords, wrong OTP attack, and SQL Injection attack. IDS will identify the suspected VM after it is identified to performing malicious activities, to collect proper and correct evidence, the suspected VM will be monitored for some more time. Simultaneously the CSP will request for log files of the suspected VM and the investigator will collect and processes the log files to obtain the evidence.
Once the investigator identifies the sources of evidence, the Ip-address of attacker VM will get blocked.
Thus the system provides prevention mechanism to preserve confidentiality, integrity, and authenticity of other VMs; also VM evidence will be protected from contamination and tampering by providing encryption to log files.

We have implemented the system which can be divided into three modules.

1. Attacker
2. Receiver
3. Investigator

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

1. Attacker:
In attacker module we have implemented SQL injection attack, DOS attacks, R2L attack. These attacks are performed on Virtual machines of amazon ec2 cloud.
SQL injection attack is implemented using cosine algorithm as described below. During search file of user module we can search keyword for that file. If keyword matches with file data then it will show file name. Also we have performed cosine similarity for keyword with SQL signature pattern to check and detect SQL Injection Attack. We have created matrix to define 16 pattern signature attacks that are stored in database Using Cosine similarity formula SQL injection attack is detected.

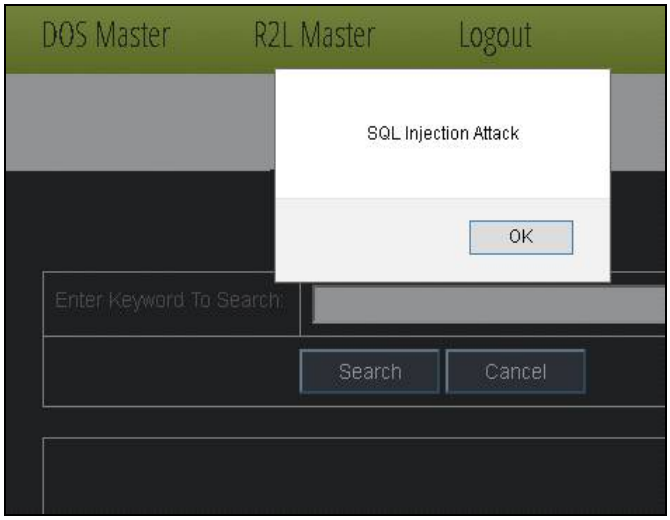

Figure 2: SQL injection attack Receiver VM

The cosine similarity between two vectors (or two documents on the Vector Space) is a measure that calculates the cosine of the angle between them. This metric is a measurement of orientation and not magnitude; it can be seen as a comparison between documents on a normalized space because we're not taking into the consideration only the magnitude of each word count (tf-idf) of each document, but the angle between the documents. What we have to do to build the cosine similarity equation is to solve the equation of the dot product for the $\cos\theta$:

$$\vec{a} \cdot \vec{b} = \|\vec{a}\| \|\vec{b}\| \cos\theta$$

$$\cos\theta = \frac{\vec{a} \cdot \vec{b}}{\|\vec{a}\| \|\vec{b}\|}$$

In Dos attack we have implemented LAND, Smurf, Remote shutdown, DOS nuke attack.
We have implemented LAND (Local area Network Denial) attack which is a DOS attack that consists of sending spoofed packet with the target host's IP address. This has caused the machine to reply to itself continuously.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

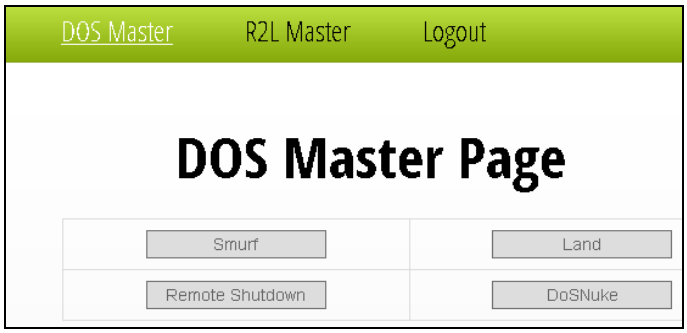

Figure 3: User Interface For dos attacks

We have implemented type of DOS attack smurf in which system is flooded with spoofed ping messages; this creates high network traffic on victim's network. We have hit following query for smurf attack
Process p1 = runtime.exec("cmd /c start taskkill /f /im explorer.exe");
Next we have implemented Remote shutdown attack by hitting following shutdown command. This has caused force shutdown of target computer.
Process p1 = runtime.exec("cmd /c start shutdown -s");
Figure 4 shows snapshot of attacker VM while performing remote shutdown attack by IDS

Figure 4: Snapshot of attacker VM for remote shutdown attack

DOS nuke attack is performed that is intended to disrupt a server. Following query is used to perform this attack.
Process p1 = runtime.exec("cmd /c start taskkill /f /im wininit.exe");
Next type of attack is Remote to local(R2L) attack; this attack can affect large number of computers in the world daily. Crashing remote server is one of the type of R2L attack .With the help of following query we have performed this attack on VM to crash the IIS server.Figure 5 shows the snapshot of IIS server on VM.

Process p1 = runtime.exec("cmd /c start net stop w3svc");

Figure 5:IIS server

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

We have also implemented OTP attack. We have assigned read and write permissions to the manager. When a user with read permission but no write permission tries to update or delete the contents of file then unique OTP is generated and this OTP is sent to manager's email id. As this user is not having access to get the OTP, he might enter random OTP to modify the contents of file. This activity is observed by IDS and compares the valid OTP with entered OTP. As OTP does not match IDS identify the wrong OTP attack. Figure 6 shows the snapshot of this attack taken by IDS.

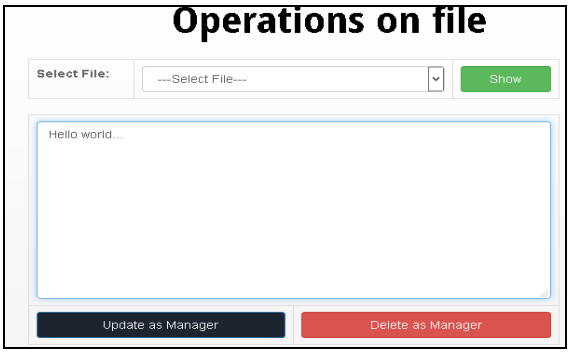

Figure 6: operations on file

2. Receiver
We have implemented Intrusion detection system ~~that is~~ continuously running on VM. IDS is created in such a way that as soon as malicious activity is observed it takes snapshots of attacker. For e.g. if user enters SQL injection signature like 1==1 or?? , this activity is observed by IDS. We have stored worldwide accepted 16 types of signature for SQL injection attack so if text entered by user matches one of these signatures then user is suspected as malicious user.

For DOS attacks Intrusion detection system matches the commands of attacks. If receiver VM gets force shutdown remotely then IDS compares this activity to shutdown –s command.

As soon as the attack is detected on receiver module, IDS system takes snapshots of malicious user on cloud. These snapshots are captured for 30 seconds of time interval because malicious user is observed for some more time in order to get more information in the form of snapshots. These snapshots are stored in database.

3. Investigator:
Investigator module is responsible for collection of snapshots Along with this Log Information of suspected VM is stored in to Log files. This log files contains IP address, MAC address of attacker VM.Also Date and time of attack gets entered in log files. Figure 7 shows snapshot of attack history of Investigator module. During log file creation we use Encryption scheme for securely store Log of attacker information. AES algorithm is used for log file encryption.

Figure 7: Attack history of investigator module

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Prevention mechanism is implemented in this module. As shown in Figure 8 when attacker is detected, IP address of that VM gets automatically blocked thus it provides prevention mechanism to Receiver VM, hence provides prevention from further activities. Figure 9 shows snapshot of attacker VM after it is prevented from further activities.

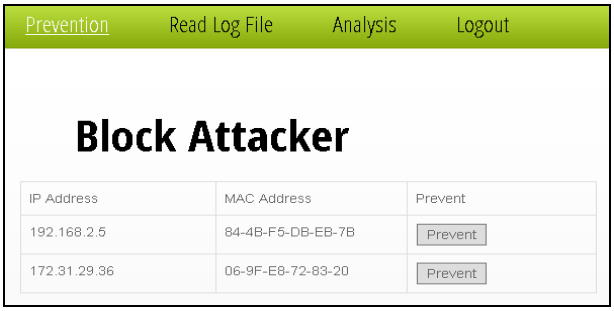

Figure 8: Prevention mechanism

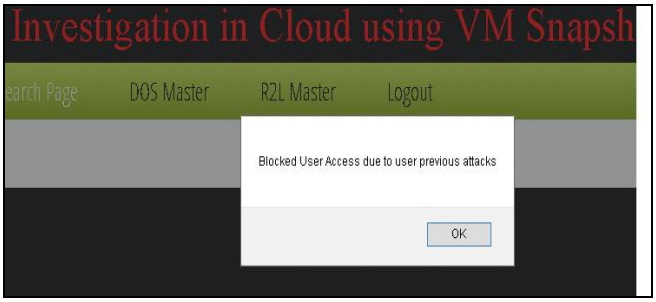

Figure 9: Blocked access after prevention

IV. RESULT AND ANALYSIS

We have implemented system to perform forensic investigation using VM snapshots as evidences along with log information about attacks. As shown in figure 13 attacker module enters the malicious query, this activity is identified by intrusion detection system. We have performed SQL injection, DOS attacks, Remote to local attacks, wrong OTP attack on VM, and we have got the following results during attack.
When user enters SQL injection signature like 1==1, snapshot of attacker VM is captured by IDS as shown in figure 10.

Figure 10: Snapshot of SQL injection attacker

Smurf is a type of DOS attack which crashes explorer of the operating system. Figure 10 shows snapshot of attacker VM captured by IDS.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Figure 11: Snapshot of Smurf attack

We have performed Remote to local attack, by crashing server on VM .Figure 12 shows snapshot captured by IDS during crash server attack.

Figure 12: Snapshot of Crash server attack

We have also implemented OTP attack, in which users with no right cannot modify the contents of file. Only manager can read and write to file. In spite of that if malicious user tries to modify the contents of file then OTP is generated and this OTP is sent to manager's email id.As this user have no access to get the OTP he might enter wrong OTP which leads to malicious activity. IDS identify this as wrong OTP attack and capture the snapshot of attacker VM. Figure 13 shows snapshot of attacker VM.

Figure 13: Snapshot of OTP attack

Along with the VM snapshots, log information of the attacks is maintained. This log information consists of date and time of attack, IP address and MAC address of attacker VM.Figure 14 shows the snapshot of Log information.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

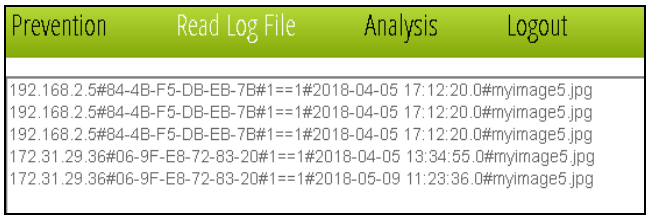

Figure 14: Log Information

All the existing approaches have implemented forensic investigation on single VM, whereas we have used multiple (four) VMs for testing different types of attacks.

V. CONCLUSION

In this work, we have proposed a novel way to deal with advanced forensics in the cloud condition by taking VM snapshot and Log Information as proof. The proposed approach takes snapshots of suspected VM and consequently enhances the execution of cloud, Log file is created which contains all Log information of attacker VM such as date and time of attack, IP address, Mac address, and investigator module can prevent the attacker VM to stop further attack by blocking the IP address (attacking VMs). We have shown better approach which have highest accuracy rate of attack detection.

The digital forensic framework that is suggested in this research can scale to cloud data for handling the analysis of the cloud crimes. The proposed method would help the forensic investigator in minimizing the overall processing time of a cloud crime under investigation. The digital forensic research community which is actively involved in the designing and development of the cyber forensic tools for cloud computing systems could consider the cloud forensic architecture presented in this work as a reference model. In brief, the work presented can be a way forward to combat cyber-crimes in cloud computing systems.

REFERENCES

[1] DeeviRadha Rani, G. Geethakumari "An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots" International Conference on Pervasive Computing (ICPC), 2015.
[2] BKSP Kumar RajuAlluri, Geethakumari G "A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing" IEEE, 2015.
[3] Saibharath S, Geethakumari G "Cloud Forensics: Evidence Collection and Preliminary Analysis" IEEE, 2015
[4] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenario-based Design for a Cloud Forensics Portal" IEEE, 2015.
[5] Ting Sang, "A Log-based Approach to Make Digital Forensics Easier on Cloud Computing"CPS,2013
[6] FilipoSharevski "Digital Forensic Investigation in Cloud Computing Environment: Impact on Privacy"
[7] Tao Xia, Guangzhi Qu, Salim Hariri and Mazin Yousif, "An efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm", IEEE, 2005.
[8] Amazon EC2 instances deletion in Cloud, https://aws.amazon.com/choosing-a-cloud-platform/?sc_channel=PS&sc_campaign=acquisition_IN&sc_publisher=google&sc_medium=cloud_computing_b&sc_content=sitelink&sc_detail=%2Bamazon%20%2Bclouds&sc_category=cloud_computing&sc_segment=choosing_a_cloud_platform&sc_matchtype=b&sc_country=IN&s_kwcid=AL!4422!3!92346737581!b!!g!!%2Bamazon%20%2Bclouds&ef_id=WKf9NAAAADDF7BAD:20170224152021:s
[9] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenario-based Design for a Cloud Forensics Portal" IEEE, 2015.
[10] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari "Providing Security and Integrity for Data Stored In Cloud Storage" ICICES, 2014.
[11] Cloud Tweaks, Cloud deployment Models,http://cloudtweaks.com/2012/07/4-primary-cloud-deployment-models/
[12] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics," Advances in Digital Forensics VII, vol. 361, no. IFIP Advances in Information and Communication Technology pp. 35-46, 2011.