# Feasibility Analysis for Incorporating/Deploying SIEM for Forensics Evidence Collection in Cloud Environment

Muhammad Irfan
National University of Sciences and Technology, Pakistan
muhammadirfan.msis12@students.mcs.edu.pk

Haider Abbas
Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
hsiddiqui@ksu.edu.sa
National University of Sciences and Technology, Pakistan
haiderabbas-mcs@nust.edu.pk

Waseem Iqbal
National University of Sciences and Technology, Pakistan
waseem.iqbal@.mcs.edu.pk

*Abstract*— **Cloud computing is the emerging field nowadays and it has truly revolutionized the domain of Information Technology. This domain is very large and not easy to handle especially when it comes to the forensic in a cloud environment that is considered a very cumbersome process. This paper presents a feasibility analysis of performing digital forensics via SIEM (Security Information and Event Management) system in cloud environment. The research work mainly focuses on passive attacks while some active attacks are also covered and the forensics analysis is done while considering the service provider end. The preliminary analysis presented in this paper will provide a comprehensive overview of the various artifacts that may be considered for performing an in-depth forensic analysis in cloud environment using Security Information and Event Management System.**

***Keywords—Cloud Forensics; Security Information and Event Management; Openstack; Ubuntu Enterprise Cloud***

## I. INTRODUCTION

The domain of Information Technology is progressing rapidly and this has brought significant improvements in the entire human life including business operations. Cloud computing for example, is one of the biggest revolution in field of Information Technology. It has changed the way in which IT performs and transformed the way in which services of IT are created, performed, outsourced and managed.

Cloud computing is a technology, utilized by using the internet only. On one hand cloud computing has given the large benefits, while on other hand it opens the door of security challenges. The most important concern now a days with respect to security in cloud environment is the cloud forensics and evidence collection in case of its misuse. Cloud service is still evolving and it is the perfect time to pay attention to cloud forensics which will help in preventing and fighting the malicious and illegal activities related to it [1].

The most important concern for cloud security is the size of cloud, cloud environment is so large that it is difficult to handle rapidly increasing threats and to see every aspect of security even by large teams in small cloud environment. So cloud forensics is much harder but a very important convergence presented in this paper can tackle proactively the security challenges in cloud environment.

Sometimes the convergence of some distinct things output a very useful end product. In this paper three different domains namely; Cloud Computing, Digital Forensics and Security Information & Event management are merged together for proactively fighting against the offensive security challenges. The end product will work rapidly in cloud environment and do the work of days and weeks in few minutes and hours. It will provide the clear picture of all the security events in a centralized location and help in preventing the advanced and sophisticated threats. So in this way, we can efficiently and effectively retrace the actions of cyber criminals, reconstruct raw data related to corresponding incident and do proactive measurement for keeping our whole cloud environment safe and running as per desire.

The paper is organized as follows; it starts with the basic overview of three important areas namely; cloud computing, cloud forensics and Security Information and Event Management System. Afterwards convergence of SIEM and digital forensics is presented in the cloud environment. Next, the feasibility model for this is proposed and discussed. Then using private cloud, experimental deployment and topology section cover the details of lab environment setup with the detail of attacks that are focused in this paper for forensic analysis using SIEM in the cloud environment.

The research findings and result section covers all the result that were found after the feasibility testing against respective attacks. The result and discussion section presents the result obtained from a systematic review. The analysis of the results is presented after this.

Finally, the conclusion and future work section ends up the paper with the conclusions along with the future intention of this research work.

## II. RESEARCH BUILDING BLOCKS

This section presents the overview of three main domains being focused during the research i.e. cloud computing, cloud forensics and Security Information and Event Management (SIEM). A brief description of each in the context of research emphasis is as follow:

### *A. Cloud Computing*

The cloud computing is considered a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing etc. It has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service [2].

There are several deployment models of cloud computing namely; private cloud, public cloud, community cloud, hybrid cloud and distributed cloud. Similarly in cloud environment we have three main service models namely; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Including these three main service models, several other service models also exist e.g. Desktop as service, Storage as a service, database as a service, Information as a service and Security as a service. There may also exist some services models but here only some major are highlighted.

Before using cloud environment it is necessary to determine the service model we are willing to use and its choice is dependent upon the service which is of our desire e.g. if our need is just deployment of a web application then our choice would be SaaS remaining will be done by service provider. We can also think about the service models in terms of the layers i.e. IaaS is the bottom layer, PaaS as middle layer and SaaS as the top most layer.

### *B. Cloud Forensics*

Now a days organizations are adopting cloud computing solution rapidly because of very charming benefits of cloud environment i.e. high availability, efficient speed, elasticity, more Scalability, large storage capacity, network access on demand and much more. This emergence has brought significant impact on the digital forensics in cloud environment. Cloud service providers lacks for a clearly defined processes for doing forensics investigation in a cloud environment which can be admissible in the court. And therefore cloud forensics becomes as great challenge for both the customer and the service provider end. This is mainly due to the decentralized nature of processing data in cloud environment. So the traditional approach of digital forensics is not very fruitful hence, we have to go beyond those traditional approaches although such approach is also mentioned in this paper.

In cloud environment a downtime of few minutes could lead a business to loss for millions therefore some proactive approach would be needed that help in tracing and mitigating the evolving threats. In customer end, for an organization whenever an incident occurs, they hire a forensic expert who will analyse the all available information and report the possible things. If he found that the attack is occurred from the service provider end network then he has nothing in his end rather than requesting a cloud provider for logs. At this point the challenging task is required because either provider don't bother for this or they don't have such forensics experts who might give us false information or hold back some very important information.

The service provider has to track all the logs and all artifacts should be characterized or segregated which is usually not done at service provider's end. So basically a well-defined mechanism would be needed that should gather all the needed information and store it at a central location for forensics purposes. This would help in getting information about the service model, virtualization, network traffic, operating system, file system, registry keys, processes, applications, middleware, storage and all other relevant information.

### *C. Security Information and Event Management (SIEM)*

Logs play a very important role in information security. They are very useful for analysing the network i.e. both internal and external, constantly so that an organization can be prevented from the breach or in case of any breach they should be aware of it and provide its effective incident response. Log management and monitoring itself is a very tough job. It is very difficult to see every single log from every appliance and timely finding out the root cause in case of incident. So there exist a SIEM Security Information and Event Management solution which will do all the desired work effectively and efficiently.

SIEM basically gather the logs from all the devices/appliances from the whole network at the centralized location and do normalization so that we can get an interpretable form of logs and then it will do correlation of all the logs/events using correlation directives and raise alarm in case of any suspicious activity. It also categorizes all the events, do risk calculation and presents reports which is highly scalable and easy to deal with.

There are several SIEM solutions available like QRadar by IBM [3], USM by AlienVault [4], Arc Sight by HP[5], Splunk by Splunk Enterprise[6] and Solar winds log and event manager by Solar Winds[7]. The research work presented in this paper uses USM by Alien Vault because of its availability, low cost and open source support.

AlienVault Unified Security Management™ (USM) is an all-in-one platform designed and priced to ensure that mid-market organizations can effectively defend themselves against today's advanced threats [8]. The AlienVault Unified Security Management™ (USM) platform provide five essential security capabilities in a single console, giving you everything you need to manage both compliance and threats. Understanding the sensitive nature of IT environments, it includes active, passive and host-based technologies so that one can match the requirements of his particular environment.

## III. Convergence of SIEM and Digital Forensics in Cloud Environment

Sometime the distinct areas of technology converge with each other and that convergence leads to a very useful end product. In similar fashion, a convergence of SIEM and digital forensics in cloud environment is expected to help in cyber security mechanisms and security professionals to deal with security challenges proactively.

SIEM provides a centralized monitoring and information of threats. It can be tuned to collect the information which is forensically important. This will help to get all the forensic data of a huge cloud environment in a central location and help in performing investigations on that centralized data. We may define our customized correlation directives and filters so that we can get as much evidence data as possible. It can also be used for providing the information of active/live threats and actions for defending against them.

## IV. Feasibility and Proposed Model

In this paper a feasibility analysis is performed to check how SIEM can be beneficial for getting forensic evidences in cloud/virtualized environment. For the initial testing purpose the SIEM solution i.e. USM (Unified Security Manager) by AlienVault was deployed and cloud environment under consideration was a private cloud that was deployed on Ubuntu Server using Openstack/DevStack. We deployed this whole setup for getting forensic evidences and information and analyse the feasibility of providing defence against cyber threats in virtualized/cloud environment.

In proposed model, there are mainly three phase's involved i.e. Input, Analysis and Output.

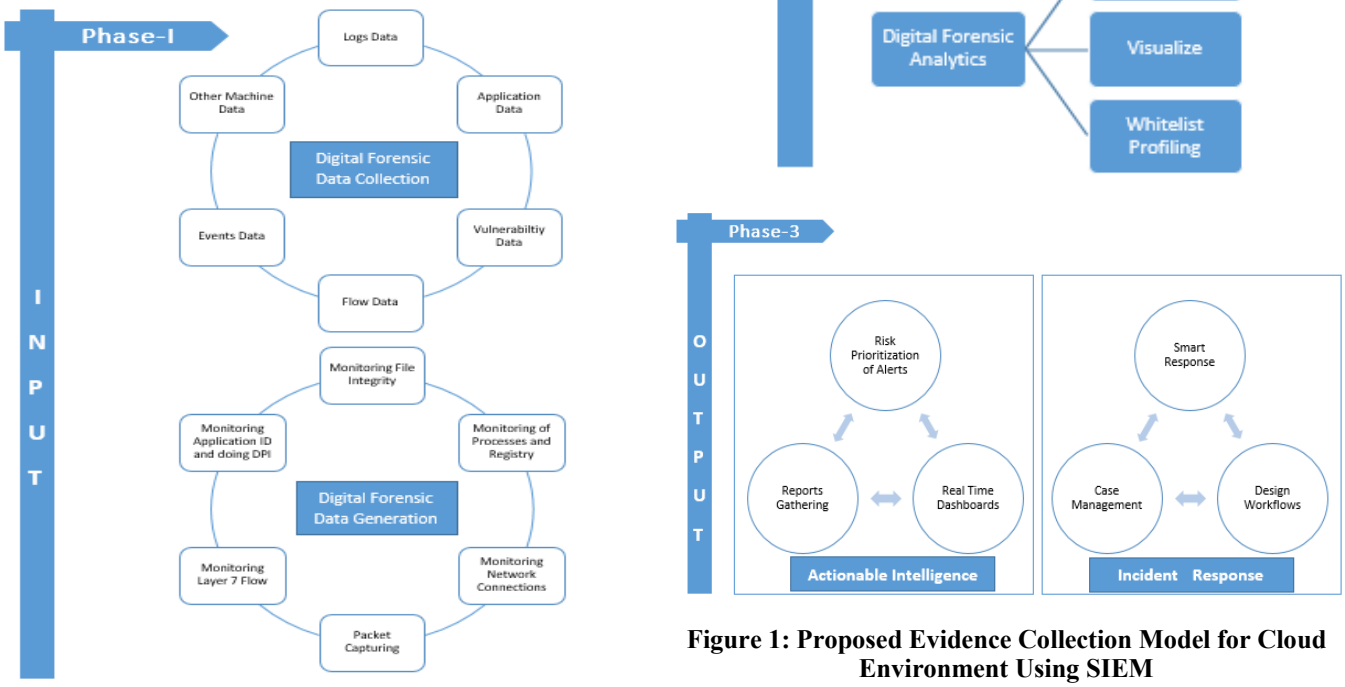


**Figure 1: Proposed Evidence Collection Model for Cloud Environment Using SIEM**

### A. Digital Forensic Data Collection

In first phase of Input, our primary goal is the forensic data collection. We will deploy the SIEM sensors or configure our assets in a manner so that they will provide us the desired data for carrying out forensic investigation. This data includes:

- Logs Data.
- Applications Data.
- Vulnerability Data.
- Flow Data.
- Events Data.
- Other Machine Data

### B. Digital Forensics Data Generation

In Forensic data generation, we basically do the host and network level forensics. This data includes the following things:

- Monitoring File Integrity.
- Monitoring of Processes and Registry.
- Monitoring Network Connections.
- Packet Capturing.
- Monitoring Layer 7 Flow.
- Monitoring Application ID and doing deep packet inspection.

### C. Real Time Processing

After the input phase the analysis phase starts, in analysis phase the first thing is the real time processing. In this phase of real time processing following things will be covered:

- Classification of Data.
- Extraction of Meta Data.
- Time Normalization.
- Context Infusion.
- Risk Prioritization.
- Indexing
- Persistence.

### D. Machine Analysis

In analysis phase after the real time processing, machine analysis is done. It includes:

- Advance Correlation.
- Behavioural and Statistical Baselines.
- Pattern Recognition.
- Whitelist Profiling.

### E. Digital Forensic Analytic

Once Real time processing and machine analysis is done in analysis phase, we finally do the forensic analysis of all the data. All this data can be filtered via following:

- Search.
- Visualize.
- Pivot/Drill Down.

### F. Actionable Intelligence

Once the analysis is done we do actions in output phase. In actionable intelligence we do:

- Risk Prioritization of Alerts.
- Real Time Dashboards.
- Reports Gathering.

### G. Incident Response

At last, incidence response is done. It is the most important of the all. In this following is carried out:

- Smart Response.
- Design Workflows.
- Case Management.

Once all three phases i.e. input, analysis and output are completed we end up with the successful defense against the incident.

## V. Experimental Lab Deployment And Topology

To start with we have deployed the lab for our feasibility testing. A private cloud is deployed using Openstack and different instances are hosted on it. Here instance mean a virtual machine is deployed. As we are considering a scenario of forensic from ISP side so one instance of SIEM also reside in this cloud environment. For setting up cloud environment Ubuntu server 14.04 LTS is installed and above that Openstack/DevStack is configured using guideline mentioned in [5][6][7][8]. The lab is setup upon VMware ESXi 5.5 OS whose underlying hardware is HP ProLiant BL460c Gen8 Blade Server with 16CPUs of 2.988 GHz and 64GB of RAM. As far as networking is concerned vSphere standard virtual switch is used for the communication between the machines, in other words, virtual networking feature of VMware ESXi is used. Following are the instances which are included in our cloud environment;

- MS Windows 8.1 Virtual Machine.
- MS Windows 7 Virtual Machine.
- MS Windows XP Virtual Machine.
- MS Windows Server 2008 R2 Virtual Machine having Active directory and DNS configured.
- Kali Linux Virtual Machine.
- VMware ESXi 5.1 Host Virtual Machine.
- AlienVault Unified Security Manager Virtual Appliance.
- Solar winds Log and Event Manager.

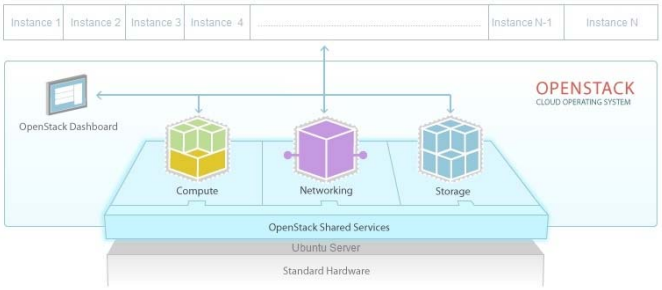


**Figure 2: Openstack Cloud Environment [10]**

Initially following are the attacks that were aimed to detect in the cloud environment using the Alien vault USM SIEM

solution. Some of these attacks are active attack and some are passive. Some are monitored on real time and some are analysed after incident. Future goal is to monitoring passive attacks and using raw logs we can extract the data of interest for forensic investigation purpose. These attacks include various categories for example in network level attacks i.e. Denial of Service (DOS) Attack, session hijacking attack involves ARP Poisoning/Man in the Middle Attack, password guessing attack includes Brute Force Attack, malicious program includes Infected Media Plugged Detection and Malicious Application Installed and other attacks include Network Flow Anomaly Detection, Vulnerability Detection in specific OS/application, Data Breaches, Data Loss, Service Traffic Hijacking and Insecure APIs.

For this setup attacking machine lies within the cloud environment. It is one of the virtual instance of the cloud environment. It is also possible that it can be placed out-side of the cloud network and used to compromise the cloud network. As far as scope of this paper is concerned the attacking machine lies inside the cloud environment. Secondly, for the purpose of virtual instances monitoring agent based approach is used to collect logs at a centralized location. For monitoring of network traffic the syslog of virtual switches are configured so they may also send logs at centralized location; the SIEM Solution.

## VI. Research Findings And Results

Some attacks were performed in the above mentioned lab setup and tested if the SIEM solution works well for this. The Alien Vault SIEM was properly configured and was getting all events from the respective targets. It was due to the detailed configurations that were done for setting up SIEM. Basically Alien vault USM SIEM came as a virtual appliance e.g. *.ova or *.ovf file. This virtual appliance is then accessible on any virtual editor like VMware, Virtual box or any cloud environment as an instance. It is preconfigured, we will just open it in virtual environment and follow on screen steps for configuration. Its sensors and plugins are installed like a normal windows or Linux application or binary program. We can also configure devices like routers, firewalls, servers and other similar devices to forward their logs to SIEM or its sensor via syslog for central monitoring. More details are mentioned in [9] and [10]. Attack wise finding details are as follows:

### *A. DOS Attack*

In the Lab environment, we used a tool name LOIC for performing the Denial of Service attack on the windows 7 virtual machine. Figure 3 shows the GUI of LOIC performing DOS attack on windows 7 target machine.

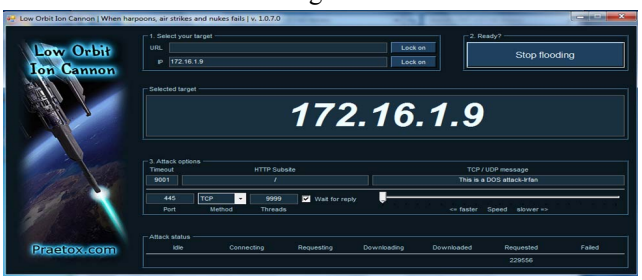


**Figure 3: DOS Attack using LOIC**

The 9999 threats were used using LOIC and 229556 TCP sessions were opened for this DOS attack. An OSSEC agent is configured on windows machine so that it will report all activities to Alien Vault USM SIEM at the central location. Figure 4 below is the logs on Alien vault USM that will show a small level DOS attack attempt is being done on the windows machine.

By default, the risk for such small level DOS attack is low in AlienVault USM but for priority we can tune it in a manner that it will trigger an alarm for such small level DOS attacks

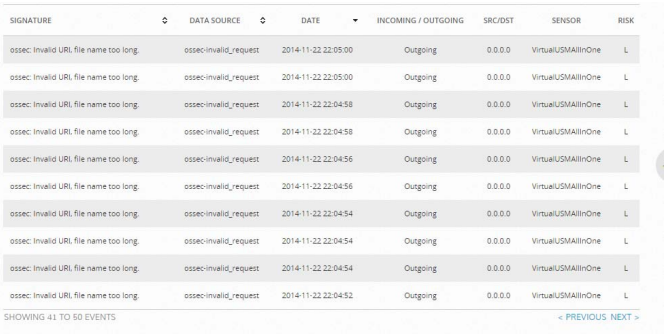


**Figure 4: AlienVault USM Logs showing DOS Attack**

### *B. Brute Force Attack*

In the lab environment by using the Kali Linux a brute force attack is performed on a windows machine. On kali Linux msf console is being used for performing the attack. Figure 5 below show the attack;

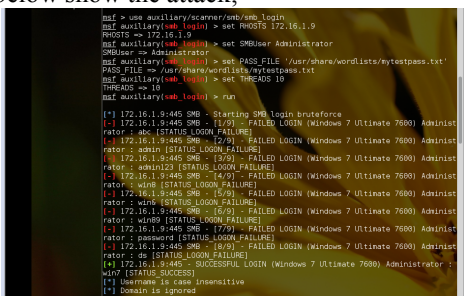


**Figure 5: Brute Force Attack using Kali Linux**

As ossec agent is already deployed on windows machine so we will get all the logs and events of windows machine at the centralized location at Alien vault USM. Figure 6 below shows the logs observed on web console.

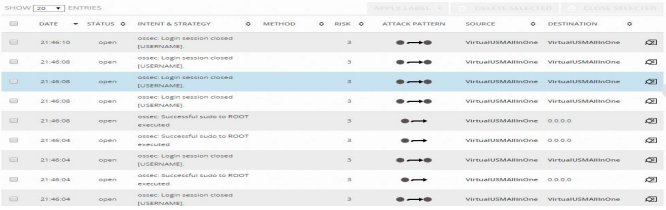


**Figure 6: AlienVault USM logs Showing Brute Force Attack**

In ossec by default, the risk for brute force attack is 3 out of 10. We can change this manually according to our requirements. Here as shown in Figure 7 as the brute force is detected so the alarm is triggered against it. In this manner we are aware of such events easily and perform actions against them accordingly.

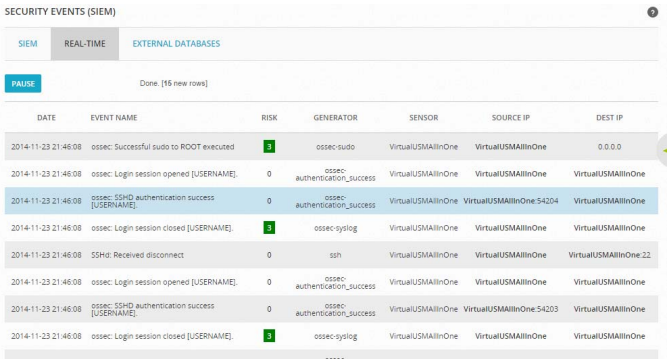


**Figure 7: Alarms Triggered in AlienVault USM against Brute Force Attack**

This Figure 7 above clearly shows the triggered alarms, their time stamps and associated risk. This can be very useful for the SIEM administrator for performing the incident response against such events.

*C. Monitoring Network Flows*

There are multiple ways for monitoring and analysing the traffic. We can monitor the network flows in the real time so we may analyse the things forensically and perform better incident response and it also secures the evidences. Figure 8 shows the real time network flow of the same brute force attack.

This gives a better understanding of how attack is started, what actually happens and where it ends. In other words it can be said that the detail analysis of whole traffic or the specific captured packets is conducted. So this will be very handy for the security personal, especially from forensics point of view.

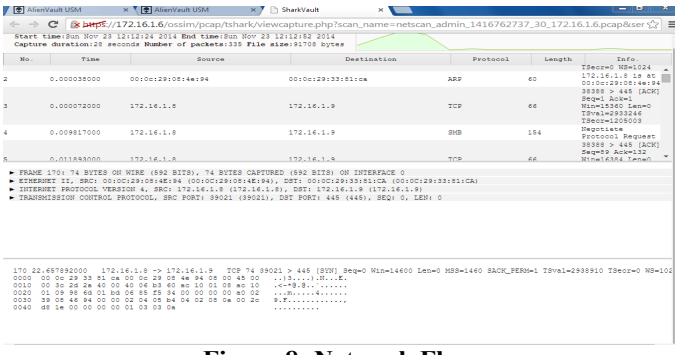

**Figure 8: Network Flow**

*D. Malicious/Unknown Application Installation Detection*

An unknown application is being installed on windows machine. Normally antivirus will detects the unknown applications but this standalone solution also does the work of malicious or unknown applications detection. It will log the installation of unknown application on the operating system and also trigger alarms for it so that respective administrator takes an action against such application e.g. isolate the system, stop spreading the malware, remove malware or ignore it if it is considered as a non-malicious program in his environment. Figure 9 below shows the detection of unknown application in Alien Vault SIEM. Triggered Alarms are also shown in figure 10.

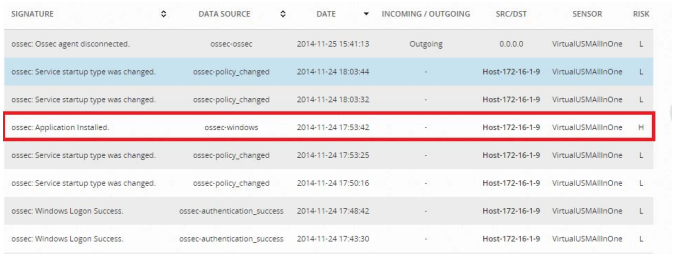


**Figure 9: Malicious Application Detection**

By default, the risk of this is high and triggered alarm have default risk value 8. We may change it manually as per our own environment.

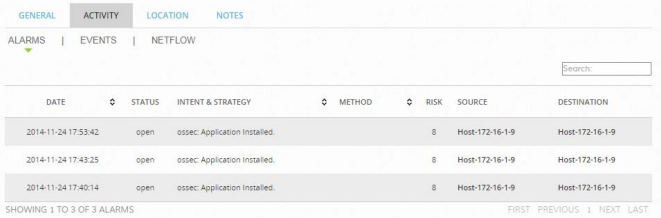


**Figure 10: Triggered Alarm**

*E. Vulnerability Detection*

Alien Vault USM have built-in vulnerability scanner. It can check for the latest vulnerabilities from its threat database. It also has a feature of open threat exchange so that we get awareness about latest threats automatically. Below Figure 11 shows the vulnerability detection on the VMware ESXi 5.1 virtual machine/instance. It identifies the vulnerability addressed by VMware in its ESXi 5.1 version.

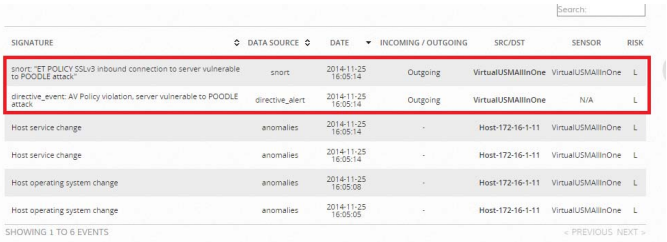


**Figure 11: Vulnerability Detection**

The above Figure 11 shows the signature of the vulnerability that is found in ESXi 5.1. The corresponding alarm triggered against this is shown in Figure 12 below:

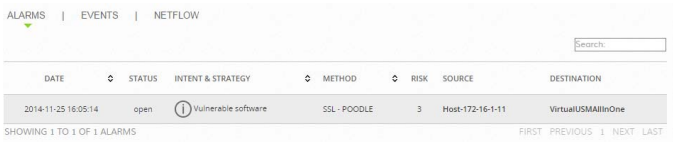


**Figure 12: Triggered Alarms against Vulnerability Detection**

The default risk value is 3 out of 10 and it is considered as low. We may tune it according to our environment.

## VII. Discussion and Analysis

This paper provides a preliminary investigation and feasibility analysis of incorporating security information and event management system in cloud environment for the purpose of forensic evidence collection in the cloud environment. The work was started with the deployment of private cloud environment using Ubuntu server and configured Openstack above it. Now on this private cloud environment several virtual instances were configured. These instances include several virtual machines and SIEM solution as mentioned before in experimental lab deployment and topology section. Then several attacks were performed in the cloud environment and we found that our SIEM solution is detecting those attacks and getting logs against those attacks. These logs are collected as a forensic evince. Initially both active and passive attacks were performed and all of them were detected by SIEM solution. Our SIEM solution also provide real time alerting for these incidents by generating alarms. Initially few attacks were focused and those are detected by our SIEM solution and forensic evidence of those are collected. Several existing IDS do such things but they may not correlate all security events at a centralized point. They may detect at a particular node or between a certain channels but SIEM gets events from everywhere and push it in a centralized location and make a correlation of it in order to better identify the attacks.

One challenge might be computing. As we know Deep packet monitoring, centralized log collections and complex correlation are the resource hungry processes. So this thing should be considered before deploying such solution that more will be CPU and Memory resources more efficient and effective will be the output.

All the results and finding shows that the proposed model is feasible and we can proceed with it for detection of more sophisticated attacks and their forensics.

## VIII. Conclusions And Future Work

The paper aimed to perform a preliminary investigation/feasibility analysis for deploying SIEM in cloud environment to collect forensics evidences from a service provider's perspective. The experimental setup deployment for launching attacks and analysis of the collected evidences shows the success and feasibility of SIEM deployment in cloud environment. The main focus was on passive attacks while some active attacks were also covered in this initial work. The future intention of this research is to extend the attacks vector stream with detailed analysis of all the factors that would in achieving more sophisticated and precise results that can be used at large scale for forensics purposes in cloud environments.

## References

[1]. Cloud Forensics. Retrieved on Nov 3, 2014 from http://www.techstagram.com/2013/03/20/cloud-forensics-importance/

[2]. Wentao Liu, "Research on cloud computing security problem and strategy," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on , vol., no., pp.1216,1219, 21-23 April 2012

[3]. IBM Security QRadar SIEM, Retrieved on Jan 10, 2014 from http://www-03.ibm.com/software/products/en/qradar-siem

[4]. AlienVault. Retrieved on Jan 10, 2014 from https://www.alienvault.com/

[5]. Security Information and Event Management. Retrieved on Jan 10,204 from http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/

[6]. Splunk Retrieved on Jan 10, 2014 from http://www.splunk.com/

[7]. Log and Event Manager. Retrieved on Jan 10, 2014 from http://www.solarwinds.com/log-event-manager.aspx

[8]. AlienVault USM. Retrieved on Nov 9, 2014 from https://www.alienvault.com/products

[9]. Incident Forensics. Retrieved on Nov 10, 2014 from http://www-03.ibm.com/software/products/en/qradar-incident-forensics

[10]. Open Stack. Retrieved on Nov 15, 2014 from http://www.discoposse.com/wp-content/uploads/2013/02/alamo-30-designconcept.png

[11]. All-In-One Single Machine. Retrieved on Dec 5, 2014 from http://docs.openstack.org/developer/devstack/guides/single-machine.html

[12]. DevStack – an Openstack Community Production. Retrieved on Dec 14, 2014 from http://docs.openstack.org/developer/devstack/

[13]. Installing Ubuntu Server. Retrieved on Dec 14, 2014 from http://www.ubuntu.com/download/server/install-ubuntu-server

[14]. USM Virtual Appliance Quick Start Guide. Retrieved on Oct, 12 ,2014 from https://alienvault.bloomfire.com/posts/717426-usm-virtual-appliance-quick-start-guide/public

[15]. AlienVault Installation Guide. Retrieved on Oct 5,2014 from https://alienvault.bloomfire.com/series/2457/