International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-06, Issue-07, OCT 2020

Network Attack Vulnerability Detection Prevention and Forensic Techniques Using Various Soft Computing Algorithms

[*]Samira Prabhune, [#]Dr. Sivakumar Nadarajan

[*,#]Computer Science, Jain University, Bangalore, India

[*]sameera.prabhune17@gmail.com, [#]drsivakumar.nadaranjan@gmail.com

***Abstract*—A daunting activity is automated investigations on the cloud platform. The purpose but behind implementation of cloud forensic analysis is the protection of evidence. In the Virtual Case, there is proof of virtual machines. If the VMDK (Virtual Machine Disk file) is lost, the VM cannot be restored. There is no sustained customer at current that can restore a destroyed (deleted) VM again, which is the VM itself fault. All activities on the VM are reported to the VM, while Cloud Service Provider (CSP) operations are reported to the server. So, even though anyone deletes the VM, all the information is gone. This causes a tragedy for the client and serves as a deterrent to a private examiner digging out the sensitive or private important information that was often stored in the virtual environment. With this academic research, we developed to improve the existing processes and problems in the cloud storage scenario and suggest an idea to avoid the unauthorized deleting of snapshots from virtual machines.**

***Keywords*—Virtual Machine, Digital, Provenance, Isolating Cloud Instance, Regeneration of events, Regeneration of events.**

I. INTRODUCTION

Cloud is an evolving technology and cloud-based storage is the recently introduced term that not only makes it easier for customers to upload data to the internet, but also allows immediate access to appropriate resources and exchange data with others at any time. But Cloud is an innovation that poses a challenge for the individual who investigates and finds forensic data that can assist in forensic investigation as cloud-based information can be accessed anywhere across and from any device and very few indications are left around.

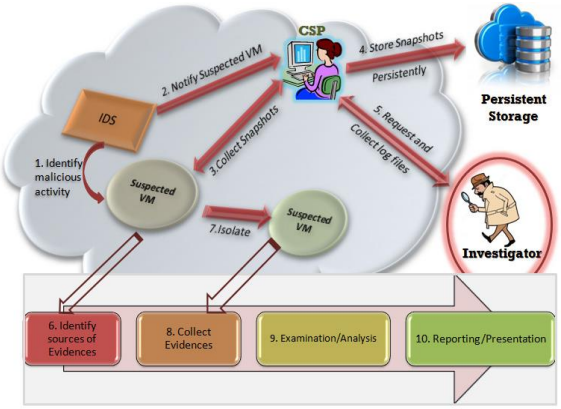

Figure 1 Current Cloud Scenario

The 21st century is known to be the age of digital world. There would be the introduction of machines to a great degree. Today, one could not live without computers and the Internet, because for almost all our function we rely on these devices. Considering everything including home to employment to banking and even corporate working, everything has since been automated into computers. In the digital format, electronic filters all our important data. With this, as seen in Figure 1 Existing Cloud Scenario, there is a need to store digital data also increased as well as the virtual world has surpassed the physical storage to store all our certificates. The cloud's greatest devastating challenge is to avoid unauthorized deletion of stored cloud data because without proper authorization, you can easily delete the things. Data deletion is entirely dependent on deleting nodes which point to a certain virtual machine information.

Various distributed computing expert co-ops are available in the cloud state with their administrations. These presidencies join different judgements, illustrates and technologies for fulfilling security. Some presidencies focus on secure access by encrypted data to administration and relevant data, and some focus on the secure server itself. Procedures obtained by various providers to achieve protection are of an evolving type. A cloud client may look for an administration based on an administration's need and level of protection. A test is to dissect a administration based on its various security properties. In terms of security, the real test is to believe in a cloud management or specialist organization. In an administration, one can try to demonstrate such "confidence," as a sort of confidence esteem. This theory explores the probability of a system such as a confidence computing process and its various aspects.

 DOI : 10.35291/2454-9150.2020.0654

II. LITERATURE REVIEW

So far, a critical review of the work on Cloud Forensics has been conducted to explain how the new research applies to what has already been conducted. Because of greater economic challenges, several businesses are now migrating to the cloud for a few days. But for small and medium-sized businesses, the primary concern is information security. The best choice for these businesses is to use a managed service, also known as an outsourced service, in which the entire service bundle, including antivirus software, is delivered for security consulting. And Security as a service (SECaaS) is the alternative model that provides such outsourced security. Together, scientists and researchers discussed their new ideas and observations about what the real world scenario is and what all attempts are being undertaken, but it was found that there is just a fraction of the overall work that has contributed to the wealth of society despite being so much research work in the field of cloud forensics. Cloud, though, came into being in the mid-90s, but it is not completely taken up by anyone. There has been a lot of work in this area before and several techniques for cloud forensic analysis, but there is a significant space for progress that needs to be carried further in the study.

A. Deevi Radha Rani and Geethakumari G have suggested an successful approach to cloud forensic analysis using VM snapshots [1].

The VM forensic investigation technique uses snapshots as evidence that can be shown before the court of law as proof. The software stored and maintained snapshots of the running VM selected by the user in that mechanism, which acted as good evidence. The user can build VMs from the physical machines available, according to his preference. Any cloud software like that of Eucalyptus instead of request of a user, takes the snapshots of the machines stores till terminated. Snapshots can only be stored until the maximum is reached, but the snapshots that were taken long before being deleted are reached when the maximum is reached. The enormous storage management of VM snapshots is therefore difficult as it impacts the system's efficiency.

1) Relation to current studies

The author suggested a model in this paper in which the VM was paired with an IDS. This helped to observe, by thoroughly observing, the disruptive activities being carried out between the VMs. The basic concept behind this work was to store the log of destructive activities in the form of snapshots using the IDS placed in the system. At the same time, the CSP was asked for the logs of the problematic VM, and the investigator retrieved those logs. In order to collect the proof that can support the investigator, the investigator then works on certain log files.

B. BKSP Kumar Raju Alluri and Geethakumari G, IEEE's Digital Forensic Model for Cloud Computing Introspection of Virtual Machines, 2015[2]

A model for VM self-analysis was presented by the authors. As follows, they break the entire introspection into three sections.

(a) Study of virtual machines by considering the swap space in which continuous swap space monitoring is carried out. This provides details on the current VM operation.

(b) For VM instances, a self-analysis method. In these three models, it was used to gather as much reliable data evidence as possible to obtain and reduce the semantic gap. But later, the in-band method of these three techniques was shown to be less useful for live forensics as it modified the data at the time of the collection phase.

(c) Introspection based on a terminated process for Virtual Machines in Cloud Computing. Every process that was terminated and later improvised was captured by this to capture only the processes that were found doubtful.

1) Relation to current studies

The suggested method for conducting introspection digital forensic observation in Cloud on VM that addressed the issues related to the assembly of evidence. They used some VM introspection techniques to overcome them. If integrated as part of the investigative process, this work could be useful in current research.

C. Hubert Ritzdorf Nikolaos, Karapanos Srdjan Capkun suggested [3] Related Material Supported Deletion in ACM, 2014

In their paper, Hubert and Karapanos discussed a system that allows the user of that system to reduce the content of any project's comparable and related files. In every way, this device did not influence the user or system components as it was guided to be embedded with the user system itself. This starts operating from the user space and maintains the files along with their metadata. When they completed their work, they found that it was possible to achieve the resulting precision and overhead. For the purpose of deployment, the findings were appropriate to be used. The aim of the system was to allow users to reduce all the related project files by showing them and it was successful in providing them.

1) Relation to current studies

Content deletion using assisted deletion of related content has been proposed here. All the relevant files were introduced to the user to be reduced in a securely structured manner. This has helped users to maintain the confidentiality of their information. This can also assist in current study, as any device offers facilities for removing files that can be combined.

 DOI : 10.35291/2454-9150.2020.0654

D. Mr. Digambar Powar and Dr. G. Geethakumari[4] Digital Evidence Detection at ACM for Cloud Computing in Virtual Environment, 2012

A technique for the Cloud Computing domain and it was called the technique of Digital Proof Detection at Hyderabad. In their work, several traditional approaches that were used as a tool for conducting forensic observations were explored and those approaches were helpful in learning and analyzing the behavior of digital evidence in a virtualized environment called the Cloud. The feasible solutions in which forensic procedures can be carried out in a simulated environment are also illustrated.

1) Relation to current studies

The author introduced the feasible solution in the above-mentioned research paper in which forensics can be practiced in a virtual environment. This work is a crucial stage because it leads to the collection and presentation of adequate data evidence that can be an aid to forensic investigators.

E. Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari proposed Provision of Data Stored in Cloud Storage Security and Integrity in ICICES, 2014[5]

In its research work, the author attempted to suggest a solution to minimize the workload and simultaneously provide the integrity and protection of the data stored in a well-organized manner on the Cloud. However, because the information stored on the cloud is not readily available to users, it is difficult to maintain its integrity. Therefore, the author has proposed a method that, once combined with SLA after agreement with CSP and user, allows users to test data integrity. The author has also sought to minimize the overhead of computation. They only performed encryption for certain bits out of the whole file block. As a result, the overhead was minimized on the side of the client and the scheme was thus more tolerated by the consumers.

1) Relation to current studies

The work presented in this paper takes due care of the information held on the cloud as it not only provides integrity control, but also data security. This allows us to test the integrity of the stored data from the cloud when it is retrieved.

III. METHODOLOGY OF PROPOSED SURVEY

A. Virtual Computer Introspection

It is a bashing-malware that measures and detects VM threats. Whenever the attack is identified, the attacked VM is evaluated by a Virtual Machine Monitor (VMM) or a VM running under the VMM. This method is called Virtual Machine (VMI) introspection and was first introduced by Garfinkel and Rosenblum. By performing Virtual Machine Introspection, which is the method of inspecting a running VM either from the another VM not under inspection or the hypervisor, malicious events can be identified. Using the open-source VMI library and Xen Suite on the target device, Live Forensic analysis is also completed. Virtual Machine Introspection is proposed as the most realistic approach to detection of the malicious VM. If the intrusion detection system resides on the host, it may be vulnerable to attack, and if the intrusion prevention system resides on the network, it is more prone to diseases. An soul searching-based virtual machine approach to intrusion detection systems is located where the intruder for strong attack sensitivity was outside of the device.

B. Digital Provenance

Digital Provenance is something that describes an investigation of the history of digital objects in the cloud that will be acceptable to the court of law. Digital provenance is an important feature for forensic investigations which describes the history of a digital object. Muniswamy and group proposed the secure provenance scheme which performs digital forensics with trusted evidence in cloud setting. This scheme proves that cloud data evidence is acceptable in court of law. Four properties that are essential for provenance systems were identified by researchers and protocols were introduced to store data provenance using cloud services. Also, provenance is accessible as a layer on top of cloud. Implementing secure provenance in cloud environment increased the importance of data on the cloud.

C. Isolating Cloud Instance

The process of separating the event of the cloud that is part of the crime event in order to prevent data misuse and exposure. Microvasculature and data collected from different clouds must be separated besides digital analysis when a crime incident happens on the cloud. Seclusion precludes potential corruption and degradation of the evidence gathered. The isolation of cloud example helps preserve the validity of the system collected from the domain example. Delport and the group have developed new techniques to disentangle cloud services made reference to in our suggested approach.

D. Model Log

The Database Model seems to be something that takes advantage of all the cloud operations that can be used for research purposes again. Dumping is a challenging issue in cloud computing systems and it is becoming common in all service models. Ting demonstrated which forensic experts can all be made kind of easier on the cloud if logging capacity is improved and suggested a log model appropriate for SaaS and PaaS. To check the actions on the cloud framework without dealing with the cloud server, a log can be used internally and successively in SaaS. To use the planned log model and for PaaS cloud, it is necessary to depend on the cloud infrastructure include a foreign government database module. The proposed try to log-based model would alleviate the analytical problems of cloud behavioural user authentication..

 DOI : 10.35291/2454-9150.2020.0654

E. Regeneration of events

It is possible to regenerate events by taking snapshots of each event in the cloud. The most commonly used method is to take snapshots of the events that have occurred in order to acquire digital evidence. Snapshots may be sequentially retrieved to regenerate the crime event using their time of production. A new technique for regenerating crime events with continuous snapshots was proposed by Belorkar and the group. OpenStack also offers a framework for uploading pictures of cloud occurrences for prominent cloud services including such Eucalyptus. The screenshots taken will be preserved in the honeysuckle walrus section. It has been noted that the size of the photo should be the same as this same original one. Though screenshots can be held in data memory, storing a large store of screenshots for each VM event would also be difficult , time-consuming, costly and performance-degrading. The CSPs could also provide a function to segregate and include mappings as to which VM belongs to the snapshots. Through our approach, we are proposing to address this issue.

F. Forensic Investigation as Evidence using VM Snapshots

Cloud service providers provide users with different types of services, few users from particular organisations often use the same type of service based on pay-per-what-they-use, and some providers provide unlimited bandwidth and storage space for free trial periods that give users the chance to perform malicious activities. Malicious users can steal the sensitive and confidential information from cloud users which in turn affect the trust of the CSP. Cloud needs protection from these malicious activities, and CSP should have a provision to track customer VMs and detect malicious activity using either introspection or intrusion detection method. Users can create VMs from the available physical machines of their choice. OpenStack generates snapshots of a running VM continuously, despite the request of the user, any cloud software such as eucalyptus, and stores it until the VM terminates. You will save the maximum number of snapshots for a given allocated VM if the maximum is reached when the oldest VM is deleted. In a cloud setting snapshots are rich sources of proof for digital investigation and can regenerate the events. Storing and handling huge store of VM snapshots is difficult. Depending on how long the snapshot is stored and how much it has changed since the previous snapshot was taken, snapshots will reduce the output of a virtual machine. Malicious activities are recognised when users of that VM conduct some operation, such as excessive location access, uploading viruses to a variety of network infrastructure systems, extreme amount of short-term downloads and uploads, introducing complex attack points, cracking encryption, flight creting web application based servers or variegated tables, corruption or obliteration of complex data, malevolent activity Our projected model includes a VM intrusion detection framework that enables it to track itself and d Installation, operation and control of the sensor network by cloud vendors.

IV. Conclusion and Future Scope

In this research, we have demonstrated a novel paradigm to enabling performance-related forensic accounting in the cloud environment and take the VM snapshot as evidence. The approach integrates the VM and Virtual machines intrusion prevention system tool to monitor the malicious VM and improved the efficiency of the data center in terms of the size but rather time by encrypting malicious VM snapshots. The suggested approach takes snapshots of suspected VMs and stores them in persistent storage, thus improving system performance. Our future work is to incorporate with several VMs the developed model. We also hope to evaluate the consequences of cloud Virtual server considering the quality and propose a framework for cyber security in cloud IaaS.

References

[1] Deevi Radha Rani, G. Geethakumari, "An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots," *International Conference on Pervasive Computing (ICPC)*, 2015.

[2] BKSP Kumar Raju Alluri, Geethakumari G, "A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing," *IEEE*, 2015.

[3] Hubert Ritzdorf, Nikolaos Karapanos, Srdjan Capkun, "Assisted Deletion of Related Content," *ACM*, 2014.

[4] Mr. Digambar Powar, Dr. G. Geethakumari, "Digital Evidence Detection in Virtual Environment for Cloud Computing," *ACM*, 2012.

[5] Saibharath S, Geethakumari G, "Cloud Forensics: Evidence Collection and Preliminary Analysis," *IEEE*, 2015.

[6] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari, "Providing Security and Integrity for Data Stored In Cloud Storage," *ICICES*, 2014.

[7] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky, "Scenario-based Design for a Cloud Forensics Portal," *IEEE*, 2015.

[8] NIST, "NIST Cloud Computing Forensic Science Challenges," *National Institute of Standards and Technology Interagency or Internal Report 8006*, 2014.

[9] David Maxwell, Cloud Lounge, [Online]. Available: http://www.cloud-lounge.org/why-use-clouds.html.

[10] Amit Kumawat, Cloud Service Models, [Online]. Available: http://www.cmswire.com/cms/information-management/cloud-service-models - --iaas -saas-paas-how-microsoft-office-365-azure-fit-in-021672.php.

[11] Jaonie M. Wexler, Apple bonjour just yet, [Online]. Available: http://www.webtorials.com/content/2012/04/dont-rush-to-bid-adieu-to-apple-bonjour-just-yet.html.

[12] Cloud Tweaks, Cloud deployment Models, [Online]. Available: http://cloudtweaks.com/2012/07/4-primary-cloud-deployment-models/.

[13] Openstack, OpenStack command-line interface cheat sheet, [Online]. Available: http://docs.openstack.org/user-guide/cli_cheat_sheet.html.

[14] Amazon EC2 instances deletion in cloud, [Online]. Available: https://aws.amazon.com/choosing-a-cloud-platform/.

 DOI : 10.35291/2454-9150.2020.0654