International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

An Efficient Approach to Forensic Investigation in Cloud Using VM Snapshots

Soleha Magdum, Nikhil Kandula, Tejal Adep, Harshali Shinde, A. S. Khandagle
AISSMS Polytechnic, Pune, Maharashtra, India

ABSTRACT

Cloud computing has recently emerged as a technology to allow users/clients to access infrastructure, storage, software and deployment environment based on a pay-for-what-they-use model. Traditional digital forensics cannot handle the multi-tenant and dynamic nature of the cloud environment as it has to address various technical, legal, and organizational challenges pertaining to the cloud systems. The dynamic nature of cloud computing gives abundant opportunities to enable digital investigations in the cloud environment. This paper addresses the challenges of digital forensics in the cloud environment and existing solutions to ease some of the challenges. We propose an efficient approach to forensic investigation in cloud using Virtual Machine (VM) snapshots.

Keywords: Digital Forensics, Cloud Computing, Virtual Machine (VM), Cloud Service Provider (CSP), Intrusion Detection System (IDS)

I. INTRODUCTION

Cloud is an emerging technology and cloud based storage is the newly adopted idea that facilitates users not only to upload data to the web but also allows instant accessibility to available resources and share data with anyone at any point of time. But Cloud is a technology that creates a challenge for the person who is investigating and finding out the forensic evidences that may help in the forensic analysis as data stored on cloud can be accessed from anywhere and from any system and very little amount of traces are left behind.

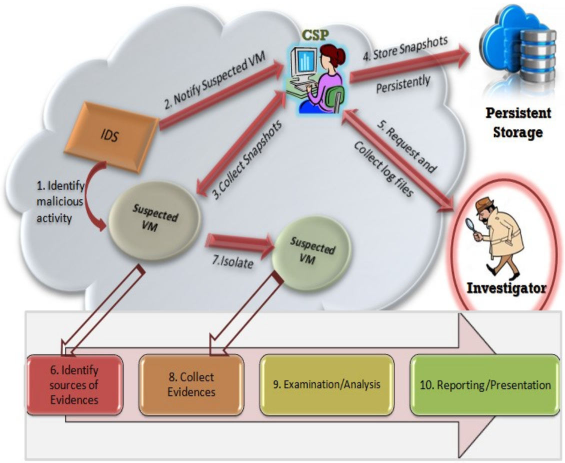

Figure 1. Current Cloud Scenario

The 21st century is known to be the age of digital world. There has been the adoption of computers to a great extent. Today without computers and Internet one cannot survive as we are dependent on these machines for almost all our work. Taking into consideration starting from home to education till banking and even corporate functioning everything has now been automated to computers. Computers contain all our important data in the digital format. With this the need to store the digital data has increased and virtual environment has replaced the physical storage for storing all our credentials as shown in Fig. 1. The most devastating challenge of cloud is to prevent the unauthorized deletion of the stored data on cloud because one can easily delete the stuff without any proper authorization. The data deletion is totally dependent on deletion of nodes that are pointing to some information in Virtual Machine.

II. PROBLEM DEFINATION

Few days ago, there was an incident where one person's VM was deleted by his own friend. Assume both persons as Jack and John respectively. John purchased some amount of cloud space and became CSP himself. Now Jack was in need to get cloud platform to host his mail exchange server. On the

CSEIT1726312 | Received : 01 Dec 2017 | Accepted : 29 Dec 2017 | November-December-2017 [(2)6: 1141-1144]

request of jack, his friend John hosted server on cloud. Jack started growing good with his business and John due to greedy intentions thought to take over his business. So John somehow was successful in hacking Jack's system and sent a mail requesting to delete his VM and deleted the VM too.

Now when investigation was held and investigator asked John to give access to logs saying that he was requested through a mail by Jack to do so. Thus the situation arises where to perform the forensic investigation and without the data evidences it is not at all possible to proceed further. And it we file a case against the criminal it would be a very long process that we cannot even imagine sometime.

Therefore, we are looking forward for a mechanism which would provide a two factor authentication by either CSP or any third party provider before deletion of any VM. This would prevent the unauthorized deletion of VM on cloud.

III. EXISTING SYSTEM

Base system presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. Some combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

IV. PROPOSED SYSTEM

In this research work, propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. Provide a secure way for key distribution with secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. Scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Scheme can achieve secure user revocation with the help of polynomial function.

Scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Provide security analysis to prove the security of scheme.

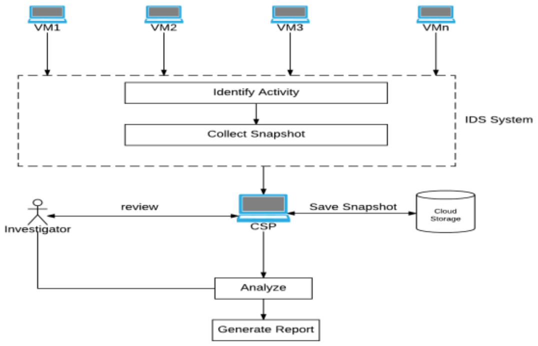

Figure 2. Proposed System Architecture

V. SYSTEM ARCHITECTURE

The idea of the proposed model is that the CSP stores snapshots of a VM whose activities are identified as malicious by an intrusion detection system. Simultaneously the CSP should be requested for log files of the suspected VM and the investigator collects and processes the log files to obtain the evidence. To collect proper and correct evidence, the suspected VM should be monitored for some more time after it is identified to be performing malicious activities. The more time the suspected VM is monitored the more it can be sure of the possibility of malicious behavior. Once the investigator identifies the sources of evidence, the suspicious VM is moved to other nodes to preserve confidentiality, integrity and authenticity of other VMs. By moving or isolating, VM evidence can be protected from contamination and tampering the proposed approach to perform forensic investigation using VM snapshots as evidence.

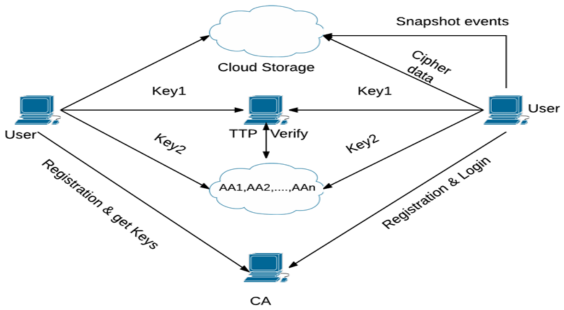

Figure 3. System Architecture

VI. PROJECT SCOPE

Many businesses whether large or small have started using cloud computing these days directly in the form of Google, Amazon or in an indirect way as in the form of Twitter apart from the already accepted alternatives. There exists a number of reasons for this technology being used so popularly amongst the businesses now a days. Cloud is an environment that provides software, platform and infrastructure as a service to satisfy one's needs as shown in Figure 2. But once data is placed on cloud what happens with that data is a point of concern as it is not in our control. This has been the major drawback of cloud till date. Research is being done so that some measures can be taken to prevent this lack of transparency which in return might even increase the user's trust towards cloud to be taken up. Cloud can benefit users in number of ways and some of them are listed as below.

1. Reduction of costs: As compared to the on-site hosting, the cost of establishing the applications in the cloud scenario can become less in comparison to hosting application on-site as it requires lower hardware expenses with much effective physical resource usage.

2. Universal access: Remotely located employees could be allowed to access the applications and work via the internet by Cloud Computing.

3. Up to date software: Software can be updated by cloud service provider taking into consideration the previous releases of the software.

4. Choice for applications: Flexibility is provided to the users of the Cloud for experimenting along with choosing the appropriate option out of all the available for their needs. Also Cloud computing facilitate businesses to make its use, access and to pay for their requirement and give a quick implementation time.

5. Greener and Economical: The mean quantity of the energy that is required for a computational activity performed in the cloud is less in comparison to the mean quantity required for an on-site deployment. The reason is different organizations are able to share the same physical resources in a secure way and gives a fine and efficient shared resources usage.

6. Flexibility: Users are allowed for switching applications easily, quickly by using the application appropriate to their needs.

7. Security: This system can also provide end level highest security

VII. FUTURE WORK

In the domain of Cloud there always remains a room for enhancement in the existing system. At present the work was successful in integrating the proposed system with the command line interface. Thus, in future, efforts for integration of an authentication mechanism with the graphical user interface of cloud would be undertaken.

VIII. CONCLUSION

In this work, we have proposed a novel approach to enable digital forensics in the cloud environment with respect to performance by taking VM snapshot as evidence. The approach incorporates intrusion detection system in VM and VMM to identify the malicious VM and improves the cloud performance in terms of size and time by storing snapshots of malicious VM. The proposed approach takes snapshots of suspected VMs and stored in persistent storage, hence improves the performance of cloud.

IX. 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 Agarwal, 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.

WEBSITE:

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

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