Proposing an authentication mechanism for Prevention of Cloud machine Deletion

Pooja Dubey[1], Vineeta Tiwari[2,] Shweta Chawla[3]

[1] *PG Student, Network Security, Gtu Pg School, Ahmedabad, Gujarat, India*
[2] *Senior Technical Officer, CDAC-acts, Pune, Maharashtra, India*
[3] *Head and Chief Investigator, SC Cyber Solutions, Pune, Maharashtra, India*

ABSTRACT

Cloud platform today is the most widely being used technology all around the world. Due to its favorable features such as pay only for what you use lure most of the audience to use it and even adopt this technology. Still the unsure understanding of cloud control, trust and transparency are the major points of concern which deflects the minds of people from using the cloud services. Cloud totally being a virtualized environment imposes a dozen of issues for the user. Most concerned issue on cloud at present is the deletion of virtual instances on cloud without any proper authentication and authorization. Thus, a single damaged virtual machine can be a great challenge for investigators to track out the activities of the person on virtual machine at particular interval of time making the forensic investigation a tough task to be performed in return.

This paper will wrap up all the theoretical key points of cloud along with the challenges which are being faced in the domain of Cloud Forensic as well as Cloud Security. Through this paper we explore the existing techniques, their drawbacks and come up with feasible solutions which will act as a guidelines for forensic investigation process in future.

Keyword: - *Cloud; Forensic Investigation; virtualization; Forensic; virtual instances;*

1. INTRODUCTION.

The 21st century was known to be the digital world. But it has changed the assumptions and the world is being diverted towards an emerging technology and this is nothing but cloud age. Now a days the virtualized environment is given much more preference due to the increased amount of data with the shortage of resources to store and main data. Besides this there are several reasons for cloud now being adapted more. This includes: infrastructure needs, platforms for applications as it is not at all affordable to set up experimental bed in every situations. Cloud serves us with variety of facility like pay for what you use, mass storage, and geographic location independent access and so on. Instead facilitating such benefits there are still some snag for the less acceptance of cloud.

The rest of this paper is organized as follows: In section II existing frameworks has been presented, in Section III we have given a glimpse on challenges presented by NIST which require lot of efforts to be worked on further, in Section IV we has studied and discussed the drawbacks of cloud forensic and in Section V proposed model followed by results and analysis with conclusion along with the possible solution that can be proposed as our future work is mentioned.

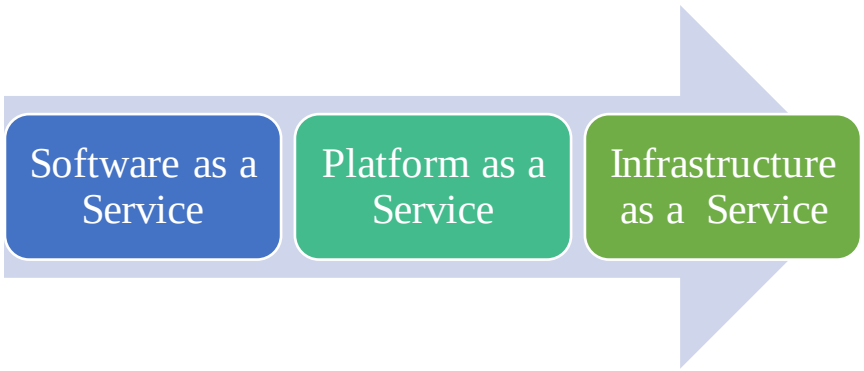

Fig. 1. Cloud Service Model

2. RELATED WORKS.

A critical analysis of the existing work has been performed by the author to present and study the working areas of the domain along with the main issues that exist in cloud. At present much work is needed to get through the loopholes by taking proper measures in the direction that can be proved as a benchmark in future to overcome such devastating issues and can also be taken as guideline for further investigations.

Table. 1. Review of Existing Frameworks

No.	Paper Title	Author Name	Key points	Remarks
1.	An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots	Deevi Radha Rani, G. Geethakumari, 2015	Incorporates Intrusion Detection System on VMs which allows it to monitor itself and on VMM to detect malicious activity through snapshots between VMs [1]	Improves the performance of cloud and can be implemented for multiple VMs.
2.	A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing	BKSP Kumar Raju Alluri, Geethakumari G, 2015	1) A proper triggering condition will only make the investigator to get the needed data 2) During the collection of data the corresponding virtual machine (VM) has to be paused for a while, leading to performance degradation [2].	Address the issues concerned with evidence collection by using the techniques of virtual machine introspection.
3.	Assisted deletion of Related Content	Hubert Ritzdorf Nikolaos Karapanos Srdjan Capkun, 2014	A system IRCUS assists the user in securely removing project-related content [3]	Used to protect data confidentiality by assisting deletion of related content, where the user is presented with files that should be securely deleted together.
4.	Digital Evidence Detection in Virtual Environment for Cloud Computing	Mr. Digambar Powar and Dr. G. Geethakumari, 2012	Focus mainly on finding and analyzing digital evidence in virtualized environment for cloud computing using traditional digital forensic analysis techniques [4].	Virtual machines that are present on a physical system or running on a portable storage device can be detected or analyzed.
5.	Providing Security and Integrity for Data Stored In Cloud Storage"	Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari, 2014	A method was proposed to save our data in the cloud storage secure and provide an integrity check to verify if integrity is preserved or not while we retrieve our data [5].	Use less computational power and processing time.

In summary, the work presented in this paper is based on prior research to explore the concepts of the existing mechanisms and works. But through review it was realized that even if earlier work focused on data storage, not on security of cloud. This has led to less acceptance of cloud. Thus, author has decided to contribute to prevent the cloud machine deletion by imposing two factor authentication mechanism.

3. CHALLENGES.

This section covers up the former research carried out by the members of the NIST (National Institute of Science and Technology) cloud computing Forensic Science Working Group [8]. They list out the existing challenges in cloud forensic needed to be worked on. Some of the challenges that still exist and needs to be overcome are shown in Fig. 2:

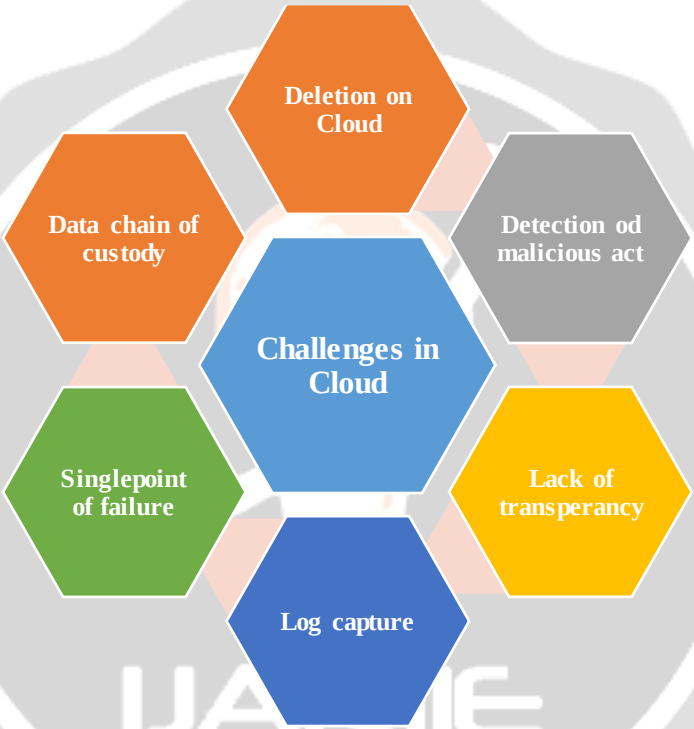

Fig. 2. Challenges in Cloud Forensics.

Besides cloud having too many challenges that yet had not came to a solution and even some limitation out of them seems impossible to get through in near future, there are many opportune sides of cloud which drags attention of minds of many people to migrate themselves on cloud.

4. DRAWBACKS IN EXISTING MECHANISMS.

The existing methodologies as described earlier has certain disadvantages such as unsure understanding about the control, trust and transparency of the stored data.

The major drawbacks seen so far can be listed as follows:

- If the proper conditions are not triggered the results of the analysis will be admissible.[2]
- VM needs to be paused for specific amount of time to collect data causing performance degradation [2].
- Cloud machine deletion without proper authorization is the burning topic among the researchers these days.

In the working cloud scenario when one try to delete any of cloud machine, deletion is proceeded without anyone concern even without the knowledge of the machine owner itself.

This section we have wrapped up the main limitations of different mechanism to be focused on and proposed a solution in return which will aid one of these mentioned drawback.

5. PROPOSED METHOD.

In this work, the center of focus is on to propose a two factor authentication mechanism for cloud machine deletion. The main target behind cloud forensic is to acquire and preserve the critical evidences which can later be beneficial for the investigators. But the current scenario depicts that if VMDK (virtual machine disk file) is harmed in any sense it can prove to a blunder as virtual machine is the container of all the evidences. Once defaced can never get back again. Even if it is managed to recover the virtual machine disk file it will be of no use for further purpose. Presently, no mechanism exists which can regain the VMDK in the same form as it was before the deletion.

Each activity performed on the VM is logged into the VM, while the actions performed by the CSP (Cloud Service Provider) are logged onto the server. The deletion of single VM can destroy the evidences entirely.

This can be hazardous for the user and can act as an obstacle for a forensic investigator to extract the crucial private data stored in virtual machine.

Thus, through this work, taking into consideration the pros and cons of the of the existing frameworks and the challenge currently being faced by investigators in the current Cloud Scenario, a model as shown in Fig. 3. is being proposed that will not only ensure the prevent the unauthorized deletion on cloud but also provide a level a security to cloud. The proposed work is assumed to provide the two factors authentication for machine deletion on cloud. The basis of the mechanism is verification via email and message. But technically the proposed model will facilitate three factor authentication. One additional is the credentials verification which is already with the user. So three factors of the authentication mechanism are as following:

a) Credentials verification

b) Email Verification

c) Message Verification

This will make sure proper authorization of user before fulfilling a deletion request of VM on cloud. Only when the authentication is bypassed successfully then only the deletion would be progressed else it would be discarded.

Thus, hopefully the proposed model will not only aid security but forensic procedure also.

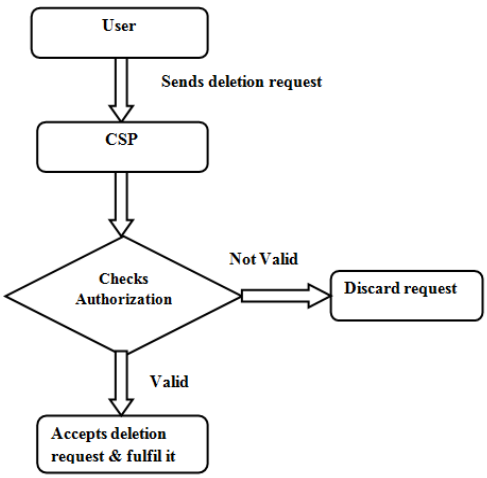

Fig. 3. Proposed Model

Firstly, a mail server needs to be established for exchanging email immediately when something wrong with user cloud machine is encountered to prevent them from being ruined. In such uncertain situations the work proposed will ensure two mediums as mentioned above for the correct and proper authorization of the person who requested for VM deletion.

Message verification Pseudo code:

Input: username and password of SMS gateway
Output: SMS sent to registered user

```
Step-1: begin
Step-2:     import library
Step-3:     Read username and password
Step-4:     prompts for the number to send SMS
Step-5:     Message = "Hi"
Step-6:     generate OTP
Step-7:     Logs into the SMS gateway using provided credentials
Step-8:           try:
Step-9:                 Open Url
Step-10:                print ("Url connected -SMS sent ")
Step-11:          except:
Step-12:                Handle all error
Step-13:                print ("Url not connected – SMS not sent ")
Step-14:          end try
Step-15: end
```

The pseudo code represented above is used by proposed work for the message verification of the user. A secret code is appended in the message and is forwarded to the user for integrity constraints of the users.

6. ANALYSIS AND RESULTS.

As per the expectations, analysis of the experiments performed with sending message to the user and authenticating via a verification message has accomplished successfully and were up to the expectations. The second module of email verification is yet to be worked on and needs to be integrated with the cloud to result the entire working framework.

7. CONCLUSIONS AND FUTURE WORK.

Cloud Forensic being one of the most popular emerging technology becomes an area of interest for the researchers as not much work is being carried out in this domain. Thus, there are handful of points associated with cloud which needs to be worked on. The proposed work is also one of them which is an effort towards making it result in as a feasible solution. Present scenario of cloud does not properly authenticate user before cloud machine deletion and this leads to a point of concern in cloud environment. So the work is being looking forward to overcome this issue.

8. ACKNOWLEDGEMENTS.

I wish to thank all the members with gratitude for constantly encouraging me during this work. Also I wish to mention that the trademarks, product names, company names, screenshots referred in this paper are acknowledged to their respective owners.

9. 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.