Enhancing Forensic Service in Distributed Cloud Computing

Dhara Prajapati[1], Gayatri S. Pandi[2]
[1]M.E Student,[2] Professor
Dept. of Computer Engineering,
L.J College of Eng. & Tech., Ahmedabad, India

Abstract :- **The Internet is growing explosively, as is the number of crime The Internet is growing explosively, as is the number of crimes committed against or using computers. As a response to the growth of computer crime, the field of computer forensics has emerged. Computer forensics involves carefully collecting examining electronic evidence that not only assesses the damage to a computer as a result of an electronic attack, but also to recover lost Information from such a system to prosecute a criminal. With the growing importance of computer security today and the seriousness of cyber crime, it is important for computer professionals to understand the technology that is used in computer forensics. It promotes the idea that the competent practice of computer forensic and awareness of applicable laws is essential for today's organization.**

Keywords :- Cloud Computing, Digital Forensic, Fraud detection, Monotoring

I. INTRODUCTION

Cloud computing is internet based computing where virtually shared servers provide software, infrastructure, platform, devices and other resources to customers on a pay-as-you-use basis. Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a datacenter from a capital-intensive set up to a variable priced environment. **Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Cloud computing is internet based computing where virtually shared servers provide software, infrastructure, platform, devices and other resources to customers on a pay-as-you-use basis. Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.It helps users to concentrate on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes. Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. They consume resources as a service and pay only for resources that they use. Most cloud computing infrastructures consist of services delivered through common centers and built on servers. Emerging discipline in computer security : No standards, few research ,Investigation that takes place after an incident has happened. One of the most important time frames in Computer forensics is the initial response to a computer related crime and how to identify important evidence necessary to make a legal case against perpetrator. Investigation that takes place after an incident has happened. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

II. FRAUD DETECTION TECHNIQUES

Fraud detection involves identifying fraud as quickly as possible once it has been perpebated. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies.

A. Credit Card Fraud. Credit card fraud is divided into two types: offline fraud and online fraud. Offline fraud is committed by using a stolen physical card at storefront or call centres. In most cases, the institution issuing the card can lock it before it is used in a fraudulent manner. Online fraud is committed via web, phone shoppin . Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase.

B. Computer Intrusion. Intrusion is defined as the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. Intruders may be from an outsider (or hacker) and an insider who knows the layout of the system, where the valuable data is and what security precautions are in place. Computer intrusion can be classified into two categories: misuse intrusions and anomaly intrusions. Misuse intrusions are well-defined attacks on known weak points of a system. Anomaly intrusions are based on observations of deviations from normal system usage patterns. These include attempted break-ins, masquerade attacks, leakage, denial of service, and malicious use.

C. Telecommunication Fraud. Fraud is costly to a network carrier both in terms of lost income and wasted capacity. The various types of telecommunication fraud can he classified into two categories: subscription fraud and superimposed fraud. Subscription fraud occurs from obtain- ing a subscription to a service, often with false identity details, with no intention of paying. Cases of bad debt are also included in this category.

III. RELATED WORK

In [1] author has proposed Examining local machine and web browser database for the trace of client-cloud interaction can be easily revoked by deleting navigation data after browsing. Anyone with little knowledge in browser history and its database can erase all the trace of their interaction with cloud The collection from the management plane method is a very attractive option since it is user driven, but it requires trust in the management plane. Forensic support as a service is a natural choice and there is already a provider who offers this service.

In [2] author has proposed Cloud computing as a technology has immense potential and offers plenty of benefits for the HPC users. Users on the other hand still do not trust cloud for running their confidential applications. Lack of transparency and security mechanisms are the major concerns. Cloud Service Providers need to enhance trust on their services. One of the ways to achieve this is to perform digital forensics in cloud. In this paper, we propose a digital forensic based model for VM introspection in cloud. We devised a framework that contains three components.

In [3] author has proposed The virtual nature of cloud computing is pushing digital forensics into a new horizon. Many challenges are existing in the cloud including jurisdictional and technical issues. This paper proposes forensic process that consists of four phases: Identification, Collection and acquisition, Examination and analysis and result dissemination.

In [4] author discussed the value of facilitating post incident cloud forensic investigations of service oriented architectures. The challenges are technical, organizational, legal and social – all of which hold back the integration of cloud data collection mechanisms to facilitate such investigations. Based on a preliminary analysis of the cloud reference architecture, the considerations presented are important for better integration of the missing considerations of forensic capabilities within a cloud forensic service oriented audit framework standardization process.

In [5] author has 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.

Fraud auditing is a very different term, encouraging the detection and prevention of frauds in commercial transactions. Fraud auditing is the process of detecting, preventing, and correcting fraudulent activities. In the broadest sense, it is an awareness of many components of fraud, such as the human element, organizational behavior, knowledge of fraud, evidence and standards of proof, an awareness of the potentiality for fraud, and an appreciation of the red flags.

IV. PROPOSED SYSTEM

A. Our approach :

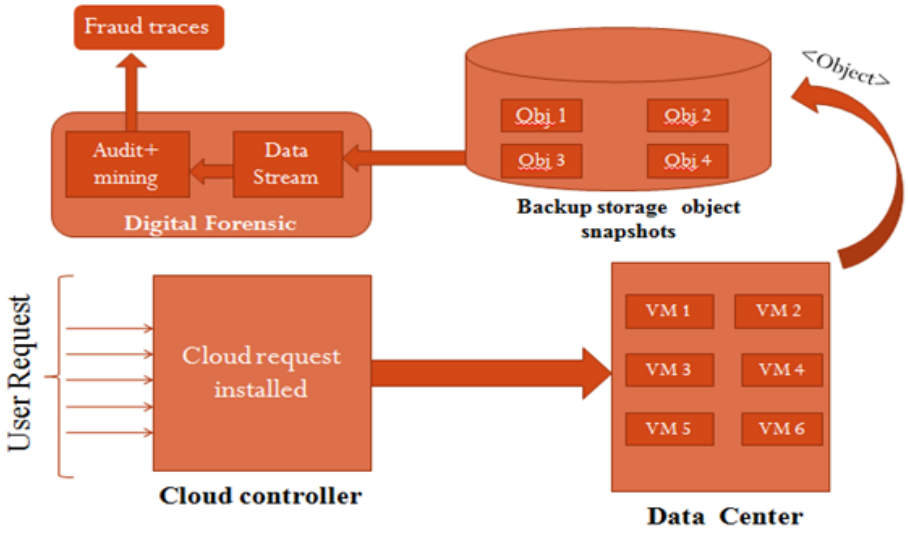

Fig.1 Propose Cloud Forensic Architecture

B. Proposed Algorithm:

Pseudo Code

Step-1: Initialize Attribute declaration// amt, credit card no, transaction date etc

Step-2: Perform Validation of all attributes

Step-3: input Transaction Entries in to Dbase

Step-4: Collect Training Data set

Step-5: Convert List of transaction data object to multidimensional

Step-6: Apply Clustering

Step-7: Assigning cluster Label

Step-8: Commit transaction to database either as "Fraud" or "LEGITIMATE"

v. RESULTS

In the frraud detection technique in prpposed model work only some types of fraud will be detect like Date,IP address,Operation,Files etc..
User enter in the system then all the transactions watch by whatcher and all data uploade in storage S3.Apply proposed algorithm and define a cluster. One of the most important time frames in Computer forensics is the initial response to a computer related crime and how to identify important evidence necessary to make a legal case against perpetrator. Investigation that takes place after an incident has happened.

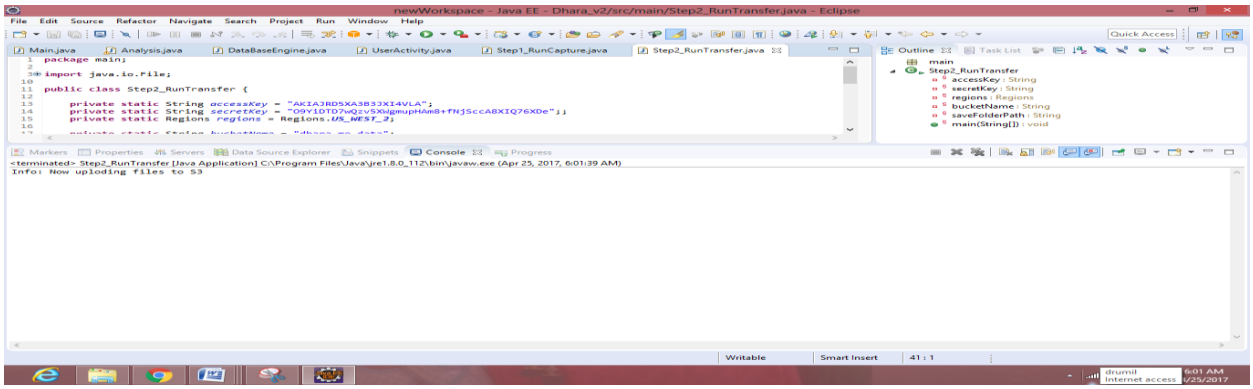

Fig.2 Upload file on S3

Then after apply on the all the data Auditing and Mining (algorithm) then result will be Show in the figure 3.

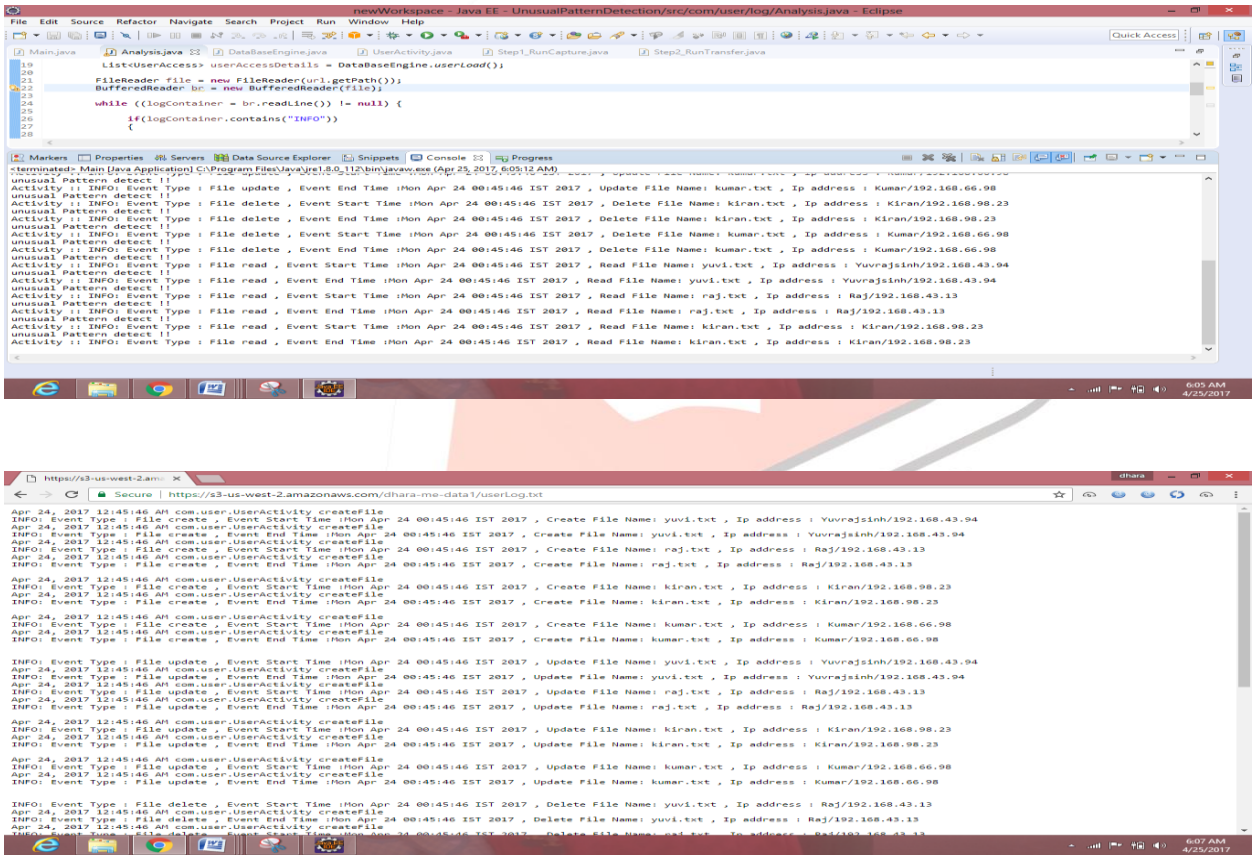

Fig.3 Upload file on S3

In our research work fetch all fraudulent activity are define in the cloud and the cloud .describe all activity In the object Storage then after we will trace the fraud. Major issue in digital forensic is tracing a Fraud. so, in our Work we purpose Digital Forensic as a software as a services in Cloud Computing enviournment to detect fraud trace in ordered to avoid such fraudulent attacks in various place in cloud computing. Like bank/credit card transaction.

V. CONCLUSIONS

Computer forensics is a vital part of the computer security process. As more knowledge is obtained about how crimes are committed with the use of computers, more forensic tools can be fine tuned to gather evidence more efficiently and combat the crime wave on technology. Our future work is to implement the proposed approach with multiple VMs. Also, we plan to explore the implications of acquisition of evidence from cloud VMs and develop framework for digital forensics in cloud IaaS. In forensic investigation Information are not completely secure and difficult to find crime in the system Lack of transparency and security, accuracy low and malicious activity and attacks on cloud difficult to prevent and investigate. Major issue in digital forensic is tracing a Fraud. so, in our Work we purpose Digital Forensic as a software as a services in Cloud Computing enviournment to detect fraud trace in ordered to avoid such fraudulent attacks in various place in cloud computing. Like bank/credit card transaction.

REFERENCES

[1] Emi Morioka and Mehrdad S. Sharbaf "Cloud Computing: Digital Forensic Solutions" IEEE, 2015, pp.589-594, DOI: 10.1109/ITNG.2015.99.

[2] Meera G, Geethakumari G"A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing. "2015 IEEE, 2015 Pages: 1 - 5, DOI: 10.1109/SPICES.2015.7091553

[3] Amna Eleyan, Derar Eleyan"Forensic Process as a Service (FPaaS) for Cloud Computing" IEEE ,2015, pp.157 - 160, DOI: 10.1109/EISIC.2015.14

[4] Sean Thorpe, Tyrone Grandison , Indrajit Ray "Towards a Forensic- based Service Oriented Architecture Framework for Auditing of Cloud Logs" IEEE 2013 Pages: 75 - 83, DOI: 10.1109/SERVICES.2013.76

[5] Deevi Radha Rani, G. Geetha kumari "An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots" IEEE 2015 pp. 1 - 5, DOI: 10.1109/PERVASIVE.2015.7087206

[6] Nasir Raza "Challenges to Network Forensics in Cloud Computing" IEEE 2015 pp 22 - 29, DOI: 10.1109/CIACS.2015.7395562

[7] Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana" Survey of Fraud Detection Techniques" IEEE2014,pp.749-751,

[8] https://en.wikipedia.org/wiki/Digital_forensics

[9] http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/