An Survey On Network Forensics based on Cloud Computing Security Management System

Khateeja Ambareen[1], Parvathi S J[2]
[1, 2] Dept. of CSE
[1, 2] GSSSIETW, Mysuru, India

Abstract- *The Network Forensics deals with the monitoring of network traffic with an aim to trace some suspected activity from normal traffic or to identify some abnormal pattern in the traffic that may give clue towards some attack. The cloud computing architecture presents aggravated and specific challenges in the network forensics. There are three challenges for network forensics first, network forensics need a mechanism for analyzing network traffic remotely in the cloud. Second, the forensics needs to be virtual resources of a specific cloud user and third, Forensics data should be processed directly in the cloud to avoid a costly transfer of huge amount of data to external investigator.*

Keywords- Network forensics, cloud computing, network forensics

I. INTRODUCTION

Network Forensics is a sub branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purpose of information gathering. The network traffic is a pro-active investigation [1]. Digital Forensics is a process of uncovering and interpreting the electronic data. Electronic data means it is the computer to computer interchange of business documents in a standard electronic format. Cloud Forensics is the application of digital forensics in cloud computing and it is a subset of network forensics. The scalability of the cloud means at one point, to access information from different sources. The Cloud computing is a delivery of hosted services over the internet. The cloud computing provides convenience, availability, elasticity, large storage capacity, speed, scalability and on-demand network access to a shared pool of computing resources. The cloud computing has three service provider those are Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS). These models have different limitations and provide different capabilities to the consumers. The cloud computing has five characteristics: on demand self-services, broad network access, Resource pooling, Rapid Elasticity and Measured Services. The forensic expert is looking for the evidence data which can be in one of the three forms, static, moving or in execution. Digital forensics is aimed to acquire legally authentic evidence through a systematic procedure. The network traffic itself and network logs are analysed to look into the event happened in the past. The purpose is to identify traces of a specific activity by a certain user and reconstruct to gain some lead to an investigation, or may be an attempt to validate some suspected activity. The network forensics domain has attracted unfortunately undue attention towards resolution of its problems from both the industry and the researchers so far. The investigation of attack is important irrespective of success factor of the attack. The phenomenon of network forensics can be termed as use of scientifically proven technical steps involving collecting, aggregating, recognizing, examining, correlating and analysing the data retrieved by capturing network traffic and reporting. The concept of the Distributed network forensics is based on the distributed techniques, which are useful for providing an integrated platform for the automatic forensic evidence gathering and important data storage, valuable support and an attack attribution graph generation mechanism to depict hacking events [6].

II. Types of Network Forensics Framework

A distributed system based framework: Internet and LANs are distributed in nature. The events related to the network attack are logged in as client at various locations. For carrying the digital proof which obtained from the crime site there are some network systems and the current systems also lack efficient attack attribution.

Soft Computing based framework: The soft computing approach comes into picture after the collection of data. It is used to examine the collected data. A step ahead, it classified the attacked data. In this approach fuzzy and neural network tools are used for the validation of attack occurrence.
Honeypot based framework: Honeypot framework is a type of trap, which attract the attackers. It helps us in understanding the process and methodology of the attacker. This system helps to improve the defensive mechanism.

Attack Graph based framework: There is a facility of evidence graph model for automated reasoning and effective evidence presentation. This framework contains six phases: collection of evidence, evidence, pre-processing of evidence, based on attack knowledge, asset knowledge based, evidence graph manipulation, and attack reasoning.

Formal Method based module: This system helps us to examine security events and make clear the attacker steps, followed by the attackers. This system integrate examined results performed by the IRT on a compromised system with the help of Incident Response Probabilistic Cognitive Maps (IRPCMs).Which offers a proper method framework, that helps to recognize potential attack patterns with the help of Investigation-based Temporal Logic of Actions (I-TLA).

Aggregation framework: Network forensic analysis consists of several phases. There are many security tools. These tools can be used for particular phase. The main aim of this framework is to handle the strength of these tools rather than constructing a new tool from scratch. The system contains three main modules – marking, capture and logging [2].

A. Network Forensics Architecture

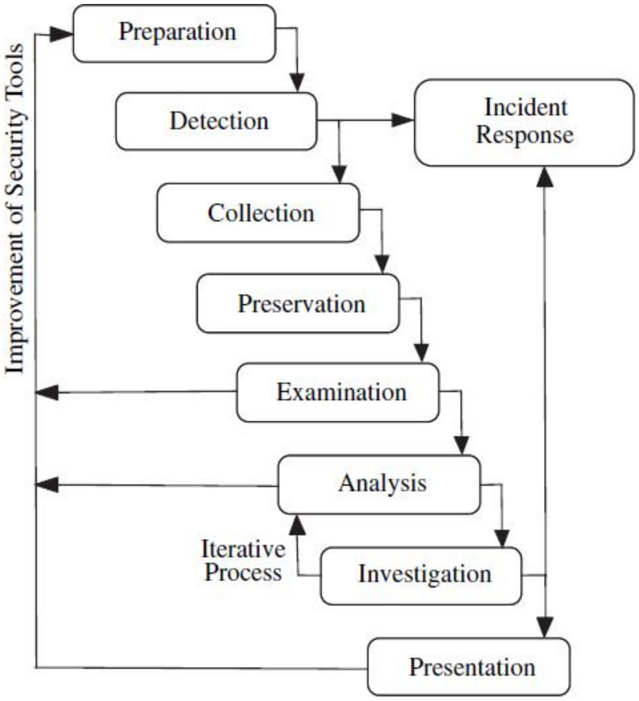

Figure 1. Process of network forensics [17]

Detection: The term detection refers to detecting unauthorized events and anomalies.

Incident Response: It is another important phase of the process model. This phase is to inform about any unauthorized and illegal action that has happened through intrusion detection system.

Collection: It is the main important phase of the generic price model, because all the things depends upon the effective data collection. We collect data in such a way that it gives us to maximum information regarding illegal activities, and it does not affect the privacy of the victim.

Preservation: After the collection of data stored on a backup device. The collected data resides in the form of the traces and logs. Preservation also refers to a hash of all the data. Copy of data has been analyzed instead of original data.

Examination: After the preservation of data move a step ahead, that is examining data. Data consists in the form of traces and logs. The data obtained from the various places integrated and fused into a single data unit on which analysis could be performed.

Analysis: It is also an important phase of the process model. In this phase attack pattern is analyzed from obtained data and matched this pattern to the attacker pattern with the help of existing statistical, soft computing and data mining approaches.

Investigation: The main motive of this phase is to find out the path between a victim network and the point of origination through intermediate system and communication pathways.

Presentation: It is the last and important phase of this process model. The presentation of the information and digital evidence must be unambiguous and in an understandable language for legal personnel [9].

B. Tools Component of Network Forensics

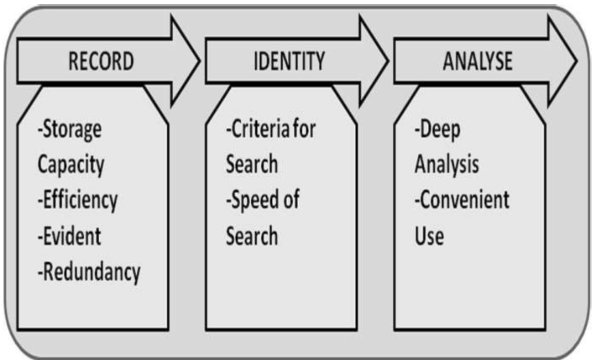

Figure 2. Typical Network Forensics Analysis Tool Components [16]

The tool used for network forensics is expected to provide some essential features, few of them are as under:

1. High Storage Capacity
2. Capturing and Analysis of network packets.

3. Analysis of Logs in multiple formats.
4. File and Disk Forensics.
5. Memory Forensics.
6. Easy in use.
7. Efficiency.

The Collection of network traces is performed by Recording component of a forensic tool whereas Examination and Analysis along with Investigation and Attribution is performed by Analyse component of the tool [11].

III. RELATED WORK OF CLOUD FORENSICS AND DIGITAL FORENSICS

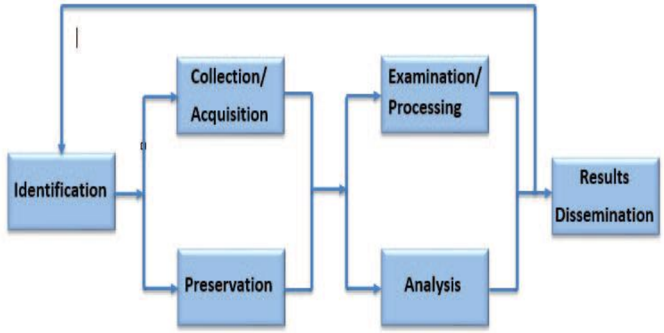

Figure 3. Cloud Forensics Process [18]

Identification:

Identification is reporting misuse of cloud or malicious activity such as deleting files, illegal use of storing files and so on [12].

Collection/Acquisition and Preservation:

The data collection and acquisition is a crucial phase of forensic procedure. Any errors that may occur will affect the whole investigation process. The data collection phase should also consider the preservation phase for collecting evidence. Preservation is the protection the protection of the integrity of the evidence throughout the investigation process [13].

Examination/Processing and Analysis:

Examination and analysis phase comes after collecting the digital evidence and preserving it. Examination is defined as “Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity”.

Results Dissemination:

This phase consists of report findings step and presentation findings step. Digital evidence and analytical reports are presented to the court in this phase. The report should include information on all processes, the tools and applications [15].

Digital Forensics:

digital forensics are the application of scientifically derived and proven methods which aims to preserve, collect, validate, identify, analyse, interpret, document, and present digital evidence maintaining a documented chain of evidence for presentation in courts.

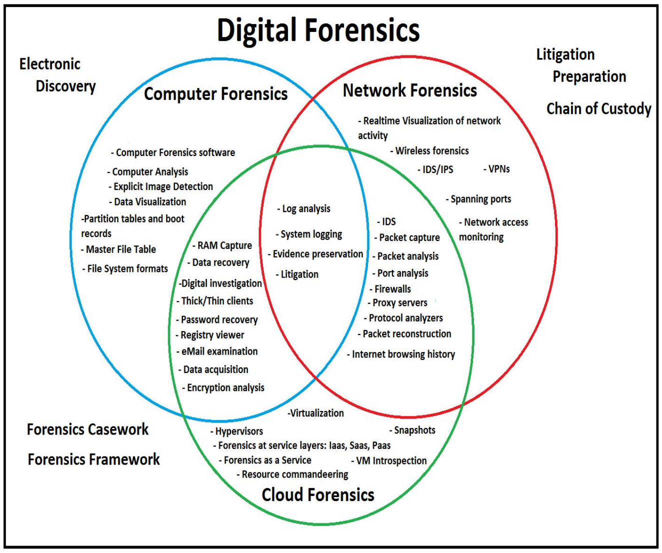

Figure 4. Diagram depicting the breakdown of Digital Forensics [19]

The diagram depicts a relationship showing differences and intersecting similarities and roles between the different forensic methods. Cloud forensics has common methods of investigation with computer forensics and network forensics. As stated earlier, digital forensics includes computer forensics, network forensics and cloud forensics. Each of the three sub-categories shares roles. These three forensics methods share the compilation and logging of the data collected. Cloud forensics is partially a combination of network forensics and computer forensics [6]. Moreover, cloud forensics’ additional challenges require interaction with the Virtual Machine Monitor or administrative tools of virtualization and storage resources. There are important differences between network forensics and cloud forensics. Network forensics is strictly concerned with analyzing communication traffic, recording the traffic, discovery of anomalies and responding appropriately. Cloud forensics which uses network forensics methods has a broader scope and several layers for introspection that make it more complex and challenging. Cloud forensics' uniqueness demands a separate framework for digital investigation requiring specially developed tools [7].

IV. THE ROLE AND LIMITATION OF NETWORK FORENSIC IN CLOUD COMPUTING

Having an effective management's suite for managing virtual machines' infrastructure is critical for any cloud computing infrastructure as a service (IaaS) vendor. Now imagine some billions of users accessing their data from those rented interfaces with each users, probably equipped with two to three devices like PC, Laptops, Smartphones, PDA and many more gadgets that allow accessing those data over the network using Apps, which allow them to perform almost all transactions, banking operations, and many more. And the job

Of Network monitoring, the data which flow like a stream with threats and fault becomes everything equivalent to impossible, and not only has this, the architecture, so called "Cloud Computing" had its own limitation to provide the basis for Network forensic and investigation process. As said before, with numerous entry and exit point for transactions, online processing, request and responses traveling across the network, making the ever complex networks even more complex, making traversing, monitoring and detecting threats over such an environment a big challenge for Network forensic and investigation for cybercrimes. It has demanded in Depth analysis using network tools and techniques to determine how best information can be extracted pertinent to an investigation [3].

Network forensic helps tries to analyse traffic data logged through firewalls or intrusion detection system or at network devices like routers and switches. A forensics investigation requires the use of disciplined investigative techniques to discover and analyses traces of evidence left behind after a committed crime [4].

Cloud computing can also frustrate network forensics because of the lack of direct access to the physical machines that are suspect. This can also frustrate network-based forensics because the way that the cloud environment is set up at the hosting facility. Accessible evidence may only be limited to data on the virtual machine or system and not across the entire network path from end-to-end. Networks are only a logical hierarchy in the investigation rather than being able to directly monitor the data from a span port off the network device. Complicating the process is that the current set of skills and tools are still being developed. This means that for now, the tools and skills are still relatively immature in relationship to the current tool sets that are available when the systems and networks are fully owned by a company [3].

V. CONCLUSION

The network forensics, an extension of digital forensics, is a science where data from network traffic and network devices is captured, preserved and analysed for purpose of investigation of a certain activity by a suspect. In this paper we tried to bring out the logical and conceptual part of investigation, challenges, tools and techniques used in Network forensic in a Cloud Environment. The effectiveness of the threat monitor is pivotal in the success of providing a secure and trustworthy service in the cloud and data centers. Attacks are increasingly becoming more sophisticated with each event. It is very important that an effective, undetectable and uninterruptible method be used to monitor or respond to digital attacks. 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. Cloud service provider or the designer of the network forensic tool on certain challenges can be helpful to bring partial improvement in the issues.

REFERENCES

[1] T. Hong; Z. Tao; J. Qi; Z. Jianbo, 2011. A Distributed Framework for Forensics Based on the Content of Network Transmission, Instrumentation, Measurement, Computer, Communication and Control, 2011 First International Conference on , vol., no., pp.852,855, 21-23

[2] Technical Issues of Forensic Investigations in Cloud Computing Environments. Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, p. 1-10, 2011.

[3] Understanding Network Forensic Analysis in an Operational Environment Proceedings of the 2013 IEEE Security and Privacy workshops, p. 111- 118 , 2013.

[4] E. S.Pilli, R.C.Joshi, R. Niyogi, 2010. Network forensics framework: Survey and research challenges, Digital Investigation.

[5] F. Marturana, M. Gianluigi, S. Tacconi, "A Case Study on

Digital Forensics in the Cloud," Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on , vol., no., pp.111,1 16, 10-12 Oct. 2012.

[6] Digital Forensic Research Workshop, "A roadmap for Digital forensic research,"

[7] "Digital Forensics for Network, Internet and Cloud Computing: A forensic evidence guide for moving targets and data."

[8] D. Wang, T. Li, S. Liu, J. Zhang, C. Liu, 2007. Dynamical Network Forensics Based on Immune Agent Third International Conference on Natural Computation (ICNC) IEEE.

[9] F. Marturana, M. Gianluigi, S. Tacconi, "A Case Study on Digital Forensics in the Cloud," Cyber- Enabled Distributed Computing and Knowledge

[10] Discovery (CyberC), 2012 International Conference on , vol., no., pp.111,1 16, 10-12 Oct. 2012.

[11] Hong-Ming Wang, Chung-Design and Implementation of a Network Forensics system for Linu Computer Symposium (ICS), 2010 IEEE international, p. 390-395, 2010.

[12] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," arXiv, vol. 1, 2013.

[13] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, vol. 9, pp. 71-80, 2012.

[14] Pichan, M. Lazarescu and S. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital Investigation, vol. 13, pp. 38-57, 2015.

[15] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response,"

[16] Challenges to Network Forensics in Cloud Computing, Nasir Raza, 2015 Conference on Information Assurance and Cyber Security (CIACS)

[17] Distributed Network Forensics Framework: A Systematic Review, Prashant Singh Thapar University, Patiala, International Journal of Computer Applications (0975 – 8887) Volume 119 – No.19, June 2015

[18] Forensic Process as a Service (FPaaS) for Cloud Computing, Amna Eleyan, 2015 European Intelligence and Security Informatics Conference

[19] Scenario-based Design for a Cloud Forensics Portal, Curtis Jackson1, Rajeev Agrawal2, Jessie Walker3, William Grosky, 978-1-4799-1737-2/15/$31.00 ©2015 IEEE