Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Forensic Investigation and Exploration on Cloud Computing Environment

By Dr. S Santhosh Baboo & S. Mani Megalai
SCSVMV University, India

Abstract- Cloud service providers are providing more services on demand. Usage of Cloud in IT Industry, Educational Institution, Social network, Medical Field and other business Industry are tremendously increased. This increases the more criminal activity on cloud. There is a need for forensic capabilities which support investigations of crime in cyber cloud. We need better secured model for cloud deployment and forensic investigation techniques to extract evidence from cloud-based environments in case of any cyber attack. This paper discusses the comprehensive models that provides cyber Forensics capabilities on cloud computing.

Keywords: cloud computing; forensic; cybercrime; forensic investigation.

GJCST-B Classification : C.2.4, C.2.1

CYBERFORENSICINVESTIGATIONANDEXPLORATIONONCLOUDCOMPUTINGENVIRONMENT

Strictly as per the compliance and regulations of:

Cyber Forensic Investigation and Exploration on Cloud Computing Environment

Dr. S Santhosh Baboo α & S. Mani Megalai σ

Abstract- Cloud service providers are providing more services on demand. Usage of Cloud in IT Industry, Educational Institution, Social network, Medical Field and other business Industry are tremendously increased. This increases the more criminal activity on cloud. There is a need for forensic capabilities which support investigations of crime in cyber cloud. We need better secured model for cloud deployment and forensic investigation techniques to extract evidence from cloud-based environments in case of any cyber attack. This paper discusses the comprehensive models that provides cyber Forensics capabilities on cloud computing.

Keywords: cloud computing; forensic; cybercrime; forensic investigation.

I. Introduction

Cloud Forensic system has the greater demand in this generation. Since the cloud computing has more advantages for the business, most of the companies are deploying their applications on cloud which leads to more cyber attack on cloud. This brings more research for the digital forensics on cloud to identify the criminals in the virtual environment. Since there is constant increase in the cyber attacks across countries in multi-tenant cloud with new trends, the Investigation system is necessary to meet the current challenges in the distributed environment.

Cyber Forensic Investigation and Exploration for cloud computing brings new technical and legal challenges. The forensic investigation on cloud computing is being different by the evidence distributed on virtual environment, less control of physical access, and more secured policies and methods to be followed by the service providers to improvise integrity and authenticity. The difficulty persists in cloud environment in acquisition of remote data, huge data volumes, data ownership and the distributed data across virtual environment.

Generally, if any cyber attack happens on any environment, there should be options to perform their investigations on the server without involving third party service providers. In the Cloud computing environment, service providers have control over the cloud environment. The Investigation process is to be handled by the service providers or the company who deployed the application. [1] To find the victim who had accessed or tampered the secured data, we need to implement digital forensics procedures in clouds [2]. The current forensic investigation practices do not match with the cloud computing characteristics. New methodology is to be implemented for investigating cyber attack on cloud. This paper will confer the forensics aspects of cloud computing by pointing out the forensic investigation issues in cloud computing and recommending new model that provides cyber forensic capabilities in cloud.

II. Related Work

The survey on cyber crime Investigation on cloud discusses various aspects of issues. Ting Shang evaluates the conventional forensic investigations and forensic investigations in cloud and analyses the challenges in cloud Forensic.[3] Shahrzad Zargari, David Benford provides an overview of cloud forensics including the issues and the existing challenges in order to give better future prospects and also offers some steps to be taken to overcome these challenges [4]. Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud and Solahuddin bin Shamsuddin presents the Investigation challenges in cloud environment. They have recommended the solutions like Utilizing TPM in hypervisor, updation of cloud service provider policy to provide the persistent storage devices and multilevel authentication to overcome the challenges in cloud [5].

The cloud computing becomes the most powerful environment for the upcoming companies. In cloud computing the forensic investigation support is not completely given by the cloud providers. There are few challenges in attaining the forensic support. The author highlights the cloud characteristics, models, architecture and the challenges in achieving Forensic support. Some of the challenges are data recovery in finding and retaining forensic evidence from law enforcement perspective. New methods are proposed to bring the evidence of the cyber attack in the cloud environment. Likewise there are challenges in Investigations on virtual machine. Henceforth, the extended Forensic Investigation system is mandatory to meet the Forensic challenges in cloud environment. [6]

a) Threats of Cloud Security Issues

The target of cloud computing is to setup a safe and reliable data storage and network service. The applications are extended over the Internet domain to the CSP, which maintains computer systems in clusters

Author α: Associate Professor, Department of Computer Science and Applications, D. G. Vaishnav College, Chennai.
Author σ: Research Scholar, Ph.D. Research Scholar SCSVMV University, Kancheepuram. e-mail: megalaimini@gmail.com

Apart from all the advantages of the cloud service, cloud data security is the main issue in the quality of service. Since cloud computing is not just a third party data warehouse, the data stored in the cloud may be updated frequently by other users, including insertion, deletion, and modification. Thus, so long as the data is stored in the cloud, there are some unavoidable threats of cloud security issues to the personal users and enterprises. [7]

A. Data Storage Issue
B. Personal Privacy Issue
C. Trust of CSP issue

III. Proposed Work

a) Proposed Architecture

Based on the Virtual Machine Introspection method the Forensic Investigation Architecture is built. Cyber forensic Investigation system involve Markov chain algorithm for Investigation.

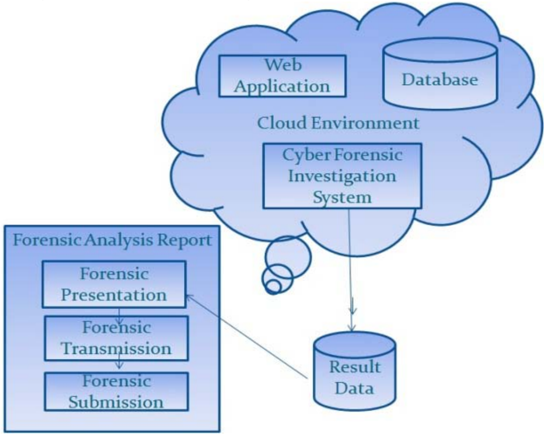


Figure 1 : Cyber Forensic System Architecture

Integrated application setup detects the runtime state of a system-level virtual machine and that information is recorded by the tracker system. Data Acquisition and reporting handled with the acquired knowledge by the Investigation system. Our Investigation system will involve in Identification of Crime, Collection of Evidence, analysis and presentation of the Forensic report.

b) Framework for Forensic Exploration

i. Virtual Machine Introspection

The framework for investigation of crime on cloud is done with the Virtual Machine Introspection (VMI). This is the technique which keeps tracking the hardware events and the user's behavior. Cyber Forensic system can be integrated in the virtual environment (Hypervisor, Virtual Architecture). For virtual machine introspection, the Investigation system logs the runtime state with the help of the registry, server memory, network etc. Based on this, Forensic Investigation report can be presented.

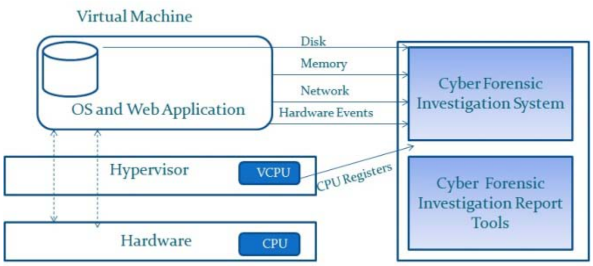


Figure 2 : Virtual Machine Introspection

c) Cloud Forensic Investigation Model using Markov Chain

Interaction of each node related with forensic actions on cloud environment and the derivation of data from the login details of the user, timestamps, event access, web page cache and logs. In this section, Cyber Criminal Activity Analysis Models using Markov Chain is proposed.

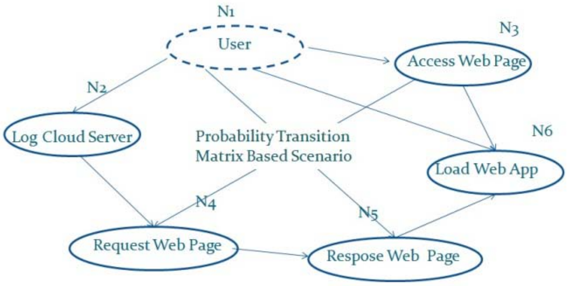


Figure 3 : Interaction of each Node Related Forensic Action on Cloud Environment

For example, the user visits the e-commerce web application deployed in cloud for hacking the user's personal information. The Node N1 and N2 comprise who logged into the server, the N3 and N4 describes when and what web page is being accessed etc. The N5, N6 specify when and which programs are being executed. Based on the six nodes of forensic actions, all of the summarized forensic data are derived and logged in the cloud server with time intervals. Based on the communication of each node, the probability of Forensic action is determined by our Cloud Forensic Investigation Model using Markov Chain.

When user established the connection to the cloud server then server allow to access the web page and request the web page from user. The cloud server allow and response to authentication users only. If the user authentication verified successfully then load web application to allow access web application and request wed application.

i. Transitional Probabilities

As we discussed, we determine w_{ij} as the number of forensic actions N_i involved by the user and N_j were number of times accessed the website or web pages. We calculate the probabilities of forensic action w_i as the sum of all the weights of edges pointing to p_i.

$$W_i = \sum_k \in In(N_i)W_{ki}$$

Using these weights, we can then estimate the prior probabilities of the forensic action, as well as the transition probabilities between two nodes.

ii. *Prior Probabilities*

The forensic probabilities are calculated with the N forensic action and the matrix of the pages visited Q. The probability of the algorithm is calculated based on the type of the forensic action. The first probability (PFA)computes the probability of the page visited by the user between the nodes N1 and N6.The second probability(SUFA) is the calculation of the more common nodes previously visited by many of the users. The third probability is the calculation of the probabilities of the same pattern of access between the nodes. *PFA (Priority of Forensic Action):*

$$O(P_i) = \frac{1}{M} \text{ and } O(P_k, P_i) = \frac{1}{|Out(P_k)|}$$

- ➢ SUFA (Semi-Usage Forensic Action):

$$O(P_i) = \frac{1}{M} \text{ and } O(P_k, P_i) = \left(\sum_{P_j} \in Out(P_k)^{w_{kj}}\right)^{-1}$$

- ➢ UFA (Usage Forensic Action):

$$O(P_i) = \frac{W_i}{\sum_{P_j} \in WS^{W_j}} \text{ and } O(P_k, P_i) = \frac{W_{ki}}{\sum_{P_j} \in Out(P_k)^{W_{kj}}}$$

IV. Results and Discussion

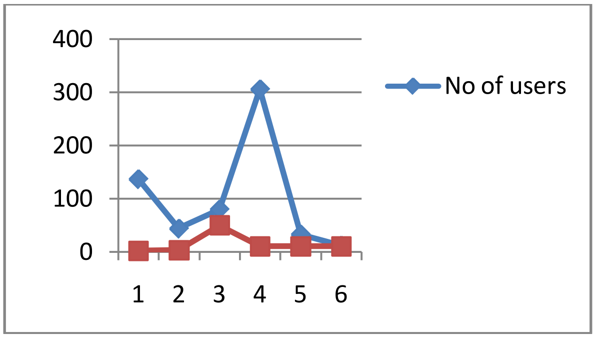
Probabilities of hacking the data or tampering the data are computed by the sum of the weights specified in the algorithm. Every action of the user are monitored and logged by our Investigation system. List of manipulated logged history of the users and the crime probability derived from the user's behavior are shown in tabular column.

Our experiments assume that some of the cloud consumer is the victim of the crime investigation. This situation demands proactive logging of data by the provider which may be of forensic relevance for investigation.

Table 1 : Probability of Forensic Relevance

No of Users	Logged Users	Page Name	Accessed Database	Crime Probability
137	10	Products	137	2
44	44	Personal Information	44	3
80	80	Payment gateway	80	50
306	0	Home page	0	10
33	0	Contact	0	10
12	0	About Us	0	10

Table 2 : Forensic Investigation Probability



V. Conclusion

This paper elaborates the opportunities of applying cyber Forensics in cloud computing. The proposed cloud Forensic model is to be designed with the above mentioned steps and methods. This paper gives a brief introduction to the cloud computing concept and its Cyber Forensics issues and challenges. We outline a new forensic issue for cybercrime in two aspects as collection and preservation. Since cybercrime evidence belongs to electronic evidence, it is easy to be destroyed and tampered with during the forensic procedure. In order to ensure the primitiveness and integrity of the evidence, it should image the relative records and files absolutely. A new cybercrime forensic system is proposed to be set up in cloud computing. An analysis is set up as a special network service in the cloud to communicate with each server. Through the analysis, forensic experts can detect behaviors threatening to servers in the cloud and capture volatile information for late-time analyses by the skilled forensic toolkit. The performance of the forensic system is relative to the scale of the cloud, which should be improved in later research.

References Références Referencias

1. Cunt P. Garrison, "Digital Forensics for Network, Internet and Cloud Computing", Publication Copyright © 2010 Elsevier Inc.
2. Mark C. Chu- Carroll, "code in the Cloud", Copyright © 2011 Pragmatic Programmers, LLC.
3. Ting Shang, "Forensic investigations in Cloud environments, 2012 International Conference on Computer Science and Information Processing (CSIP).
4. Shahrzad Zargari, David Benford, "Cloud Forensics: Concepts, Issues, and Challenges", 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT).
5. Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud, Solahuddin bin Shamsuddin, "Forensics investigation challenges in cloud computing environments", 2012 International Conference ON

Cyber Security, Cyber Warfare and Digital Forensic(Cyber Sec).

6. Tony Krone, Concepts and Terms: High-Tech Crime Brief. No. 1 (2005); Kim-Kwang Raymond Choo, Russell Smith and Rob Mc Cusker, ‘Future Directions in Technology-Enabled Crime: 2007-09’ (Research and public policy series No 78, Australian Institute of Criminology, 2007).
7. Yan, Cheng, “Cybercrime Forensics System in Cloud Computing”, 2011 International Conference On Image Analysis and Signal Processing (IASP).