*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. II (July – Aug. 2015), PP 44-48*
*www.iosrjournals.org*

# Analysis of Forensic Activity on Multitenant Cloud Web Hosting

Capt. Dr. S Santhosh Baboo[1], S. Mani Megalai[2]
[1] *Associate Professor,* [2] *Research Scholar,*
[1]*Department of Computer Science and Applications, D.G.Vaishnav College, Chennai – 600106*
[2] *Ph.D. Research Scholar SCSVMV University, Kancheepuram*

***Abstract:*** *Cloud computing has become bounteous target for populous IT Industry and other Commercial Industries. Multitenant Cloud Hosting is the popular hosting for numberless providers. Multitenant shares the single application and the data would be different. There should be isolation of data and the logs between each company. There is a challenge to analyze the criminal activity on multitenant cloud environment. It is strenuous to analyze the forensic activity without violating the privacy of other company users. We require desirable forensic processes which support investigations of crime in multi tenant cloud hosting. This paper explains the methodology to trace the physical network location of the criminal who has accessed the highly secured Account Information of the customer. And also demonstrates the architecture and methodology to investigate crime in multi tenant cloud hosting.*

***Keywords:*** *cloud computing; forensic; cybercrime; forensic investigation; multitenant*

## I. Introduction

Cloud computing is the current trend in real time web environment. Mulititenancy Model Cloud is the utmost used model which is very cost effective for the customers and business benefit for the service providers. Multitenant Architecture is a financial gain for Service providers who handle Business Information System (BIS), Customer relationship Management (CRM) and Enterprise Resource Planning (ERM). The degree of multitenancy can be measured based on how much of the business architecture is shared across tenants. The database schema can also be shared across multi tenants for Business logic, User Interface design, task flow are customized based on the requirements. Extended complexity is available for Investigation of crime in multitenancy cloud. [1] When we have physical storage we will be able to find where exactly the data is located although in cloud storage the data could be anywhere in the machine, we perceive where the data is located. When data is stored in cloud, it is mere hard to identify the location it may be anywhere inside the country or in other countries. In a previous generation system, forensic investigation is handled on physical servers and we can analyze the data on the same. This is not the case with cloud servers. The data is scattered in virtual machine via multiple data centers which leads through multiple data centers and it is burdensome to collect the required data for investigation in virtual environment. In a local environment, we have access to the virtualization environment, where we can access the hypervisor, manage existing virtual machines, delete a virtual machine, or create a new virtual machine. In the public cloud, we ordinarily do not have access to the hypervisor, however if we absolutely have access, we can run a private cloud.[2]

In the traditional way of forensic Investigation we will be able to analyze the data from the physical servers. We can accomplish the Investigation on data in cloud environment with the support of the service providers. Since he will not be an expert in forensic investigation, it will be very hard to acquire the necessary data for our Investigation.[2]

Network forensics comes in to picture when cyber attack involved in web hosting. Organization is responsible for extracting evidence from the data hosted on web, to determine the hacker who had executed the illegal access of the web application, to identify the methodology used to hack the service and to determine what type of data is attacked. Network forensic investigators must scrutinize the collected data such as file systems, processes, registry and network traffic to derive the Investigation Analysis.[3] This paper provides the methodology to identify the criminal activity and locate the physical location of the hacker and submit the Investigation Report for further Investigation.

## II. Challenges of Cyber Forensics in Multitenant cloud hosting

Multi tenant hosting in cloud environment enables the customer to avail the advantages of sharing the infrastructure with lower cost. In case of cyber attack there are bountiful challenges to be handled by the organization. The tenant can always question regarding the privacy of their private data while collecting the evidence of other tenants, it may contain the confidential data of other tenant's data. As discussed, it is possible to collect the traces of attack from the registry, network logs or through certain attack pattern algorithm. Soon

after there is further possibility for the hacker on cloud to erase all the evidence on cloud network and this cannot be detected for numerous years.[4]

Another major issue is the lack of control over the evidence. The physical inaccessibility of the evidence and lack of control over the systems acquiring proof is a challenging task. In order to access network logs or data logs, cloud consumers are necessitated to depend on cloud service providers. The adoption of virtual machines fabricates the service providers a herculean task to track the origin of the attack. For example, VMware provides a snapshot facility that can be utilized to provide a picture of your system. The picture provides an image of hard drive, data stored on the hard drive, and its VMware configuration. The snapshot may sound like an ideal source for evidence, although the use of VM artifacts in court is questionable.[5]

There is a risk of insider attack when it comes to accessing evidence from the cloud service provider. Due to lack of physical access to evidence in order to carry out an investigation, forensic experts are compelled to rely on cloud service providers to obtain the data and network log.

## III. Related Work

According to Keyun Ruan, "Cloud forensics is intricate as long as there are challenges with multi-tenant hosting, synchronization problems and techniques for segregating the data in the logs [6].Jason Flood describes a possible system and methodology that would prevent the gap analysis phase of a cyber-attack and proposed a distinct approach to defending a modern complex multi-tenant cloud system from outside attack by detecting the attacker during the discovery phase and neutralizing the attack before damage is rendered to the organization [7].Virtual Machine Introspection (VMI) can also be comfort in forensic investigation. Using this process, the investigators can execute a live forensic analysis of the system, while keeping the target system unchanged. Cheng Yan illustrated a network service in the cloud as an analysis engine to monitor the behavior of the network user and extract the evidence neverthless provide the determined results [8]. Tobias Gebhardt discusses the complications of dynamic migration of virtual machines and provided a generic model for network forensics in the cloud. Network Forensics on cloud discussed collection, analysis, and reporting of information in related with security incidents and computer-based criminal activity [9]. Shams Zawoad and Ragib Hasan proposed a methodology to build proof and evaluated its performance. [10]. Rama Satish K V, Dr. N P Kavya demonstrated Cloud model for Data Intensive Application and compared the performance with Data Acquisition and Analysis Method.[11] With reference to all these papers we demonstrated a prominent architecture and compared the performance with Data Acquisition and Analysis Method.

## IV. Proposed Work

### A. Proposed Architecture

The Investigation is handled with the Dynamic Host Configuration protocol in the multi tenant cloud web hosting. It is crucial to maintain the DHCP logs of multiple tenants without attaining conflicts in to one another. The IP Address of all the clients who accessed the website hosted in cloud environment is identified from the firewall logs, event logs. IP Address can be queried based on the DHCP server and stored in the database. The IP Address will not be sufficient to locate the physical location of the client's machine used for hacking since the IP changes in Virtual environment. We require Media Access Control Address (MAC) to identify the Physical Address of the machine.

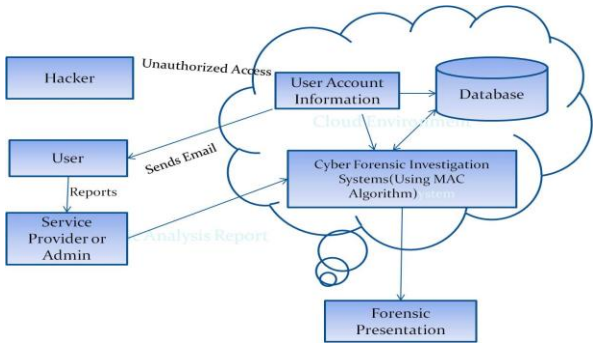


**Figure - 1:** Forensic Architecture on Multitenant Cloud

### B. MADA Algorithm (MAC Address Derivation Algorithm)

This algorithm is used for Identifying IP Address and MAC Address of Client Machine.

Procedure LogMACAddress (user_ID)

1. Require ip_address, mac_address
2. If ip_address = 'Null' then

**3.** ip_address <- Getenv(serverid or client id);
**4.** end if
**5.** If mac_address = 'Null' then
**6.** mac_address<-shellexecute('arp- a'.escapeshellarg(ip_address));;
**7.** end if
**8.** if tb_MAC_details = 'Null' then
**9.** tb_MAC_details <- userid;
**10.** else
**11.** MAC_Address <- MacAddress + tb_MAC_details <- userid
**12.** End if
End Procedure
Function GenInvestigationRep (Userid)
**13.** GetMacAddress(Userid);
**14.** GenerateReport(Userid);
End GenInvestigationRep

### C. Flowchart for Investigation Process:

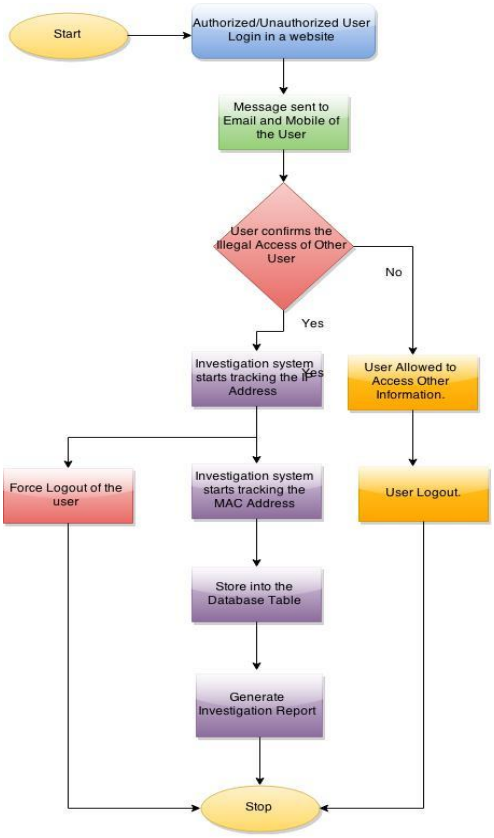


**Figure - 2:** Flowchart for Investigation Process

Illegal access of User's Profile by anonymous user is identified through email base algorithm. Log History is maintained for all the Authenticated Users or unauthenticated users. When user logged in to the system, the user receives the confirmation message on his successful login to his email. If he denies his authentication, the Investigation process will be triggered. The Investigation system will identify the IP Address from User log/events log and obtain the MAC Address with the IP Address of the machine and Store the MAC address of the client machine which is used for unauthorized access of user profile. With the MAC Address, we derive the physical location of the machine and at that point store the Mac Address for the user id in the Database and generate the Investigation Report.

## V. Experimental Results and Discussion

Multitenant cloud model help reducing the cost for service providers in delivering the SAAS in multi tenant architecture. The Integration of Investigation system in to multi tenant is implemented. Segregation of DATA and the Investigation of crime for all the tenants are discreetly performed. The Network Information

such as IP Address, MAC Address and other related information is captured in the proposed Methodology which helps to investigate the Crime in Multi tenant Cloud Environment. The performance of our Investigation system has been analyzed with the parameters of number of users and the execution time with the existing Data Acquisition
and Analysis method.

**Table-1:** Execution time of Forensic Investigation

| **Proposed Method** | | | | |
|---|---|---|---|---|
| **No.of Users** | **No. of Users** | | **No. of Attacks** | **Execution Time (in ms)** |
| | **Authorized** | **Un authorized** | | |
| 100 | 70 | 40 | 30 | 40 |
| 200 | 180 | 30 | 20 | 30 |
| 300 | 295 | 8 | 5 | 6 |
| 400 | 360 | 50 | 40 | 55 |
| 500 | 475 | 35 | 25 | 35 |
| 600 | 590 | 10 | 10 | 15 |
| 700 | 645 | 55 | 55 | 68 |
| 800 | 780 | 20 | 20 | 30 |
| 900 | 895 | 5 | 5 | 6 |
| 1000 | 1000 | 0 | 0 | 0 |

**Table-2:** Execution time of Data Acquisition Method

| **Existing Method** | | | | |
|---|---|---|---|---|
| **No.of Users** | **No. of Users** | | **No. of Attacks** | **Execution Time (in ms)** |
| | **Authorized** | **Un authorized** | | |
| 100 | 70 | 40 | 30 | 500 |
| 200 | 180 | 30 | 20 | 400 |
| 300 | 295 | 8 | 5 | 70 |
| 400 | 360 | 50 | 40 | 660 |
| 500 | 475 | 35 | 25 | 470 |
| 600 | 590 | 10 | 10 | 200 |
| 700 | 645 | 55 | 55 | 800 |
| 800 | 780 | 20 | 20 | 400 |
| 900 | 895 | 5 | 5 | 70 |
| 1000 | 1000 | 0 | 0 | 0 |

The advantages in the proposed method is the minimal execution time in investigation of crime and the probability of finding physical location of cyber attack on multi tenant cloud hosting is higher with proven results.

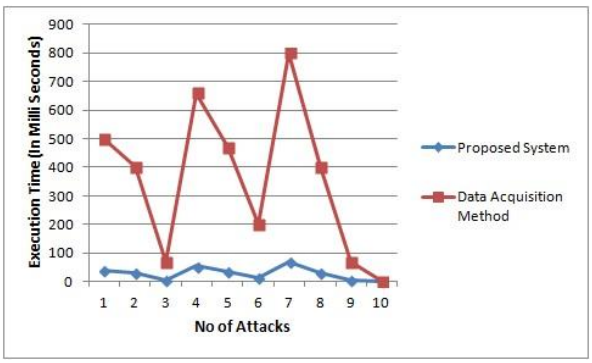


**Figure - 3 :** Forensic Investigation Execution Performance

For every attack the Investigation system triggers the event for identifying the IP Address and MAC Address of the system used to hack the profile. The performance of the proposed Investigation is compared with Data Acquisition Method and highlighted in the above graph. We have measured the execution time for number of attacks (varying from 1 to 60) among 1000 users. The determination of results proves that the proposed Investigation system's execution speed performs at higher rate as compared to the Data Acquisition method.

## VI. Conclusion

Cyber forensic investigation is one of the key concerns in cloud computing. Organizations are not convenient in adopting the cloud when highly confidential data are hacked and due to the lack of the availability of Cloud Forensic methods. In this paper, we present MAC Algorithm to Investigate in Multi tenant cloud environment with prevention of accessing other tenant's data. Introduced a framework to handle the Forensic investigation on multitenant cloud deployment,

## References

[1]. http://www.computerworld.com/article/2517005/data-center/multi-tenancy-in-the-cloud--why-it-matters.html
[2]. http://resources.infosecinstitute.com/overview-cloud-forensics/
http://searchcloudsecurity.techtarget.com/tip/Cloud-forensics-An-intro-to-cloud-network-forensic-data-collection
[3]. http://www.dummies.com/how-to/content/multitenancy-and-its-benefits-in-a-saas-cloud-comp.html
[4]. Manish Hirwani Yin Pan Bill Stackpole Daryl Johnson, Forensic Acquisition and Analysis of VMware Virtual Hard Disks, 2012 Rochester Institute of Technology
[5]. http://ccskguide.org/an-introduction-to-cloud-forensics/ Jason Flood, AnthonyKeane, A Proposed Framework for the active detection of security vulnerabilities in multitenancy cloud systems. , 2012 Third International Conference on Emerging Intelligent Data and Web Technologies, IEEE 978-0-7695-4734-3/12
[6]. Cheng yan, Cybercrime Forensic System in Cloud Computing, Department of Computer Science and Engineering, East China University of Political Science and Law, Shanghai, China, IEEE 2011, 978-1-61284-881-5/11 Tobias Gebhardt, Hans P. Reiser, Network Forensics for Cloud Computing, Volume 7891, 2013, pp 29-42
[7]. Shams Zawoad, Ragib Hasan, I Have the Proof: Providing Proofs of Past DataPossession in Cloud Forensics, 2012 International Conference on Cyber Security, IEEE978-0-7695-5014-5/12
[8]. Rama Satish K V, Dr. N P Kavya , A New Efficient Cloud Model for Data Intensive, Global Journal of Computer Science and Technology (B), Volume XV Issue I Version I, 19-30.