International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

A Log-based Approach Cloud Computing to Access Secure File to Make Digital Forensics Easier

Gundecha Nilesh
nil.gundecha@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Supekar Namdev
namdevsupekar@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Ransing Kailas
Kailasransing92@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Bhambure Ratndip
Ratnadip143@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Prof.Ritesh Thakur
hod_comp_iok@yahoo.com
SP'sInstitute of Knowledge College Of Engineering, Department of computer engineering,

Savitribai Phule University

Abstract:

Cloud computing is getting more and more attention from the information and communication technologies industry recently. Almost all the leading companies of the information area show their interesting and efforts on cloud computing and release services about cloud computing in succession. But if want to make it go further, we should pay more effort on security issues. Especially, the Internet environment now has become more and more unsecure. With the popularization of computers and intelligent devices, the number of crime on them has increased rapidly in last decades, and will be quicker on the cloud computing environment in future. No wall is wall in the world. We should enhance the cloud computing not only at the aspect of precaution, but also at the aspect of dealing with the security events to defend it from crime activities. In this paper, I propose a approach which using logs model to building a forensic-friendly system. Using this model we can quickly gather information from cloud computing for some kinds of forensic purpose. And this will decrease the complexity of those kinds of forensics.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Keywords: Cloud computing; digital forensic; log; security

Introduction:

Cloud computing is a hot topic in recent years. It exhibits the following key characteristics: agility, low cost in using, device and location independence, virtualization, reliability,scalability and elasticity, performance and etc. All those features show fascinating benefit to companies. As they can get free from the worry about the investment on hardware and can setup up their business easily. There are three major types of cloud services delivery model: Infrastructure as Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Different type of delivery model provides different convenience. IaaS just likes server-hosting services, but consumers do not need pay for hardware and maintain them anymore. They benefit much from the scalability and elasticity. PaaS is like service-hosting, but consumers do not need to worry about the servers out of working or not able to response to large number of requests. They benefit much from the performance and reliability. SaaS looks like the Representational State Transfer (REST) very much, and makes consumers benefit from performance, multi-tenancy architecture and many other features. But both of the three models share a weakness from the characteristics of the cloud computing. As consumers put their logical procedurals on the cloud, which means that they do not own the control of the hardware especially for PaaS and SaaS. This is not friendly to digital forensic. Because traditional digital forensic is deeply depending on the media seized from the crime scene. At this point, there should be changes or enhancement for cloud computing to be friendlier with digital forensics. In this paper I will focus on analyzing challenge for forensic investigation in cloud environments.

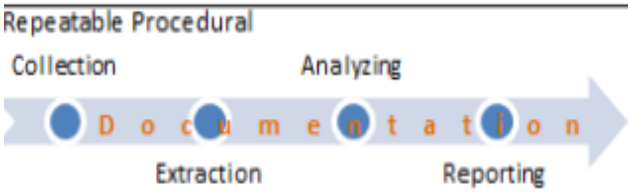


Figure 1. Main steps of digital forensics.

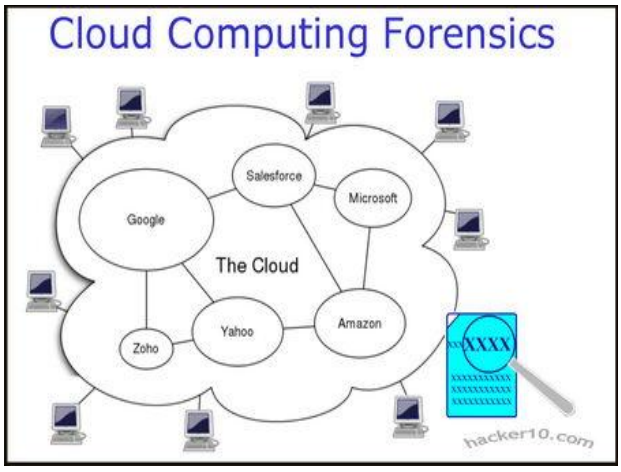
Problem Statement:

Existing system does not guarantee the security, there are lot of disadvantages are there. Here we are going to overcome that.

Scope:

We are going to develop A Log-based Approach to Make Digital Forensics Easier.

Architecture:



Existing System:

The identification of evidence in the cloud computing environment can be very complex. To different deployment model, which knows as

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

public cloud, private cloud and hybrid, has deep affection on forensics procedural. If the evidence resides within a public cloud, it will be much more difficult to identify. There are different computer forensic challenges related to the different services models, PaaS, IaaS and SaaS. These models present subtly different challenges to the forensic investigator. While trying to process the forensics procedural in cloud, we will meet grate obstruction at the very beginning. We cannot seize the hardware containing or processing the target applications from the cloud, as they can be everywhere in the world or even no real hardware such as Virtual Machine. By the use of Existing System, the nature of dynamic scaling up and down makes the possibility of losing information higher.

Disadvantages of Existing System:

No Security, attempt to block the account, hacking password etc.

Proposed System:

Here we should keep another log locally and synchronously, so we can use it to check the activities on cloud while without the help of the CSPs. The content that would be recorded in the log files (the log files can be files or database) should be decided by the CSPs, but not the agent itself. That is to say the log files should be operated by a module created by the CSP. This is to make sure that the log files stored in local and in cloud are comparable. The local log module will use that information on the log record locally. Then we compare the local log with the log files that are maintained in the cloud, we can easily identify the fake users.

Advantages of Proposed System:

In this proposal, if anyone made an attempt to hack the password, the account will be blocked. Only account holder can renew it. We are maintaining log files, from that we got users registration time, file download time etc.

System Configuration:-

H/W System Configuration:-

- Processor - Pentium –III
- Speed - 1.1 GHz
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVG

S/W System Configuration:-

- Operating System :Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Java, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : My sql
- Database Connectivity : JDBC.

Acknowledgement:

We have taken effort in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend my sincere thanks to all of them

We are highly indebted to our Head of Department Prof. Retesh Thakur and Project Guide Prof. Ajay K.Gupta for his guidance and constant supervision as well as providing necessary information regarding the project & also for their support in completing this work

Conclusion:

There is no doubt that cloud computing will be the most popular operation mode for business. Whilst there will be more and more crimes against it too. For all the participator of cloud computing, they should prepare for that change. In this paper we have proposed a log-based model for. The log-based model can help to reduce the complexity of forensic for non repudiation of behaviors on cloud. However, it is totally no enough for the other kinds of digital forensics. What makes matters worse is that, till now, there are still no guidelines or standards for the cloud security. Most of times, we modified the guidelines of traditional digital forensics to suit for cloud computing environment independently.

References:

[1] D. Brezinski and T. Killalea. Guidelines for evidence collection and archiving. RFC 3227, IETF, 2002.

[2] Birk, D.; Wegener, C. Technical Issues of Forensic Investigations in Cloud Computing Environments. 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)

[3] Ahmed, S.; Raja, M.Y.A. Tackling cloud security issues and forensics model. High-Capacity Optical Networks and Enabling Technologies (HONET.

[4] Stephen D. Wolthusen, Overcast: Forensic Discovery in Cloud Environments, 5th International Conference on IT Security Incident Management and IT Forensics

[5] Cheng Yan, Cybercrime forensic system in cloud computing, Image Analysis and Signal Processing (IASP)

[6] Stephen Biggs, Stilianos Vidalis. Cloud Computing: The impact on digital forensic investigations. International Conference for Internet Technology and Secured Transactions

[7] Hong Guo; Bo Jing. Forensic investigations in Cloud environments. International Conference on Computer Science and Information Processing (CSIP)