An Approach for Digital Forensics on Cloud Computing

[1]Kandikuti Amara Babu, [2]M.Madhava Rao
[1,2]Sir C.R.Reddy College of Engineering, Eluru, Andhra Pradesh, India

Abstract
Cloud computing became the most talked about technology in Information and communication technology in recent times.
Many technology majors are using this technology and the scope of cloud computing is increasing day by day. Very important concern of the industry now is the Security. The cloud computing architectures often lack support for computer forensic investigations. Besides this, the existing digital forensics tools cannot cope with the dynamic nature of the cloud. This paper examines the challenges of digital forensics in the cloud, possible attacks on cloud-evidence, and mitigation strategies against those challenges.

Keywords
Cloud Computing, Forensic Investigations, Digital Forensics, Mitigation Strategies

I. Introduction

Cloud computing offers immense opportunities for business and IT organizations by providing highly scalable infrastructure resources, pay-as-you-go service, and low-cost on-demand computing. While clouds attract diverse organizations, the security and trustworthiness of cloud infrastructure has become a rising concern. Clouds can be a target of attacks or can be used as a tool to launch attacks. Malicious individuals can easily exploit the power of cloud computing and can perform attacks from machines inside the cloud. Many of these attacks are novel and unique to clouds digital forensics can be defined as an applied science for the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Figure 1 illustrates the process flow of digital forensics. Cloud forensics can be defined as applying all the processes of digital forensics in the cloud environment. Cloud forensics can be defined as a subset of network forensics , because cloud computing is based on extensive network access, and network forensics handles forensic investigation in private and public networks. However, cloud forensics also includes investigating file systems, process, cash, and registry history. Different steps of digital forensics shown in Figure 1 vary according to the service and deployment model of cloud computing.

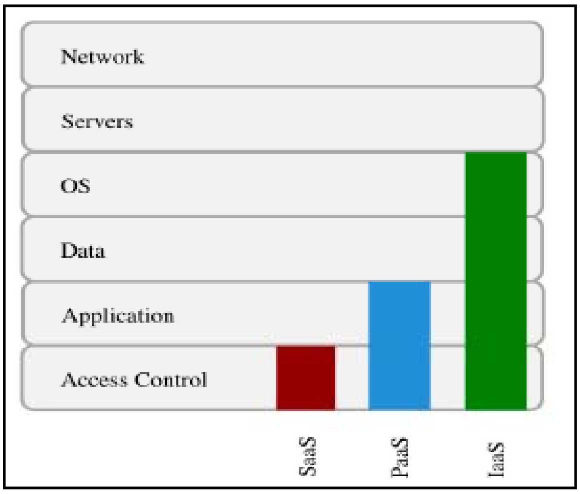

Fig. 1: Different Layers in Different Service Model

II. Existing System

The identification of evidence in the cloud computing environment can be very complex. To different deployment model, which knows as 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. The disadvantage of the existing system is that No Security, attempt to block the account, hacking password etc.

III. Proposed System

In the proposed system 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. Several characteristics of cloud computing complicate the process of cloud forensics. As the storage system is no longer local, law enforcement agents cannot confiscate the suspect's computer and get access to the digital evidence even with a subpoena. In a cloud, each server contains files from many users. Hence, it is not feasible to seize servers from a data center without violating the privacy of many other benign users. Moreover, even if the data belonging to a particular suspect is identified, separating it from other users' data is difficult. The trustworthiness of the evidence is also questionable, because other than the cloud provider's word, there is no usual way to link a given evidence to a particular suspect. The following issues make cloud forensics challenging.

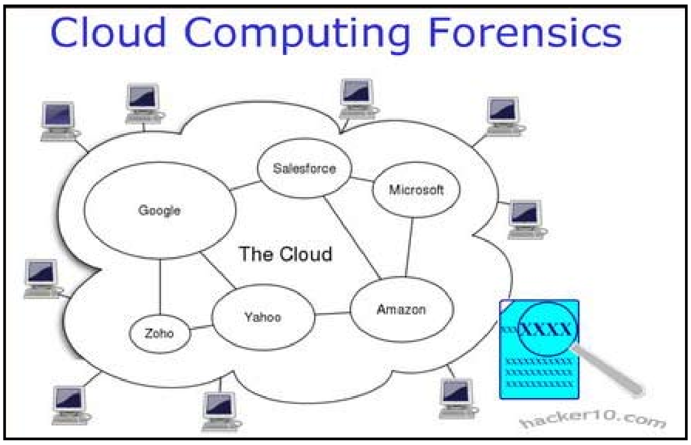

Fig. 2:

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. 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. In traditional computer forensics, investigators have full control over the evidence. Unfortunately, in a cloud, the control over data varies in different service models. Cloud computing is a multi-tenant system, while traditional computing is a single owner system. To give an analogy, the cloud can be compared to a motel, while the other can be compared to a personal house. In a cloud, multiple Virtual Machines can share the same physical infrastructure, i.e., data for multiple customers can be co-located. Currently, investigators are completely dependent on CSPs for acquiring cloud evidence. However, the employee of a cloud provider, who collects data on behalf of investigators, is most likely not a licensed forensics investigator and it is not possible to guarantee his integrity in a court of law. A dishonest employee of a CSP can collude with a malicious user to hide important evidence or to inject invalid evidence to prove the malicious user is innocent. On the other hand, a dishonest investigator can also collude with an attacker. Even if CSPs provide valid evidence to investigators, a dishonest investigator can remove some crucial evidence before presenting it to the court or can provide some fake evidence to the court to frame an honest cloud user. In traditional storage systems, only the suspect and the investigator can collude. The three-way collusion in the cloud certainly increases the attack surface and makes cloud forensics more challenging.

IV. Conclusion

we discussed the technical challenges of executing digital forensic investigations in a cloud environment and presented the requirements to make clouds forensics-friendly. Collecting trustworthy evidence from a cloud is challenging as we have very little control over clouds compared to traditional computing systems. For now, investigators need to depend on the CSP to collect evidence from a cloud. To make the situation even worse, there is no way to verify whether the CSP is providing correct evidence to the investigators, or the investigators are presenting valid evidence to the court. Thus, we need to build a trust model to preserve the trustworthiness of evidence.

References

[1] K. Kent, S. Chevalier, T. Grance, H. Dang,“Guide to integrating forensic techniques into incident response”, NIST Special Publication, pp. 800–86, 2006.
[2] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie,“Cloud forensics: An overview”, In proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.
[3] AWS (2012),“Amazon web services”, [Online] Available: http://aws.amazon.com
[4] R. Marty,“Cloud application logging for forensics”, In proceedings of the 2011 ACM Symposium on Applied Computing", ACM, 2011, pp. 178–184.
[5] T. Ristenpart, E. Tromer, H. Shacham, S. Savage,“Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds”, In Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 199–212.
[6] D. Birk, C. Wegener,“Technical issues of forensic investigations in cloud computing environments”, Systematic Approaches to Digital Forensic Engineering, 2011.
[7] J. Vacca,"Computer forensics: Computer crime scene investigation", Delmar Thomson Learning, 2005, Vol. 1.
[8] S. Zawoad, R. Hasan,“Towards building proofs of past data possession in cloud forensics”, ASE Science Journal, 2012.