Securing Digital Forensics on Cloud Computing through Log based Accession

Raju Kadari¹, Janapati Venkata Krishna²

¹pursuing M.Tech (CSE), ²Associate Professor & HOD (CSE Department)

Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

ABSTRACT: Cloud computing is getting huge attention from the IT industry recently. Almost all the top most companies of the IT sector showing their interest and efforts on cloud computing and release services about cloud computing in succession. But it is vulnerable for security threats. If we want to make it go further, we should pay more attention on security threats. Particularly the Internet environment now has become unsecure. The number of crime on internet has increased at a great rate in last decades, and this unsecurity will be very fast on the cloud computing environment in future. We should further improve the cloud computing not only at the feature of precaution, but also at the feature of dealing with the security events to defend it from the crime persuit. In this paper, I propose a perspective which using logs model to build a forensic-friendly system. Using this forensic-friendly system model we can quickly gather information from cloud computing for some kinds of forensic purpose. And this perspective decrease the complexity of those kinds of forensics.

Keywords: digital-forensic, log, cloud-computing, security.

I. INTRODUCTION

Cloud computing is one of the leading technology in recent years. Many companies fascinated about the cloud computing because of these main characteristics like low cost in using, independence of location, performance and reliability and etc. Because of these benefits, all companies no need to waste money on hardware and they can setup their business easily. Cloud services provide three major delivery models those are PaaS i.e Platform as a service, IaaS i.e Infrastructure as a Service and SaaS i.e Software as a service. We can say In normal usage, the term "the cloud" is essentially a trope for the Internet. Marketers have made popularized the phrase "in the cloud" to says software, platforms and infrastructure that are sold "as a service" to the end users, i.e. remotely through the Internet. Typically, the vendor has actual energy-consuming servers which host products and services from a remote location, so end-users don't have to bother about server maintenance etc.; they can simply log on to the network without installing anything they can access services. The major models of cloud computing service are known as , platform as a service, Software as a Service and Infrastructure as,service. Google, Amazon, IBM, OracleCloud, Rackspace, Salesforce, Zoho and Microsoft Azure are some well-known cloud vendors. These cloud services may be offered in a public, private ,hybrid, network.

These models provides different services, Infrastructure as a service provides server-hosting service in this customer no need to pay and no need to worry about maintenance of hardware and other things related to service. Different type of delivery model provides different benefits. IaaS just likes server-hosting services, but endusers do not need pay amount for hardware and maintenance them anymore. They benefit much from the quality of being scalable and elasticity. PaaS is like service-hosting, but endusers do not need to worry about the servers or not able to response to large number of requests. They benefit much from the accomplishment and reliability. SaaS looks the Representational State Transfer (REST) very much, and makes endusers benefit from performance, multi-tenancy architecture and many different features. All of the three models share a weakness from the characteristics of the cloud computing. As endusers put their logical procedurals on the cloud, that means they do not own the control of the hardware particularly for PaaS and SaaS. These are not friendly to digital forensic. Because Conventional digital forensic is highly depending on the media seized from the crime scene. At this point, it should be change or enhance for cloud computing to be friendlier with digital forensics.

II. RELATED WORK

In this era of globalization, concentrating is the key to success for the small companies or those just on their beginning, mostly for those information technology (IT) industry. At this situation, outsourcing is a perfect way for progressive success, as they can more concentrate on the core business. At first level, they can outsource non-critical software or modules to other companies to reduce the risk and human resources of the company. The other one is to be outsourced should be the services or the hardware for computing and storage. And in my opinion, this is just the original driver to the popular of the cloud computing. Cloud computing is virtual computing
environment which can provide, platform and software support as remote services. And those services are accessed by Internet all over the world by consumers. Cloud computing is not a glossary in information technology as it wont replace the IT companies completely. It is more like an pseudonym for the new kind of business operation mode named “pay-per-use”. But it involves with many new technologies, for example virtual computing, distributed computing, parallel computing, massive data processing and etc. The CSP i.e Cloud Service Provider maintains large scale computer systems in clusters, and usually has large storage capacity on Data Center. The CSP provide effective system to meeting the customers’ requirements on software, service, computing and storage in a scalable mode. So we can think that the customer companies outsource some kinds of requirement to those CSPs.

Digital Forensic

Generally speaking, cloud security should contain two categories. One is how to protect cloud and other one is applications running inside from attack. And then how to deal with the happened security events. Precaution is the major concern on cloud security, but we should know that “no wall is wall in the world”. Criminal always can discover any way to overcome the security threats to get succeed in their goals illegally. In the digital world, the security department had started a new field of battle with criminals. They use digital forensic technology to disclose the crime events and the criminals.

Digital forensics (also referred to at times as computer forensics) enclose approaches and techniques for gathering and analyzing traces of human and computer generated activity in such a way that it is suitable in a court of law. The main goal of digital forensics is hence to perform a structured investigation into past and ongoing occurrences of data processing and transmission whilst maintaining a documented chain of evidence, which can be reproduced unambiguously and validated by competent third parties. According to RFC3227 we can come to an end the structured in and validated by competent third parties.

Challenges for cloud Forensic

The identification of evidence in the cloud computing environment can be very critical. To different deployment model, which knows as to be private cloud ,public cloud and hybrid, has deep affection on the forensics procedural. If the evidence reside in a public cloud, it will be more difficult to identify. There are vast different computer forensic challenges related to the different services models, SaaS, PaaS, IaaS. These models present different challenges to the forensic investigator. While trying to process forensics procedural in cloud, we will meet grate obstacle at the very beginning. We cannot block the hardware containing or we cannot processing the target applications from the cloud, as they can be presented everywhere in the world or even no real hardware such as a Virtual Machine. And the nature of effective scaling up and down makes the possibility of losing information at higher rate.

III Log-Based Approach for Cloud Forensic

In digital world, log is a regular or methodical record of actions that object has taken or statuses that object have been. Log is the most common component that be used in digital forensics. Gartner has warned that “Investigating inappropriate or illegal activity and it would be impossible in cloud computing. Cloud services are particularly difficult to investigate, because logging and data for multiple consumers may be co-located and may also be spread into an ever-changing set of hosts and data centers so ultimately this process is very complex.If you cannot get agreed in contract of commitment to support specific forms of investigation - along with evidence that the vendor has already successfully supported such activities - then your only safe assumption is that investigation and discovery requests will be impossible.”

On SaaS and PaaS, an application is always for only one single impetus. While what we can get from IaaS are VMs, and we can use them to many different motivations. Logging outside the VMs is not so useful, so the log model proposed later may just outfit for SaaS and PaaS.

PaaS

The way using SaaS is similar how we are using using software locally. The difference is we send command to server through network by using SaaS.

Figure 1. Main steps of digital forensics.
The Figure 2 shows how to communicate with SaaS.

In this model, endusers uses agent to send commands to SaaS. Then after SaaS exercise the commands and creates logs for that commands, then it will send back response. While enduser gets the reply, the agent may make its own logs or just exercise the response to enduser.

nevertheless, how can we prove that the enduser has used the Software as a Service or the nonrepudiation of activity? The easy answer is asking the Software as a Service CSP i.e Cloud Service Provider to furnish the logs of the software or services conventionally. But in a cloud environment, we should not await the Cloud Service Providers to contribute as much help and quick as the local servers can give. This means that we should remain another log locally, synchronously, so we can utilize it to check the activities on the Software as a Service cloud while without help of the Cloud Service Providers. The content that is recorded in the log files should be pronounced by the Cloud Service Providers, but not with agent itself. Ultimately to say the log files should be operated by a single module created by the Cloud Service Provider. This is to say that the log files stored in local and in cloud are similar. While the application on

PaaS
In Platform as a Service cloud, Cloud Service Providers can provide a type of runtime environment and further useful libraries or tools, for example a cloud service company Microsoft Azure supplies .NET framework and Google company supplies python tech and java runtime environment. The biggest difference between Platform as a Service and Software as a Service is that who develop the softwares, the Cloud Service Provider itself or a third-party. The Cloud Service Provider can use the resources on cloud such as storage system and file system easier than third-party systems. To apply the new model to Platform as a Service, the Cloud Service Provider should supply a log module on Platform as a Service to the third-party. So they can use it to store their own log information on the cloud. Even if the Cloud Service Provider supply then lower level APIs, the other third-party can create a customized log module, and of course it would applicable, for both of the enduser side and cloud side. So they can define the best quality and frequency for their business. And this is the manner they can do the

Software as a Service sends back the response, there will be a precise info. of the log record keep in Software as a Service such as unique id and timestamp. The local log module will use that info on the log record locally. Furthermore, for the consideration of preserving personal information, those files that should be readable only to particular tools or softwares that made by the Cloud Service Provider.

The Figure 3
Demonstrate the whole process of the communication briefly.

Figure 3. New communication model with SaaS
forensics even it don’t have any participation of Cloud Service Providers.

Figure 4 and 5 demonstrates the little difference of the two types

Figure 4. PaaS Using the log module

Figure 5. the log module of its own
IV Conclusion

There is no uncertainty that cloud computing will be the more popular operation mode for business aspects. While there will be huge crimes against it too. For all the participators of cloud computing environment, participators should prepare for that change. This present paper we have proposed a log-based model accession. The log based model can help to reduce the complications of forensic for non-repudiation of bearing on cloud. Nonetheless, it is totally not adequate for the other kinds of digital forensics. What matter makes worse is that, till now, there are no directions or standards for the cloud security. Many times, we modified the directions of conventional digital forensics to outfit for cloud computing environment separately.

REFERENCES


