Artifact Acquisition in Cloud: Will Garbage be Always Useful??

Leeba Merin Sam, Raj Kumar. T

Abstract— Cloud Computing is a promising technology and provides abundant economic opportunities. It is not a new technology but it was not accepted in the past decade. Now the scenario changed and in the present tech world, it is one of the best alternatives for many problems and hence widely deployed irrespective of the domain. Presently, the crime rate is increasing in a faster pace compared to some years ago. Cloud is also prone to much type of attacks and hence the deployment is seriously affected. This paper briefly gives an insight into forensic data acquisition in cloud.

Index Terms— acquisition, artifacts, cloud computing, forensics, investigation, logs, artifacts, threats.

1 INTRODUCTION

Cloud Computing is coming to the fore, what once viewed with much skepticism is now being perceived as a best alternative to increase productivity. It is considered as one of the prominent technology. The adoption of cloud varies from the academics to enterprises; small scale to large scale enterprises is now part of the cloud. Barack Obama's describe the use of cloud computing as one of the most important transformations his government will go through in the coming decade. The Cloud is a Fast-Evolving Technology, growing and evolving at a rate far quicker than expected. The global demand for cloud services will cross $100 Billion by next year. Presently, the SaaS (software-as-a-service) market is more popular and by 2018, the cloud will take up over 10 percent of the total enterprise IT expenditure. Cloud computing is defined by NIST[1] as a model which enables convenient, on demand network access to a shared pool of computing resources such as networks, servers, storage, applications etc that can be rapidly supplied and released with minimum management effort or interaction. Therefore the cloud model is composed of these five essential characteristics, three service models, and four deployment models.

The three service models are namely, SaaS – Software as a Service, IaaS- Infrastructure as a Service, and PaaS- Platform as a Service. The service models are defined based on the various services offered by the cloud providers. IaaS is the foundation layer of the cloud stack where we can manage the applications, data, operating system etc. The service provider manages our virtualization, servers, networking and storage. In PaaS we can manage our applications and data and the cloud vendor manages everything else.

SaaS is the final layer of the cloud services model. This service model enables us to run programs in the cloud where everything is managed by the cloud vendor, where the user has no control and just to use the available service facilitated by the provider.

The deployment model is defined based on how the pools of resources are shared and it provides a better way of planning. The various deployment models are Public, Private, Community and Hybrid. The Public cloud it is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage The Private is also known as internal cloud. The platform for cloud computing is implemented on a cloud-based secure environment which is under the governance of the IT department that belongs to the particular corporate. The Hybrid cloud is the combination of both public and private such that the advantages of both the deployment models are adopted neglecting the negatives of them. The Community cloud is a hosting in which the setup is mutually shared between many organizations that belong to a particular community, i.e. banks and trading firms.

Advantages of cloud computing

The wide adoption of cloud in all sectors of life is due to the advantages it has over the traditional models of computing. In an ideal world, cloud computing would free administrators from the hardware headaches such as scalability, availability…in a geographical sense, giving them time to get on with running their applications.

Cloud Adoption Reduces Costs- using the right type of cloud service results in a reduction of overall IT expenses. This is one of the major reasons for the steep increase in the adoption of this technology. Cost control and the convenience of working with data in the cloud is a key factor in driving it ahead

Unlimited Storage- Cloud provides unlimited storage and hence we are devoid of storage concern.

Backup and Recovery- Taking back-ups and restoring it is easy in cloud. This is easy compared to traditional methods of storage as cloud service providers are competent enough to handle all sort of information recovery.

Easy Access to Information- It is possible to access information in cloud, if there is an internet connection. This helps a lot in getting rid of time zone and geographic location issues.

Threats for Cloud

Utilizing the cloud provides organizations with many business benefits, not only benefits but there comes some threats also. Some of them are familiar traditional threats while others are unique to the cloud. Understanding the various threats related

to our data and services in the cloud we are better prepared to determine how best to secure them. Threat is defined as an entity that has likelihood to cause damage or danger."

Data Breaches: It is the number one security threat for cloud computing, which is the loss of confidentiality for data stored within a particular cloud instance. Such a threat is likely to exist even within an on-premise solution, or traditional outsourced solution.

Data Loss: unavailability of data stored within the cloud for the end customer.

Shared Technology Vulnerabilities: Resource sharing is the main benefit of cloud computing, but this result in a serious flaw as strong isolation is required. Otherwise vulnerability in one instance is affected by other instances also. The likelihood of this scenario is high in public and low in private and depends heavily on the cloud model used. The impact can either be loss of valuable data or reputation or service interruption.

2 Digital Forensics

Digital Forensics [4] is defined by NIST as the application of science to the acquisition and examination of data and while preservation, a strict chain of custody for the data [8] has to be followed.

Evidence is one of the crucial terms associated with digital investigation. Digital evidence is information stored or transmitted in machine readable form that can be submitted to court [10]. It can be found both on a computer hard drive or a mobile phone or a personal digital assistant (PDA) and among other places.

3 Cloud Forensics

Cloud forensics [5] is the applying digital forensics in cloud computing environment as a branch of network forensics. So, it is a combination of cloud computing and digital forensics. Cloud computing forensic science consists of application of forensic methods and derived and proven strategies to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

Cloud security involves two aspects. First off all protect cloud and all applications running on it from attack. Next is dealing with happened security events. Precaution is of major concern in cloud security. Criminals always try to thwart the security blocks to realize their intentions. Therefore a new battle has started between security department and the black hat hackers in digital world.

There are various dimensions composed in cloud forensics enumerated as technical, organizational and legal. The technical aspect deals with set of tools and procedures needed to carry out the forensic process in cloud computing environments while organizational is about the involving parties in forensic investigations ie, the cloud consumer and the CSP. When there is an outsourcing again done by CSP, there is a tendency for the scope of the investigation to widen. The Legal Dimension has several coincidences. The multi-jurisdiction and multi-tenancy challenges are considered as top level concerns among digital forensic experts.

4 Acquisition of Artifacts in Cloud

Digital investigation is an ongoing process. It goes on iteratively until the whole investigation gets completed. So this is not a linear process where the investigation goes from one step to the next. The examination and analysis of evidence at hand may lead to the identification of new cloud data. Investigation depends up on both the service and deployment model used in the environment. IaaS is more flexible to investigation compared to other service model. In SaaS, the only source of evidence is the application log provided by the provider. In case of account compromise, provider does not offer any possibility for customer to figure out which data and information has been compromised. In PaaS, the application is under the control of customer. The interaction of application and the dependencies [database, network etc] can be dictated.

Less data are left on the hard drive by the applications and therefore we should rely more on browser artifacts and RAM. Nowadays, there is a trend of increased RAM size and this implies that more data can be found from RAM. Live RAM captures is the best source for volatile artifacts. Many artifacts which cannot be located anywhere can be found in this volatile memory.

Pagefile.sys which is used as "virtual memory" and data is paged in and out of the file as needed. It is even found on systems with a large amount of RAM. Microsoft recommends keeping the pagefile enabled. Pagefile.sys provides volatile artifacts abundantly. Artifacts that are present in RAM only can make a way into this file.

Hiberfil.sys consists of complete image of RAM and system state which is used to restore system from hibernation. Artifacts from a historic point in time (the last time the system was hibernated) can be obtained. Unallocated space provides us with a great deal of deleted data including browser cache data.

During the installation of a cloud application, lot of changes takes place in registry; different keys and values are created like:
SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules. From the registry we can obtain, Install Location and Installed version. If the client is installed on the PC, we can find in RAM information about the sessions. It is possible to find user email, display name, server time (UNIX timestamp) file list and deleted file. Similar values can be obtained from Hiberfil.sys and Pagefile.sys. On uninstall, we can also recover information from registry keys about recent files, LNK files, Browser history and cache, thumbnails. Registry Point / Volume Shadow Copies, pagefile.sys and hiberfil.sys information can also be obtained. In Dropbox online access, it is possible to extract the username and password from the RAM analysis.

Log is another main source of evidence. Different types of log such as process logs, application logs and network logs are useful in computer forensics. But there are limitations in using logs in a cloud crime scenario. Many providers started providing logs to the customers.

Management plane is a solution provided by cloud providers from where the investigators can collect their data of interest particular to the case in their hand.

5 CHALLENGES IN ACQUISITION

Cloud revolutionized the world of technology. Now cloud became an indispensable part of our life. The technology has proven as a great asset to the firms in terms of both technical as well as economic. Yet cloud computing has not been developed so far in terms of forensics. The afore-mentioned methods are not suitable in one or other way.

There exists trust as well as legal issues in cloud forensics. Logs cannot be trusted as they are provided by CSP. Similar is the case of acquisition from management plane. Logs have the issues of volatility and decentralization too. Very few amount of information can be obtained from hard drives. Hence we rely on RAM which is volatile and cannot be obtained always. A culprit who is intended to commit and hide the crime can easily delete all these source of evidence collection.

6 CONCLUSION

The usage of cloud computing increased in the past couple of years. Cloud crimes are also increasing in a faster rate. This paper goes through the various threats to cloud and also the various artifact retrieval schemes. The present approaches are not apt. There should be better methods of artifacts collection. Also there is a need of authentication mechanism that can equip investigators with trustworthy evidences.

REFERENCES

1) 4 Types of Cloud Computing Deployment Model You Need to Know www.ibm.com/developerworks/community/blogs
2) [2]. http://www.nist.gov/oles/forensics/digital_evidence.cfm
3) [3].advantages and disadvantages of cloud computing
4) [4]. https://en.wikipedia.org/wiki/Digital_evidence
5) http://www.examiner.com/article/advantages-and-disadvantages-of-cloud-computing
6) [5].**David Wilson** Legal issues with cloud Forensics http://www.forensicmag.com/articles/2015/05/legal-issues-cloud-forensics
7) [6]. Cloud Times The Basics of Cloud Forensics http://cloudtimes.org/
8) [7].Darren Quick, Kim-Kwang Raymond Choo(2013) "Cloud Storage forensics frame work", Digital Investigation: The International Journal of Digital Forensics & Incident Response, 266-277
9) [8].George Grispos, Tim Storer, William Bradley(2012)"Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics"
10) [9].Shams Zawoad Ragib Hasan (2013) "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems" arXiv:1302.6312v1 [cs.DC]
11) [10].Challenges of Cloud forensics: A survey of the missing capabilities http://ercim-news.ercim.eu/en90/special/challenges-of-cloud-forensics-a-survey-of-the-missing-capabilities
12) [11].Overview of cloud platforms and appliances Obscured by Clouds Article from ADMIN 02/2010 By Jörg Fritsch

Leeba Merin Sam is currently pursuing M.Tech from College of engineering, Kalloopara affiliated to Cochin University of Science and Technology, Kerala, India, leebamsam@gmail.com. The areas of interest include virtualization forensics and network security.

Raj Kumar T graduated the degree of Master of Technology from National institute of Technology Karnataka Surathkal and is presently working as Assistant Professor in Computer Science and Engineering at College of Engineering Kallooppara, Kerala. The area of interested includes cloud computing, data mining, networks and virtualization