Article can be accessed online at http://www.publishingindia.com

About Cloud Forensics: Challenges and Solutions

Vaithianathan Geetha*

Abstract

Cloud computing is gaining wide popularity due to low infrastructure cost and high resource utilization. Cloud can be private or public. Users can store their data and avail cloud sessions on pay-per-use basis. This multi-tenancy support can lead to several problems. Cloud forensics is a cross discipline of cloud computing and digital forensics. It ensures to find out the culprit when there is a security breach. Several techniques are proposed to secure user data and provide legally acceptable evidences in case of cyber crime. This chapter aims at discussing the issues and challenges of cloud forensics and the currently available solutions. Logs are widely accepted as legal evidence of how fraud was perpetrated. Creation and maintenance of logs also poses a number of challenges. This chapter also aims at exploring these challenges and solutions for managing logs.

Keywords: Cloud Security, Cloud Service Providers, Cloud Users, Service Level Agreement (SLA), Digital Forensics, Cloud Forensics Phases, Forensic Readiness, Log Formats, Log Architecture, Log Security, Log Database

INTRODUCTION

Cloud computing has turned out to be a profitable solution to business world and IT industry. Small and medium enterprises (SME) shift their business process to cloud to reduce their infrastructure investment and maintenance costs. The data center owners rent out their data centers comprising of seamless computing power, huge storage and unlimited bandwidth to make more money. The pricing model is pay-per-use and hence very attractive to business owners.

However the cloud offers several benefits to its users, it is vulnerable to various security attacks from the outside world. The reasons for these vulnerabilities are due to the features the attracted the users. Several research contributions are available in the literature to tighten the cloud security. Even then, the public cloud environment is not immune to security attacks. Cloud forensics deals with investigation of cyber and digital crimes in cloud and collection of evidences to be produced in the court of law. Therefore, cloud forensics involves legal, technical and management aspects of cloud.

This chapter discusses about the various aspects of cloud forensics and the importance of logs as acceptable legal evidence. Cloud forensics is an emerging field of research. Researchers are exploring the various issues of cloud forensics such as

- Can digital forensics be extended to cloud?
- What are the technical challenges in cloud forensics?
- How to prepare cloud to be forensic friendly?
- What is the methodical way of conducting cloud forensics?
- Whether cloud forensic techniques are common for all layers of cloud?
- How to protect the evidences collected?
- What are the standards/organizations involved in cloud forensics? What is their role?
- What are the popular cloud forensic tools?

It is universally accepted that log is the best evidence for proving cloud crime. Therefore, there is a shift of focus

* Department of Information Technology, Pondicherry Engineering College, Puducherry, India. E-mail: vgeetha@pec.edu

from cloud data security to log security as logs can also be compromised. This chapter also aims to provide insight into the following aspects of logs.

- Various log formats
- Log management policies
- Log security techniques

The forensic solutions currently available are explored. The chapter is concluded by highlighting the major findings and the areas where focus is required.

Background

Cloud computing is a major transformation in the way IT companies are utilizing their resources. The IT companies provide hardware and software services to small and medium business owners over the internet. They let out their data centers to provide these services. They use virtualization technologies and Service Oriented Architecture (SOA) to provide seamless support. There are several advantages in cloud computing for cloud providers and cloud users. Cloud providers enjoy high resource utilization and better returns for their investment in infrastructure as they are renting their resources when they do not use it for their own purpose.

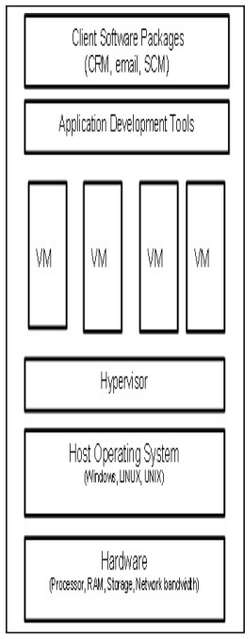
Cloud users need not make an investment in hardware resources. They need not know about or maintain computer resources. They also do not have to engage any computer professionals to manage hardware and software upgradation, resolve hang-ups, or system maintenance. The cloud providers charge them on pay-per-use basis.

Cloud Architecture

According to NIST definition of (Mell P. and Grance T. 2009), *Cloud model is composed of five essential characteristics, i.e., On-Demand Self Service, broad network access, resource pooling, rapid elasticity and measured service, three service models i.e., SaaS, PaaS and IaaS and four deployment models i.e., Private cloud, Community cloud, Public cloud and Hybrid cloud.*

Figure 1 shows the basic architecture of cloud. The cloud supports SPI (Software, Platform and Infrastructure) model. It supports a layered architecture with Infrastructure as a Service (IaaS) as the lowest layer in which the hardware resources like processors, RAM, storage and network bandwidth are let out. The users can hire them in bundle offer or individually. In Platform as a Service (PaaS) layer, the users can also hire development environment like OS, application development tools along with hardware resources. The highest layer, Software as a Service (SaaS) provides client software packages like CRM, email and SCM etc. along with the environment. All the users need to avail these services are cheap desktops, mobile phones, PDA or tablet etc. Service Level Agreement (SLA) signed by the service providers and users binds the services. Clouds are classified as Private clouds (internal), Public clouds (external), Community clouds, Hybrid clouds and a new type of cloud called Virtual private clouds. The private cloud is closed and restricted to an organization. Public cloud is open to all and managed by a cloud provider. Community cloud is a collection of private clouds with common interest. Hybrid cloud is a combination of two or more cloud models. Virtual private clouds are created inside public clouds to provide private communication using VPN connectivity.

Figure 1. Cloud Architecture



The major characteristics of cloud are

1. Resource abstraction (through virtualization)
2. On-Demand elastic resource provisioning
3. Multi-tenancy support
4. Multi-jurisdiction support
5. Location Independence
6. Service bound by Service Level Agreement (SLA) contract.

(Skok, M. J., 2014) has done a survey on business growth of cloud. SaaS adoption has increased from 11% to 74%. Cloud has become integral to 45% of businesses who are running their company from cloud. Recent International Data Corporation (IDC, 2013) cloud research has predicted that $107 billion will be spent on public IT cloud services. Over the 2013-2017 prediction periods, more companies will build out the infrastructure to deliver cloud services and Compound Annual Growth Rate (CAGR) will be 23.5%.

Broad View of Issues in Cloud Computing

The well claimed features and merits of cloud computing are also viewed as issues by the experts. The major issues highlighted are

- System downtime/business interruptions.
- Vendor lock-in.
- Lack of legal clauses in SLA.
- Loss of control due to locational transparency.
- Lack of data security.
- Energy efficiency in cloud(Green Cloud)

All the commercial public clouds claim that they provide 24X7 support claiming 0% downtime, which is not always true in reality. They fail to provide services sometime because of system failure or non- availability of resources. Once the users get familiar to a particular cloud, they will come for repeat sessions to continue the business transactions. Though penalty is included in Service Level Agreement for not providing the service or not providing it on time, the lack of assurance that the cloud is always available to provide services reduces cloud's reliability. Vendor lock-in prevents the migration of users from one cloud to another cloud, as they are dependent on specific tools or environment to continue with their earlier sessions. These dependencies on a particular tool or environment still exist even after enforcing standards and provide support for interoperability. The datacenters are spread across the globe. A user request may be placed in one or more of these data centers and the exact location of user session are unpredictable. In case of dispute, this multi-jurisdiction uncertainty makes it difficult for the cloud users to take legal action against the cloud provider. Further, this location independence makes it difficult for the user to monitor and control his session. Recent researches focus on power conservation and explore solutions for making green clouds.

Security Issues in Cloud

Among all the above-mentioned issues, security is viewed as the topmost concern. In (CompTIA, 2012) CompTIA's 9th Annual Information Security Trends Report, the top cloud security concerns are listed.

- Exposure or loss of data during file transfers to the cloud.
- Concerns over encryption of data (either transactional or at rest)
- Physical security at the data centers.
- Shared technology vulnerabilities in a multi-tenant environment.
- Malicious activity from privileged insiders.
- Identifying/authenticating users.
- Difficulty in assessing and comparing security of cloud service providers.
- Complying with legal/regulatory requirements.
- Ability to conduct audits, review cloud security logs etc.
- Insecure APIs.

The ideal cloud security mechanisms are expected to provide support on the following aspects:

- Define role, actions and privileges of users, administrators, management personnel and security personnel.
- Isolate the user data and session from co-users.
- Preserve the user confidentiality.
- Identify inside threats, risks and vulnerabilities. Define company policy against these insecurities.
- Define the consequences of violation.
- Track the policy compliance and provide evidence for legal action in case of violation.

(Boampong and Luay, 2012) summarizes the strategies to attend the above aspects. The security measures are summarized as policies, software security and physical security. Policies are suggested for good governance of employees, build confidence level of the users and standards for system portability. Software security suggests

identification of best security practices and applies them iteratively. Physical security suggests measures to be taken against natural disasters and thefts. Backups, providing tight physical security for server locations and firewall solutions are suggested as solutions. Though there are several security solutions proposed for cloud, it is still vulnerable to attacks. Traditional security mechanisms such as identity, authentication and authorization are not effective for clouds. (Li W, Ping L, 2009).

Table 1 lists the possible threats, related vulnerabilities and suggested counter measures in cloud. Cloud is used as a medium or object for cyber crime. Several cases have been registered against storing of banned content like child pornography, contraband images/video etc in cloud. Dark clouds exist which threatens the operation and safety of other cloud. Apart from this, internal threats also exist which threaten the cloud security as mentioned above.

Cloud forensics is needed to investigate the digital crime in which cloud is a victim, instrument or medium. It proposes a methodical way of suspecting a crime, collecting digital evidences from cloud, preserving the evidences and producing them in the court of law. (Stephenson.P, 2003) has suggested six phases for conducting computer forensics investigations as given below:

Identification: Determine items, components and data possibly associated with the allegation or incident.

Preservation: Ensure evidence integrity or state.

Collection: Extract or harvest individual data items or groupings

Examination: Scrutinize data items and their characteristics

Analysis: Fuse, correlate and assimilate material to produce reasoned conclusions

Presentation: Report facts in an organized, clear, concise and objective manner.

The above phases are adopted for cloud forensics also.

Issues in Cloud Forensics and Log Management

Need for Cloud Forensics

(Ruan K., Carthy J.,Kechadi T., Crosbie M. 2011) have defined *Cloud Forensics as the application of digital forensics in cloud computing as a subset of network forensics. Cloud forensics has three dimensions namely organizational, legal and technical dimensions.* Technical

Table 1: Relationships between Threats, Vulnerabilities and Countermeasures (Hazhizume.K., Rosado D.G., Fernandez-Medina E. and Fernandez E.B, 2013)

Threats	*Due to Vulnerabilities*	*Counter Measures*	*Layer*
Account or Service hijacking	Insecure APIs and Interfaces.	Identity and Access Management Guidance	SPI
Data scavenging	Data related Vulnerabilities	Specify destruction strategies on SLAs	SPI
Data leakage	Data related Vulnerabilities Vulnerabilities in VM, VM images and Virtual networks	FRS techniques, Digital signatures, Encryption, Homomorphic encryption	SPI
Denial of Service	Insecure APIs and Interfaces. Unlimited allocation of resources	Cloud Providers can force policies to offer limited computational resources.	SPI
Customer data manipulation	Insecure APIs and Interfaces	Web application scanners	S
VM escape	Vulnerabilities in Hypervisors	HyperSafe	I
VM hopping	Vulnerabilities in VM and VM images	TCCP AND TVDc	I
Malicious VM creation	Vulnerabilities in VM images	Mirage	I
Insecure VM migration	Vulnerabilities in VM	PALM, TCCP,VNSS	I
Sniffing/Spoofing virtual networks	Vulnerabilities in Virtual networks	Virtual network framework based on Xen network modes	I

Table 2: Challenges of Cloud Forensics Due to Cloud Characteristics (Dykstra J. and Sherman A.T, 2011)

Cloud Characteristic	*Forensic Challenge*
Location independence	Discovery of Computational Structure, Legal jurisdiction
Self-provisioned and elastic	Evidence Preservation, Data integrity
Data Reliability(replication)	Chain of custody, Evidence integrity
Multi-tenancy	Data attribution, Chain of Custody
General, abstract data structures	Best evidence Presentation / Visualization of evidence
Sustainable business	Cooperation, logging, data location & preservation

dimension involves developing tools and methods to carry out the forensic process in cloud environment. Tools are needed for evidence acquisition, data recovery, evidence examination, evidence analysis and evidence segregation. In organizational dimension, the hierarchy of organizational staff, their association and role in cloud forensics are defined. Apart from internal structure of a cloud, its association with other clouds is also explored. In legal dimensions, the regulation policies related to multi-jurisdiction and multi-tenancy, amendment in SLA for forensic investigations are recommended. They have also listed the scenarios where cloud forensics can be useful.

1. The obvious use of cloud forensics is to investigate on cloud crime.
2. It can also be used for trouble shooting operational issues in cloud environments.
3. It is useful in framing proper regulatory compliance for cloud operations.
4. For log monitoring.
5. For data recovery lost due to accidental damage or attacks.

Though cloud forensics can have multi-purposes, it is still in infancy. Researchers identify several issues and propose solutions. (Dykstra J. and Sherman A.T, 2011) have listed the forensic challenges due to the characteristics of cloud computing as given in table 2.

(Reilly D., Wren C. and Berry T., 2011) have listed the features of Cloud computing that is favorable to conduct forensics investigations as summarized below:

1. Centralized data for easy access of crime details.
2. Immense computational power and huge data storage to store and process digital evidences.
3. In built security mechanism to secure digital evidence.
4. Support for effective management of logs.
5. Virtualization supports snapshot facility to take an image of RAM and Hard disk and virtual introspection for monitoring VMs.

Features of Cloud computing that are not favorable for forensic investigations are also listed as given below: (Reilly,2011)

1. As the physical location of cloud data is unknown, evidence search and seizure procedures are impractical.
2. Maintenance of chain of custody is also very difficult to track.
3. There is a general loss of control for investigation due to remote data centers.
4. Lack of cloud forensic tool to support in cloud investigations.

Technical Challenges in Cloud Forensics

The technical challenges to be addressed for effective conduct of cloud forensic investigations are listed in this subsection. This is based on the phases involved in conducting cloud forensics investigations. The cloud forensic investigations prove to be difficult mostly because of the inherent features of cloud architecture. Researchers have analyzed the challenges faced in collecting digital evidence and preserving before submitting in the court of law. The evidence data can be at rest (Stored in storage device), in transit (sent across a network) or in process (executed in a processor). This means that each of them require different type of tool to capture the data. Further based on the cloud layer the evidence may be present in the RAM, storage of server, in the VM or a part of the client application. Further the data can be volatile or non-volatile. Registry entries, processes, temporary internet files are examples of volatile data. Then there is

the issue of capturing the data before the server or VM that is hosting it is shut down or rebooted. It is observed that the evidence can be collected relatively easily at IaaS layer that is of lower abstraction than that of SaaS which is of higher abstraction. (Ruan K., Carthy J., Kechadi T., Crosbie M., 2011) say that the SaaS users are not aware of the location of forensic data, log files and metadata to monitor their sessions. There is a universal claim that the cloud service providers intentionally hide the details from the users. The distribution of datacenters across the globe makes the data collection more difficult. The investigators have to get a warrant for cloud data access from sites with different jurisdictions and laws. Getting a warrant is usually time consuming and costly and lead to loss of data (Simou. S., Kalloniatis. C., Kavakli. E., Gritzalis. S., 2014). Further, the investigators have to rely on CSP for investigation. The CSPs may not be willing to extend the support due to the fear that it may be used against them. Further there may be availing services of other CSPs. Then all the parties are to be involved. They also state the problems in preserving the data without compromise from the CSP. Proper security mechanisms are needed to protect the evidence. Further timelines are needed to maintain the chain of event across different time zones. It is also important to note that co-users of a session under investigation should not be affected in any way by the investigation procedures.

Organizational Challenges in Cloud Forensics

The cloud providers have no specific employees to handle cloud forensics. Cloud is vulnerable to risks, attacks and scandals. Apart from managing globally distributed data centers, Cloud should have dedicated personnel to handle each of these problems for better operation. Internal security professionals are needed to protect cloud from various types of attacks. Incident handlers are needed to handle complaints on mis-management of cloud like data leakage, data loss, storing objectionable content, internal staff threats etc.

It is also essential for the CSP to build goodwill with the internal staff and users to avoid these problems.

Legal Challenges in Cloud Forensics

(Eecke P.V., 2015) has listed a number of legal issues to be addressed due to the multi-jurisdiction and multi-tenancy nature of cloud. The cloud providers are also held responsible for hosting the illegal data. Hence a distinction is needed to find who is responsible. Further easy registration service systems allow users to create multiple, proxy accounts that may be used for malicious purpose. At present, issues are raised on storing of objectionable content. However there is no notice on execution of harmful processes. On the other side, CSPs maintain the overall control and include clauses to terminate services without further clarification.

Amendments Needed in SLA

The terms and conditions of a cloud service are bound by SLA signed by the cloud user and provider. Usually SLA contains the details of the service and delivery conditions. Researchers have identified the limitations of clauses in terms of security and cloud forensics. The SLA clauses must protect the CSP from legal action due to malicious activity of a cloud user. The clauses should also grant CSP rights to remove/block the objectionable content. (Ruan K., Carthy J.,Kechadi T., Crosbie M., 2011) say that there are no terms and conditions in Sla regarding the segregation of duties between CSP and user. Terms of use to enable general forensic readiness in the cloud is missing. Providers do not provide interfaces to gather forensic data as they have no control over the location of data.

Conclusion

The challenges and available solutions for cloud forensic investigations and log management are explored in this paper. It can also be inferred that cloud forensics is more complex than computer forensics because of its features such as location independence, elastic resource provision, loss of control etc. Further new forensic tools are also to be developed for effective cloud forensic investigations. Focus is also required in devising new international law standards, amending SLA to incorporate forensic clauses. Regulations are required for secured access of cloud services. New mechanisms are needed for safe custody of logs until produced in the court of law.

References

Boampong, P. A., & Wahsheh, L. A. (2012). *Different facets of security in the cloud*. In Proceedings of the

15th Communications and Networking Simulation Symposium, (5, pp. 5.1-5.7), Society for Computer Simulation International, San Diego, CA, USA.

Comp TIA. (2012). *9th Annual Information Security Trends*. Retrieved from https://www.comptia.org/resources/9th-annual-information-security-trends

Dykstra, J., & Sherman, A. T. (2011). Understanding issues in cloud Forensics: Two *Hypothetical Case Studies*. *Journal of Network Forensics*, 3(1), 19-31.

Eecke, P. V. (2015). *Cloud Computing Legal issues*. Retrieved from http://www.isaca.org/Groups/ProfessionalEnglish/cloudcomputing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf

Hazhizume, K., Rosado, D. G., Fernandez-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(5), 1-13.

IDC. (2013). *Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast*. Retrieved from http://www.idc.com/get.doc.jsp?containerId=242464 .

Hashizume, K., Rosado, D. G., Medina, E. F., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *International Journal of Internet Services and Applications,* 4(5), 1-13.

Li, W., & Ping, L. (2009). *Trust model to enhance security and interoperability of cloud environment*. In proceedings of the 1st International Conference on Cloud Computing, Springer Berlin Heidelberg, Berlin, China, (pp. 69-79).

Mell, P., & Grance, T. (2009). *The NIST Definition of Cloud Computing Version 15 NIST*.

Reilly, D., Wren, C., & Berry, T. (2011). Cloud Computing: Pros and Cons for Computer forensic Investigations. *International Journal of Multimedia and Image Processing, Infonomics Society*, 1(1), 26-34.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). *Cloud forensics: An Overview*. Advances in Digital forensics, 7, 35-49.

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud Forensics: Identifying the major issues and challenges*, In Proceedings of* 26th International Conference, CAiSE, Thessaloniki, Greece, June 16-20.

Skok, M. J., (2014). *2014 Future of Cloud Computing 4th Annual Survey Results* http://mjskok.com/resource/2014-future-cloud-computing-4th-annual-survey-results Retrieved in June 2015.

Stephenson, P. (2003). *A comprehensive approach to digital incident investigation*. Information Security Technical Report, 8(2), 42-52.

Key Terms and Definitions

Cloud Crime: A crime in which cloud is instrument, victim or medium.

Cloud Forensics: Investigation procedure for finding the hidden truth about a cloud crime.

Dark Cloud: A cloud that is used for the malicious objective of attacking other clouds.

Digital Evidence: Data represented as files, documents, audio, video or packets that is stored or transmitted as a proof for digital crime.

Live Forensics: Collection of evidence from a computing device's memory, processes, secondary storage and network connections when the power is ON.

Dead Forensics: Examination of a computing device when its power is OFF.

Chain of Custody: Keep track of the custody of crime evidence by various phases of forensic investigations starting from identification till it is produced in the court.