Volume 6, Issue 1 (XXXIV)
January - March 2019

ISSN 2394 - 7780

ज्ञान-विज्ञान विमुक्तये
UGC
University Grants Commission
Journal No.: 63571

International Journal of

Advance and Innovative Research

(Conference Special)

Indian Academicians and Researchers Association
www.iaraedu.com

NATIONAL CONFERENCE ON CYBER INTELLIGENCE, CYBER FORENSICS & INVESTIGATION (CICFI 2018 - 19)

ORGANIZED BY

Department of Computer Science and Information Technology

Jnan Vikas Mandal's Mehta Degree College

Navi Mumbai

&

Hexa Digital Forensic Corporation

22nd & 23rd March, 2019

In Association with

Knowledge Partners

Publication Partner

Indian Academicians and Researcher's Association

Journal - 63571

UGC Journal Details

Name of the Journal :	International Journal of Advance & Innovative Research
ISSN Number :	
e-ISSN Number :	23947780
Source:	UNIV
Subject:	Multidisciplinary
Publisher:	Indian Academicians and Researchers Association
Country of Publication:	India
Broad Subject Category:	Multidisciplinary

International Journal of Advance and Innovative Research

Volume 6, Issue 1 (XXXIV) : January – March 2019

CONTENTS

Research Papers

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

CLOUD FORENSIC INVESTIGATION: NEW INVESTIGATION TREND

Shweta Pawar
Assistant Professor, M V Mandali's Colleges of Commerce & Science, Mogaveera Bhavan, MVM Educational Campus Road

ABSTRACT
The Cloud Computing is one of the most evolutionary technologies. Cloud environment include the service provider and customers of cloud services. Without distinct forensic capabilities, they are unable to ensure the robustness and suitability of their services to support investigations of any criminal activity. In this paper, the new area in forensic investigation, its challenges and opportunities are going to examine.

Keywords: Cloud Forensics, Cloud Computing, Digital Forensic Investigation

I. INTRODUCTION

Cloud computing is radically changing the way Information services were introduced long before. Cloud computing platform increases the scale of the computer systems in both hardware and software wise. The definition of digital forensics and cloud computing from NIST are:

Digital forensics is used for the identification, collection, examination, and analysis of data and preserving the reliability of the information and maintaining a strict chain of protection for the data. [1]

Cloud computing could be a model for enabling convenient, on-demand network access the configurable resources (e.g. network, servers, storage, various applications, and services) that can be speedily provisioned and free with minimum management effort or service supplier interaction. Cloud computing has 5main characteristics, i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. It has 3 service models, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). And it has 4 deployment models, i.e., private cloud, community cloud, public cloud and hybrid cloud. [2]

The data is held and managed remotely via cloud software, platform or infrastructure by authenticating or authorized users. Despite many advantages, cloud computing involves greater exposure to various security threats and privacy breaches.

II. DIMENSIONS OF CLOUD FORENSIC

The default settings for cloud forensics are multiple jurisdictions and multi-tenancy, which create additional legal challenges. The interactions between Cloud Service Providers (CSP[1]) and Customers, by resource sharing and collaboration between International Law Enforcement agencies, are most important in cloud forensic investigation. In order to examine the domain of cloud forensics more comprehensively, it can be divided into three dimensions, the technical, organizational and legal dimensions.

A. Technical Dimension

The technical dimension encloses the procedure and tools that are needed to perform forensic investigation in the cloud computing environment. These include data collection, evidence segregation, virtualized environments and proactive measures.

Data collection is the process of identifying, collecting, cataloguing and obtaining the forensic data. The forensic data includes customer-side artifacts that conferred on customer's premises and provider-side artifacts that are located in the provider's infrastructure. To collect forensic database on the specific model of data in place, various procedures and tools are used. The collection method ought to preserve the integrity of information. It should not breach any law or any rules and regulations in the jurisdictions where data is collected, or compromise the confidentiality of other occupants that share the resources.

Another essential feature of cloud computing is resource management [3]. Multi-tenant environments reduce IT costs through resource sharing. However, the method of segregating evidence within the cloud needs compartmentalization [4].

[1] Cloud Service Providers (CSP) are those service providers which provides various services of Cloud such as IAAS, PAAS and SAAS.

ISSN 2394 - 7780

B. Organizational Dimension

A cloud forensic investigation includes at least two entities: the CSP and the cloud customer. However, the scope of the investigation can increase when a CSP outsources services to the other parties. Figure 1 show the various entities involved in a cloud forensic investigation.

Organizational policies or Service Level Agreement (SLA) facilitate communication and collaboration in forensic activities. In addition to enforcement, the chain of CSPs must communicate and collaborate with third parties and academia. Third parties will assist with auditing and compliance whereas academia will offer the technical experience that would enhance the potency and effectiveness of investigations.

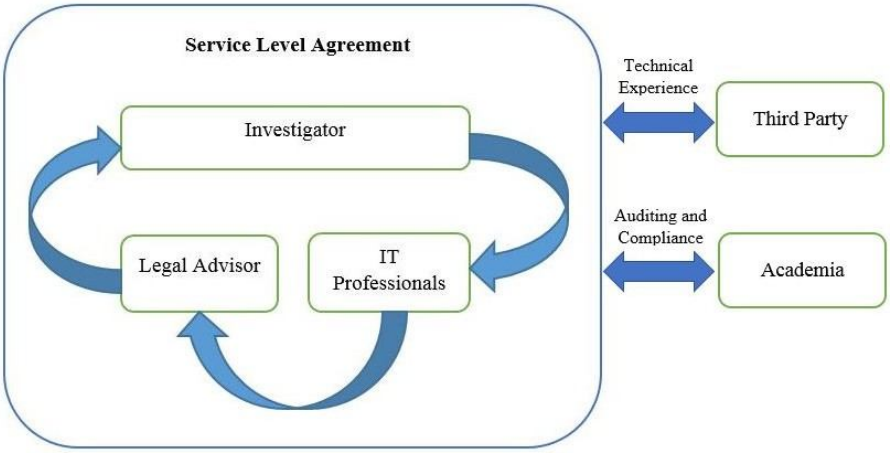

Fig-1: Entities in Cloud Forensic Investigation

To establish a cloud forensic process, each cloud entity must provide provider-customer collaboration and external assistance that fulfill the following roles:

- **Investigators**: Investigators examine allegations of misconduct and working with external law enforcement agencies. They must have enough experience to perform investigations of their own assets in addition as act with alternative parties in rhetorical investigations.
- **IT Professionals**: IT professionals include a system, network and security administrators, ethical hackers, cloud security architects, and technical and support staff. They provide skilled information in support of investigations, assist investigators in accessing crime scenes, and should perform data collection on behalf of investigators.
- **Legal Advisers**: Legal advisers are familiar with multi-jurisdictional and multi-tenancy issues in the cloud. They make sure that forensic activities don't violate rules and regulations, and maintain the confidentiality of different tenants that share the resources. SLAs must clarify the procedures that are followed in forensic investigations.

  Internal legal advisers should be involved in drafting the SLAs to cover all the jurisdictions in which a CSP operates. Internal legal advisers are also responsible for communicating and collaborating with external law enforcement agencies during the course of forensic investigations.

C. Legal Dimension

Traditional digital forensic professionals establish multi-jurisdictional and multi-tenancy challenges as prime legal considerations [5] [6]. Performing forensics in the cloud exacerbates these challenges. The legal dimension of cloud forensics needs the development of rules and agreements to make sure that forensic activities don't breach laws and rules within the jurisdictions wherever the information resides. Also, the confidentiality of alternative tenants that share a similar infrastructure ought to be preserved. SLAs define the terms of use between a CSP and its customers.

The following terms regarding forensic investigations should be included in SLAs:

(i) The services provided, techniques supported and access granted by the CSP to customers during forensic investigations;

(ii) Trust boundaries, roles and responsibilities between the CSP and customers concerning forensic investigations; and

ISSN 2394 - 7780

(iii) The method for conducting investigations in multi-jurisdictional environments while not violating the applicable laws, rules, and customer confidentiality and privacy policies.

III. CHALLENGES

Based on abovementioned dimensions of Cloud Forensic there may be following challenges can occur during the investigation:

A. Data Collection

In every combination of the cloud service model and deployment model, the cloud customer faces the challenge of decreased access to forensic data. Access to forensic data varies significantly based on the cloud model that's implemented [7].

Decreased access to forensic data means cloud customers typically have very little or no control or perhaps knowledge of the physical locations of their information. In fact, they'll solely be able to specify location at a high level of abstraction, typically as an object or container. CSPs advisedly hide information locations from customers to facilitate data movement and replication.

B. Evidence Segregation

In the cloud, different instances running on an individual physical machine are isolated from one another via virtualization. The neighbours of an instance have no more access to the instance than any other host on the Internet. Neighbours behave as if they are on separate hosts. Customer instances don't have any access to raw disk devices; instead, they access virtualized disks.

At the physical level, system audit logs of shared resources collect data from multiple tenants. Technologies used for provisioning and de-provisioning resources are perpetually being improved [4].

It is a challenge for CSPs and enforcement agencies to segregate resources throughout investigations without breaching the confidentiality of alternative tenants that share the infrastructure.

C. Virtualized Environment

Cloud computing provides information and computational redundancy by replicating and distributing resources. A hypervisor monitored and provisioned instances of servers. Hypervisors are main targets for cyber-attack, however, there's a lack of policies, procedures and techniques for forensic investigations of hypervisors.

Data mirroring over multiple machines in several jurisdictions and also the lack of transparent, real-time data concerning information locations introduces difficulties in forensic investigations. Investigators could unwittingly violate rules and regulations as a result of they do not have clear data concerning information storage jurisdictions [8].

D. Service Level Agreement

Current SLAs omit important terms regarding forensic investigations. This is because of low customer awareness, restricted CSP transparency and therefore the lack of international regulation. Most cloud customers are unaware of the problems that will arise in an exceedingly cloud forensic investigation and their significance.

IV. OPPORTUNITIES

Despite many challenges facing during Cloud Forensics, there are many opportunities that can support the forensic investigation.

A. Cost Effectiveness

Security and forensic services may be more cost-effective once enforced on a large scale. Cloud computing is engaging with small and medium enterprises as a result of it reduces IT costs. Enterprises that cannot afford dedicated internal or external forensic capabilities could also be ready to take advantage of low-cost cloud forensic services.

B. Robustness

Some technologies facilitate to improve the general hardiness of cloud forensics. IaaS offerings support on-demand cloning of virtual machines. As a result, within the event of a suspected security breach, a client will take an image of a live virtual machine for offline rhetorical analysis, which ends up in less downtime. Also, multiple image clones can speed up the analysis by simultaneously performing investigation tasks. This enhances the analysis of security incidents and will increase the likelihood of following attackers and patching weaknesses.

ISSN 2394 - 7780

C. Scalability

Cloud computing provides unlimited pay-per-use storage, permitting comprehensive logging without compromising performance. It additionally increases the potency of categorization, searching and query in globs. Cloud instances can be scaled as needed based on the logging load.

V. CONCLUSION

The traditional forensic process of investigation cannot applicable with cloud technology. The cloud exacerbates several technological, structure and legal challenges. Several of those challenges, like information replication, location transparency and multi-tenancy, are distinctive to cloud forensics. Opportunities and Challenges of cloud forensics were discussed in order to overcome the difficulties in the forensic investigation process in cloud computing. Nevertheless, cloud forensics brings unique opportunities which will considerably advance the effectiveness and speed of forensic investigations.

VI. REFERENCES

1. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," August 2006, NIST SP800-86 Notes.
2. P. Melland T. Grance "Effectively and Securely Using the Cloud Computing Paradigm,"2009, NIST.
3. Keyun Ruan, Centre for Cybercrime Investigation, Prof. Joe Carthy, Centre for Cybercrime Investigation, Prof. Tahar Kechadi, Centre for Cybercrime Investigation, and Mark Crosbie, "Cloud forensics: An overview." [Online]. Available: https: //www .researchgate .net /profile /Tahar_Kechadi/publication/ 229021339_Cloud_ forensics_An_overview/links/02bfe50f55377829e3000000/Cloud-forensics-An-overview.pdf
4. https://www.infosecinstitute.com/career-profiles/computer-forensics-investigator/
5. R. Broadhurst, "Developments within the international enforcement of cyber crime," Policing: International Journal of Police methods and Management, vol. Vol 29(2), pp. 408–433, 2006. [Online]. Available: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=2089650
6. S. Liles, M. Rogers, and M. Hoebich, "A Survey of the Legal Issues Facing Digital Forensic Experts," in IFIP International Conference on Digital Forensics, vol. Vol V. Digital Forensics 2009: Advances in Digital Forensics V, 2009,pp. 267–276.[Online]. Available: https:// link. springer.com /chapter /10.1007 /978-3-642-04155-6_20
7. "Amazon, AWS Security Center, Washington." [Online]. Available: https://aws.amazon.com/security/
8. "Cloud Computing Risk Assessment," Nov 2009. [Online]. Available: https://www.enisa.europa.eu/ publications/cloud- computing-risk-assessment
9. https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations
10. Cloud Security Alliance [CSA] 2009 Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
11. https://www.7safe.com/digital-investigation-services/digital-forensics-investigations
12. https://www.csoonline.com/article/2120792/what-to-bring-on-a-computer-forensics-investigation.html
13. http://www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf
14. Birk D., "Technical Challenges of Forensic Investigations in Cloud Computing Environments", 2011: http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf
15. https://www.prodaft.com/resources/articles/why-cyber-intelligence-is-necessary/
16. https://cyberintelligence.my/
17. https://www.bankinfosecurity.com/blogs/cyber-intelligence-what-exactly-it-p-1061
18. https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html
19. Burke W., Baving R., "Cyber Forensics in the Cloud: Challenges and Best Practice", Sequirt CSi BV, 2011.
20. http://www.hackerhalted.com/Portals/3/Docs/Presentation%20Slides/Cyber-Forensic-in-The-Cloud-day3-Wayne-Burke.pdf