International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Comparing Forensic Analysis Methods: A Roadmap to Cost-Effective Forensic Investigation

Ms. Pooja Gupta

Assistant Professor, Uttaranchal Institute of Management, Uttaranchal University, Dehradun, Uttrakhand, India

poojagupta010@gmail.com

***Abstract*— Cloud computing is a powerful and cost effective computing but it lacks in security and forensics. Many factors complicate the digital forensics process in cloud. Digital forensics investigators are facing new challenges in obtaining evidence because data is not on a single computer, Distributing computing implies that evidence may exist in and reflect activities on many computers. In fact, the data may be stored in multiple physical locations across the globe. Further rapid self-creation and destruction of cloud resources can be an add-on challenge for the investigators. Therefore, in this paper, we highlight the cloud forensics challenges in collecting evidence and compares different forensics analysis methods for the purpose of maximizing the environment's capability of collecting evidences and minimizing the cost of a forensic investigation.**

Keywords: Digital forensics; Cloud Computing; Digital Evidence; security issue, Digital Forensics Readiness.

I. INTRODUCTION

Data is now more accessible and timely available using cloud computing, but the same technologies that make it readily available – on-demand provisioning and virtual environments – also can obscure it. Data in the cloud is stored in data center and a data center might have hundreds of servers hosting thousands of virtual machines being used in sequence by thousands of customers, and data can be replicated across multiple sites in different countries across the globe. The cloud exacerbates many technological, organizational and legal challenges already faced by digital forensics investigators. Digital forensics involves getting information in a digital format, usually from a computer or some electronic media. It requires getting access to the device, locating the data and copying it and analyzing it to turn the data into information that can be used as evidence in the law of court. However, with cloud computing and with storage capacity outpacing network bandwidth and latency improvements, forensic data is starting to grow exponentially to the point that it makes it harder to process them in a timely manner and as of now, there are no tools designed specifically to address the challenges of locating, isolating and preserving information from the cloud in a way that protects privacy and enables it to be used in court as evidence [1].

II. BACKGROUND

2.1DIGITAL FORENSICS:

Digital forensics/digital forensic science is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.Murphy defines Digital Forensics as the application of science to the identification, collection, analysis and examination of digital evidence, whilst preserving the integrity of the information and maintaining a strict chain of custody for the evidence [2].

2.2 CLOUD FORENSICS:

We define Cloud forensics as the application of computer forensic principles and procedures in a cloud computing environment. Since cloud computing is based on extensive network access, and as network forensics handles forensic investigation in private and public network, Ruan et al.defined cloud forensics as a subset of network forensics. They also identified three dimensions in cloud forensics – technical, organizational, and legal.[3]

2.3 DIFFERENCE BETWEEN TRADITIONAL FORENSICS AND CLOUD FORENSICS

TRADITIONAL FORENSICS	CLOUD FORENSICS
Physical access to computing resources	Physical Inaccessibility.
No need to depend on third party	Dependence on the CSP.
No Multi-tenancy	Multi-tenancy
Better forensics tools	limitation of current forensics tools
No cloud environment.	Different types of cloud services (SaaS,PaaS, IaaS),in forensics face different opportunities and challenges.

in traditional computer forensics data is collected and analysed after and as a result of a security incident	in network forensics data is often collected and analysed with the specific aim to actively detect security intrusions

III. CLOUD FORENSIC METHODS CLASSIFICATION

We have classified cloud forensics methods in to two categories:

Traditional Cloud Forensics (reactive approach)

Digital forensics Readiness (Proactive approach)

3.1 TRADITIONAL CLOUD FORENSICS METHOD:

The cloud forensics process cycle including the eight major phases [4]:

1. Acquiring Subpoena: Digital Forensics Investigators require search warrant or subpoena in order to conduct a search of data and seize evidence.
2. Chain of custody: In multi-jurisdictional environments. Chronological ordered documentation of evidences is required to avoid allegations of evidence tampering or misconduct.
3. Imaging/hashing function. When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.
4. Validated tools. When possible, tools used for forensics should be validated to ensure reliability and correctness.
5. Analysis. Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.
6. Quality assurance. The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts.
7. Reporting. The forensic analyst must document his or her analytical procedure and conclusions for use by others.
8. Possible presentation. In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience.

The traditional digital forensic investigation process can be applied only after the crime has occurred .This process is perhaps too long for the cloud. There is always a technological gap between the rate of crime and the rate of research done in this.

3.1.1 ISSUES AT EACH STAGE OF A TRADITIONAL CLOUD FORENSIC INVESTIGATION:

There are many challenges defined at each stage of forensic process model.

Collection: this is the first and most crucial phase of the forensics process model as it includes identification of incident and evidence and then preservation of data. When conducting investigation with data stored with cloud services, one of the main issues is to identify where potential data resides. Digital evidence may be located in multiple client browser history caches, which also presents difficulty in collection and verification. Delays in accessing data due to legal or logistical issues could result in data being deleted before access is granted. Therefore timely identification and preservation are desirable [5].

Physical inaccessibility Distributing computing implies that evidence may exist in and reflect activities on many computers. In fact, the data may be stored in multiple physical locations and this makes the evidence collection procedure harder in cloud forensics. According to Ruan, Carthy and Kechadi (2011) there is a need for a procedure and set of toolkits to collect data in the cloud.

Lesser Control and More Dependence on the CSP: In digital forensics, investigators know that exact location of crime and can acquire full control over the evidence such as seizing hard drive. Cloud computing only exacerbates the problem; unfortunately, the control over data varies in different service models IaaS, PaaS, and SaaS [6]. Hence investigators have to depend on the CSP to collect the digital evidence in cloud computing environment. In the child pornography case study, Dykstra et al. highlighted the trust issue in collecting evidence [7].

Volatile Data: When dealing with computers and electronic data, the volume of data cannot only be overwhelming, and difficult and costly to manage. Once the Virtual Machine (VM) is turned off, all the data will be lost if investigators do not have the copy of data. Cloud data is mobile and can move from location to location rapidly, disappear just as quickly, and is difficult to collect. This needs to be considered in line with the volatility of data when undertaking collection from cloud sources [8] [9].

Large Bandwidth: Large bandwidth is necessary for evidence collection process; Guo et al .pointed out the requirement of large bandwidth issue for time critical investigation [10].

Multi-tenancy: In cloud computing, multiple VM can share the same physical infrastructure, i.e., data for multiple customers may be co-located. This nature of clouds is different from the traditional single owner computer system. In any adversarial case, when we acquire evidence two issues can arise. First, we need to prove that data were not comingled with other users' data [11], [12]. And secondly, we need to preserve the privacy of other tenants while performing an investigation [33]. Both of these issues make acquiring digital evidence more challenging.

Analysis of data: Data should be normalized according to the need of the investigation and irrelevant data should be ignored, this can be difficult task, as at the beginning of an investigation, it is difficult to determine what is and what is not relevant. This also highlights a need to identify the purpose of an investigation early in the process [11].

Chain of Custody Chain of custody is defined as a verifiable provenance or log of the location and possession

history of evidence from the point of collection at the crime scene to the point of presentation in a court of law. It is one of the most vital issues in traditional digital forensic investigation. Chain of custody should clearly depicts how the evidence was collected, analyzed, and preserved in order to be presented as admissible evidence in court [13]. Tools and procedures are yet to be developed for investigations in virtualized environment, especially on hypervisor level. Ruan et al. expressed the need of forensic aware tools for the CSP and the clients to collect forensic data [14]. However, the chain of custody must be preserved as well, which is challenging in multi-geographical and multi-jurisdictional environments.

Cross Border Law Multi-jurisdictional or cross border law is intensifying the challenge of cloud forensics. Data centers of the service providers are distributed worldwide. However, the privacy preservation or information sharing laws are not in harmonic throughout the world, even it may not be same in different states of a country. Cross border legislation and cross border red tape issues came in several cloud forensic research works [15], [16], [17].

Presentation For an investigator, prosecutor, and those involve in the court process, there is a need to understand the importance of the information being presented to them, and the implications of the information. In this stage an investigator accumulates his findings and presents to the court as the evidence of a case. Challenges also lie in this step of cloud forensics. Proving the evidence in front of the jury for traditional computer forensics isrelatively easy compared to the complex structure of cloud computing. Jury members possibly have basic knowledge of personal computers or at most privately owned local storage. But the technicalities of a cloud data center, running thousands of VM, accessed simultaneously by hundreds of users is far too complex for them to understand [18].

3.2 PROACTIVE FORENSICS

Traditional cloud forensics works on reactive approach principle:"wait until something fails and then take the necessary steps to fix it, this often results in hours or even days of lost productivity.

Proactive Forensics adopts automation to make the forensic evidence gathering process proactively, allowing the digital devices (computer) to adaptively focus resources on identifying and collecting possible traces to potential transgressors, in advance of an incident alert or evidence request [19].It is the same as traditional digital forensics in the sense that it still involves the analytical and investigative techniques used for the identification, extraction, preservation, documentation, analysis and interpretation of digital evidence. As the literature will show, the topic of Proactive Forensics is presented and an attempt to define, as well as interpret the scope of it. Even though Proactive Forensics is still a young branch of Digital Forensics, the academic researchers have already had a reasonably different perspective on the focus and spirit of Proactive Forensics [20].

DEFINITION OF PROACTIVE FORENSCIS:

Among all the definition of proactive forensics given by many researchers, fortoo*et al.* (2010) gave a more comprehensive definition covering all of the points:

"A forensic approach that focuses effort and resource to facilitate dynamic evidence collection, behavior upon detection of activities prior to an incident, storing the evidence proactively to make them amendable for future analysis and judicial review" [20].

This highlights three main special features of Proactive Forensics: dynamic evidence Collection, storage of relevant information, and judicial review standard evidence.

Related Disciplines:

3.2.1 Forensic Readiness (FR)

Forensics Readiness (FR) is defined as the ability of an organization to maximise its potential, in terms of preparing its system, physical and procedural security of data, and staff security-awareness, to gather data of evidential standards for admissibility,and at the same time minimizing the cost of investigation [21].

DEFINITION OF DFR:

Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation [22].Benefits of achieving a high level of digital forensic investigation readiness include, but are not limited to, higher admissibility of digital evidence in a court of law, better utilisation of resources (including time and financial resources) and higher awareness of forensic investigation readiness [23].

"Digital Forensic Readiness is defined as the pre-incident plan that deals with an organization's ability to maximize digital evidence usage and anticipate litigation.[24]

Digital forensic readiness is defined as the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [25]

(A) TOP 10 OBJECTIVES OF DIGITAL FORENSICS READINESS: [19] [21] [25]

1. To prepare organization in advance of an crime or evidence request
2. To gather admissible evidence legally
3. No interference with business process while collecting evidences.
4. To gather evidence targeting the potential crimes and disputes that may adversely impact an organization.
5. To allow an investigation to proceed at a cost in proportion to the incident.

6. To minimize interruption to the business from any investigation.
7. To ensure that evidence makes a positive impact on the outcome of any legal action
8. To maximize an environment's ability to harvest credible evidence
9. To maximize the potential to use comprehensive digital evidence.
10. To minimize the cost of forensics during an incident response.

(B) BENEFITS OF IMPLEMENTING DFR:[21]

1. Shortened investigation process
2. Cost efficinecy-due to short investigaton process
3. Quick access to court-admissible evidence
4. Demonstraton of due diligence and good governance
5. Improved chances for successful litigation
6. Support employee restriction or permission
7. Resolve business related dispute, example SLAs that have/have not been met.
8. Comprehensive evidence harvested without major disruption of business
9. The gathered evidence will be company's security in the event of a court case.
10. It can be a deterrent to inside threat as staff and stakeholders
11. It can enhance the interaction with legal authorities and law enforceres.

(C)COST ASSOCIATED TO IMPLEMENTING DFR:

1. DFR implementation could be expensive , organization should be aware of following costs:[21]
2. Revision to exixting policies and the establishment of new ones.
3. Training staff, especailly first responders.
4. Legal advice-to guide and authorise doumentation and communicatons.

3.2.2 Active (Live) Forensics:

Active (Live) Forensics is another big branch of digital forensics gaining notice in the recent years as an alteration to the traditional digital forensics [20]. However, its focus is on gathering relevant evidence while minimizing the effect of the incident during an on-going incident [19]. As opposed to traditional (dead) digital forensics, live forensics works to achieve retention of volatile data, and countermeasures for encrypted files on a live system, while the incident is taking place. The difference of Proactive Forensics is clear here in terms of when they are applicable in an incident.

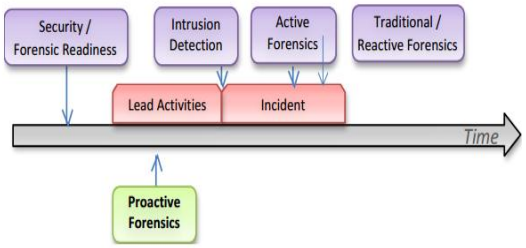

Fig. 1 - Timeline of Application of Different Approaches

The figure shows a timeline which different approaches above come in place in relation to an incident. So far the ideal existence of Proactive Forensics has been discussed through different researchers' view on its focus, the elements that it deals with, as well as how Proactive Forensics fits into the different current technologies [26].

IV. CONCLUSION

Authors' emphasis was on study and analysis of different cloud forensics models in order to provide trustworthy cloud forensics schemes and minimizing the cost of investigation. Researchers have explored the challenges and classified cloud forensics models. Authors suggest that proactive approach of forensics in cloud computing environment is the need of hour. The rate at which cyber crime is increasing, Research in this direction is still in its infancy. We conclude that more research is required in the digital world, especially in cloud forensics, to identify and collect digital evidences.

V. REFERENCES

[1] (http://gcn.com/articles/2014/06/30/nist-cloud-forensics.aspx).
[2] J. J. Murphey, "Forensic readiness'," 2007. [Online]. Available: www.dexisive.com/wp-content/.../06/Forensic-Readiness.pdf.
[3] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," in proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.
[4] Zatyko, K. (2007). Defining Digital Forensics, Forensic Magazine..
[5] Taylor, M, Haggerty, J, Gresty, D & Hegarty, R (2010), 'Digital Evidence in Cloud Computing Systems', Computer Law & Security Review, vol. 26, no. 3, pp. 304-308.
[6] Shams Zawoad:Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems.
[7] Dykstra, J & Sherman, A (2012), 'Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques', Digital Investigation.
[8] Ruan, K, Carthy, J, Kechadi, T & Crosbie, M (2011), 'Cloud Forensics', Advances in Digital Forensics VII, pp. 35-46.
[9] D. Birk, "Technical challenges of forensic investigations in cloud computing environments," in Workshop on Cryptography and Security in Clouds, January 2011.
[10] Guo, H, Shang, T & Jin, B (2012), 'Forensic Investigations in Cloud Environments', paper presented at the IEEE International Conference on Computer Science and Information Processing (CSIP).

[11] J. Dykstra and A. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies," Journal of Network Forensics, vol. b, no. 3, pp. 19–31, 2011.
[12] Taylor, M, Haggerty, J, Gresty, D & Lamb, D (2011), 'Forensic Investigation of Cloud Computing Systems', Network Security, vol. 2011, no. 3, pp. 4-10.
[13] Draft NISTIR 8006: NIST Cloud Computing, Forensic Science Challenges.
[14] Ruan, K, Carthy, J & Kechadi, T (2011), 'Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis'.
[15] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," in proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.
[16] Zafarullah, F. Anwar, and Z. Anwar, "Digital forensics for eucalyptus," in Frontiers of Information Technology (FIT). IEEE, 2011, pp. 110–116.
[17] G. Grispos, T. Storer, andW. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," International Journal of Digital Crime and Forensics (IJDCF),2012.
[18] D. Reilly, C. Wren, and T. Berry, "Cloud computing: Pros and cons for computer forensic investigations," International Journal Multimedia and Image Processing (IJMIP), vol. 1, no. 1, pp. 26–34, March 2011.