ISSN: 2321-7782 (Online)
Volume 3, Issue 8, August 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Study of Cloud Forensic

Kalyani A. Bhawar[1]
Anuradha Engineering College,
Department Computer Science & Engineering,
Chikhli, Maharashtra,
India

Dhiraj G. Vyawahare[2]
Professor
Anuradha Engineering College,
Department Computer Science & Engineering,
Chikhli, Maharashtra, India

Abstract: ***In this paper, we have a tendency to consistently examine the cloud forensics downside and explore the challenges and problems in cloud forensics. We have a tendency to then discuss existing analysis comes and finally, we have a tendency to highlight the open issues and future directions in cloud forensics analysis space. We have a tendency to posit that our systematic approach towards understanding the character and challenges of cloud forensics can enable U.S. to look at attainable secure answer approaches, resulting in magnified trust on and adoption of cloud computing, particularly in business, healthcare, and national security. This successively can cause lower value and long-run benefit to our society as a full.***

I. INTRODUCTION

Cloud computing has emerged as a most well-liked and inexpensive computing paradigm in recent years. Inside the last 5 years alone, we have got seen associate explosion of applications of cloud computing technology, for every enterprise and other people seeking any computing power and extra storage at associate occasional price. very little and medium scale industries find cloud computing very price effective as a result of it replaces the need for expensive physical and body infrastructure, and offers the flexible pay-as-you-go structure for payment. Khajeh-Hosseini et al. found that a company may save thirty seventh prices if they\'d migrate their IT infrastructure from associate outsourced info centre to the Amazon's Cloud.

Clouds use the multi-tenant usage model and virtualization to verify higher utilization of resources. However, these elementary characteristics of cloud computing are actually a ambiguous instrument – constant properties to boot build cloud-based crimes and attacks on clouds and their users difficult to forestall and investigate. in step with a recent IDCI survey, seventy four of IT executives and CIOs referred security as a result of the most reason to forestall their migration to the cloud services model . Some recent attacks on cloud computing platforms strengthen the security concern. as an example, a bonnet attack on Amazon's cloud infrastructure was reportable in 2009 . Besides offensive cloud infrastructure, adversaries can use the cloud to launch attack on different systems.

BACKGROUD

1. Cloud Computing

According to the definition by the National Institute of Standards and Technology (NIST), "Cloud computing is a model that provides a convenient means of on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), which will be apace provisioned and released with marginal management effort or service supplier interaction" [8]. The Open Cloud pronunciamento association defines cloud computing as "the ability to manage the computing power dynamically in a very efficient means and also the ability of the top user, organization, and IT workers to utilize the most of that power while not having to manage the underlying complexity of the technology". Cloud computing has some vital characteristics –On-demand self-service, broad network access, resource pooling, speedy snap, and measured service. Parkhill proposed utility computing in the past and Michael et al. mention cloud computing as a brand new

term for "computing as a utility". They outlined cloud computing as a Combination of Software-as-a-Service and utility computing, but they contemplate personal clouds outside of cloud computing.

2. *Cloud Forensic*

We outline Cloud forensics because the application of pc forensic principles and procedures in an exceedingly cloud computing environment. Since cloud computing is predicated on intensive network access and as network rhetorical handles forensic investigation in camera and public network, Ruan et al. defined cloud forensics as a set of network forensics. They conjointly have known 3 dimensions in cloud forensics– technical, structure, and legal. Consistent with the authors' information, until currently this can be solely definition of cloud forensics. Cloud forensics procedures can vary consistent with the service and preparation model of cloud computing. For SaaS and PaaS, we've terribly restricted management over method or network observation. Whereas, we will gain a lot of management in IaaS and might deploy some rhetorical friendly work mechanism. The primary 3 steps of pc forensics can vary for various services and preparation models. For example, the gathering procedure of SaaS and IaaS cannot be same. For SaaS, we tend to entirely depend upon the CSP to get the applying log, whereas in IaaS, we will acquire the Virtual machine instance from the client and might enter into examination and analysis part. On the opposite hand, in the personal preparation model, we've physical access to the digital proof; however we tend to just will get physical access to the general public preparation model.

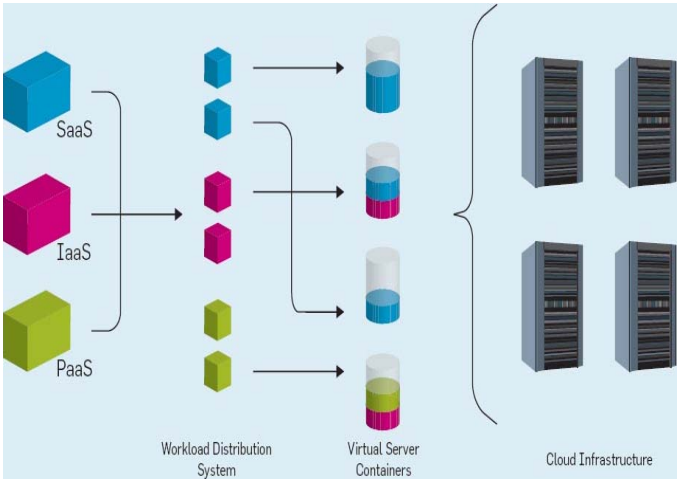

Fig 1: Customers' control over different layers in different service model.

Cloud forensic we define Cloud rhetorical because the application of laptop forensic principles and procedures in a very cloud computing atmosphere. Since cloud computing is predicated on intensive network access, and as network rhetorical handles forensic investigation in camera and public network, Ruan et al. defined cloud forensics as a set of network forensics [27]. They additionally identified 3 dimensions in cloud forensics – technical, structure, and legal. In step with the authors' data, until currently this can be solely definition of cloud forensics. Cloud forensics procedures can vary in step with the service and preparation model of cloud computing. For SaaS and PaaS, we've got terribly restricted management over method or network observance. Whereas, we are able to gain additional management in IaaS and may deploy some rhetorical friendly work mechanism. The first 3 steps of laptop forensics can vary for various services and preparation models. For instance, the gathering procedure of SaaS and IaaS won't be same. For SaaS, we have a tendency to only depend upon the CSP to urge the applying log, whereas in IaaS, we are able to acquire the Virtual machine instance from the client and may enter into examination and analysis part. On the opposite hand, within the non-public preparation model, we've got physical access to the digital proof; however we have a tendency to simply will get physical access to the general public preparation model.

II. CHALLENGES OF CLOUD FORENSICS

» ***Forensic Data Acquisation***

In this section, we have a tendency to examine the challenges in cloud forensics, as mentioned within the current analysis literature. We present our analysis by wanting into the challenges moon-faced by investigators in every of the stages of pc forensics (as described in Section II-B). a number of the vital challenges we address here are: rhetorical information acquisition, logging, preserving chain of custody, limitation of current forensics tools, crime scene reconstruction, cross border law, and presentation.

» ***Physical Inaccessibility.***

Physical unavailability of digital evidence makes the proof assortment procedure more durable in cloud forensics. The established digital rhetorical procedures and tools assume that we've physical access to the computers. However, in cloud forensics, things are different. Sometimes, we tend to don't even grasp wherever the info is located because it is distributed among several hosts in multiple data centers. Variety of researchers addresses this issue in their work.

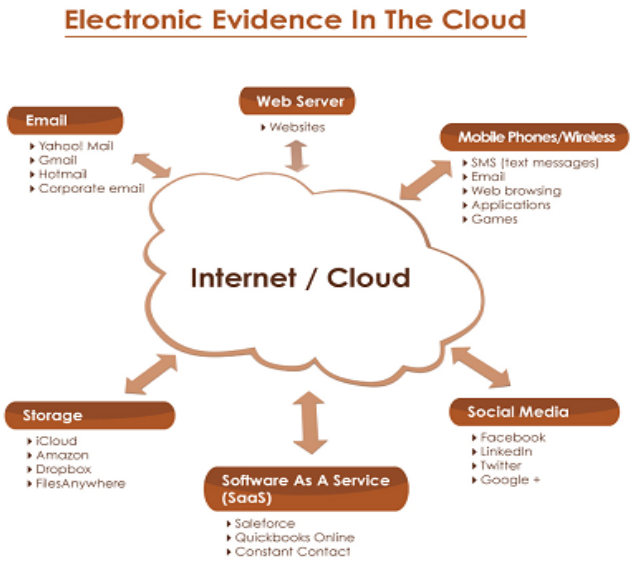

Fig2: Electronic evidence in the cloud.

» ***Less Control in Clouds and Dependence on the CSP.***

In ancient pc forensics, investigators have full management over the proof (e.g., a tough drive taken by police). In a cloud, sadly, the management over information varies in different service models. Figure shows the restricted quantity of management that customers have in several layers for the three service models – IaaS, PaaS, and SaaS. For this reason, we have a tendency to largely rely upon the CSP to gather the digital evidence from cloud computing surroundings. This is a serious bottleneck within the assortment part. In IaaS, users have a lot of management than SaaS or PaaS. The lower level of management has created the info assortment in SaaS and PaaS tougher than in IaaS. Sometimes, it is even not possible. If we have a tendency to manage to urge the image of an IaaS instance, it'll create our life simple to investigate the system. For SaaS and PaaS, we'd like to rely upon the CSP. We are able to solely get a high level of work info from this 2 service models. As customers have management over the applying deployed in PaaS, they'll keep log of different actions to facilitate the investigation procedure. On the contrary in SaaS, customers primarily haven't any management to log the actions. Dykstra et al. conferred the problem of information acquisition by employing a theoretic case study of kid smut. to analyze this case, the forensics examiner desires a bit-for-bit duplication of the info to prove the existence of contraband pictures and video, however in a very cloud, he cannot collect information by himself. At first, he must issue a search warrant to the cloud supplier. However, there are some issues with the warrant in respect of cloud environment. as an example, warrant should specify a location, but in cloud the info might not be set at a definite location or a selected storage server. What is more, the info can't be confiscated by confiscating the storage server

in a very cloud, as the same disk will contain information from several unrelated users. To identify the criminal, we'd like to grasp whether or not the virtual machine contains a static informatics. Nearly altogether aspects, it depends on the transparency and cooperation of the cloud supplier.

» ***Volatile data***

Volatile knowledge cannot sustain while not power. When we shut down a Virtual Machine (VM), all the info will be lost if we tend to don't have the image of the instance. This issue is highlighted in many analysis works. The ' IaaS has some benefits over SaaS and PaaS, store is a retardant in IaaS model if knowledge isn't forever synchronal in persistent storage, such as, Amazon S3 or compass point. If we tend to restart or flip off a VM instance in IaaS (e.g., in Amazon EC2), we will lose all the info. Written account entries or temporary web files, that reside or be hold on at intervals the virtual atmosphere can be lost once the user exits the system. The' with further payment customers will get persistent storage, this can be not common for little or medium scale business organizations. Moreover, a malicious user will exploit this vulnerability. After doing a little malicious activity (e.g., launch DoS attack, send spam mail), associate degree oppose will power off her virtual machine instance, which can result in an entire loss of the volatile knowledge and build the rhetorical investigation nearly impossible. Birk additionally mentioned a significant drawback relating to the volatile nature of proof in cloud. The matter states that some owner of a cloud instance will fraudulently claim that her instance was compromised by some other person and had launched a malicious activity. Later, it'll be troublesome to prove her claim as false by a rhetorical investigation [35].

» ***Trust Issue.***

Dependence on the third party additionally poses trust issue in investigation procedure. Within the erotica case study, Dykstra et al. highlighted the trust issue in collecting proof. Once supply an enquiry warrant, the examiner wants a technician of the cloud supplier to collect knowledge. However, the worker of the cloud supplier who collects knowledge is possibly not a licensed forensics investigator and it's unimaginable to ensure his integrity in a court of law. The date and timestamps of the info are also questionable if it comes from multiple systems.

Dykstra et al. experimented with aggregation proof from cloud atmosphere. One in all the shortcomings they found is that it's unimaginable to verify the integrity of the rhetorical disk image in Amazon's EC2 cloud as a result of Amazon will not offer checksums of volumes, as they exist in EC2.

» ***Large Bandwidth:***

In Section I, we've got seen that the amount of digital proof is increasing apace. Guo etal pointed out the need of enormous information measure issue for time critical investigation [30]. The on-demand characteristic of cloud computing can have important role in increasing the digital evidence in close to future. In ancient rhetorical investigation, we collect the proof from the suspect's laptop disc. Conversely, in cloud, we have a tendency to don't have physical access to the information. a method of obtaining knowledge from cloud VM is downloading the VM instance's image. The dimensions of this image can increase with the rise of knowledge within the VM instance. We'll need adequate information measure and incur expense to transfer this huge image. Multitenancy in cloud computing, multiple VM will share an equivalent physical infrastructure, i.e., knowledge for multiple customers could also be co-located. This nature of clouds is different from the standard single owner automatic data processing system. In any adversarial case, once we acquire proof 2 problems can arise. First, we want to prove that knowledge weren't comingled with alternative users' knowledge [29], [30]. And second, we need to preserve the privacy of alternative tenants whereas performing Associate in nursing investigation [33]. Each of those problems builds acquiring digital proof more difficult. The multitenancy characteristic additionally brings the side-channel attacks [36] that area unit troublesome to research.

III. LOGGING

Analyzing logs from completely different processes plays a significant role in digital rhetorical investigation. method logs, network logs, and application logs are extremely helpful to spot a malicious user. However, gathering this important data in cloud surroundings isn't as easy because it is in private owned ADPS, generally even not possible. Cloud forensic researchers have already known variety of challenges in cloud primarily based log analysis and forensics [30], [33], [37]. We tend to concisely discuss these challenges below.

» ***Decentralization***

In cloud infrastructure, log data is not situated at any single centralized log server; rather logs are suburbanized among many servers. Multiple users' log data could also be collocated or unfold across multiple servers. Volatility of Logs. A number of the logs in cloud surroundings are volatile, particularly just in case of VM. All the logs are unavailable if the user power off the VM instance. Therefore, logs are out there just for bound amount of your time. Multiple Tiers and Layers. There are many layers and tiers in cloud design. Logs are generated in every tier. For example, application, network, software system, and database – all of those layers manufacture valuable logs for forensic investigation. Assembling logs from these multiple layers is difficult for the investigators .Accessibility of Logs. The logs generated in several layers are have to be compelled to accessible to completely different stakeholders of the system, e.g., computer user, rhetorical investigator, and developer. System directors want relevant log to troubleshoot the system. Developers want the desired log to fix the bug of the appliance. Rhetorical investigators want logs which will facilitate in their investigation. Hence, there ought to be some access management mechanism, so everyone can get what they have specifically – nothing a lot of, nothing less and obviously, during a secure approach. Dependence on the CSP. Currently, to amass the logs, we extensively depend upon the CSPs. the supply of the logs varies betting on the service model. In SaaS, customers do no get any log of their system, unless the CSP provides the logs. In PaaS, it's solely potential to induce the appliance log from the purchasers. To induce the network log, information log, or software system log we want to depend upon the CSP. For example, Amazon doesn't give load balancer log to the Customers. During a recent analysis work, Marty mentioned that he was unable to induce MySql log knowledge from Amazon's Relational Database Service. In IaaS, customers don't have the network or method log. Absence of crucial data in Logs. There's no standard format of logs. Logs are out there in heterogeneous formats – from {different totally completely different completely different} layers and from different service providers. Moreover, not all the logs give crucial data for rhetorical purpose, e.g., who, when, where, and why some incident was dead.

IV. ADVANTAGE

Though cloud forensics could be a sophisticated method and Imposes new challenges in digital rhetorical procedure, it offers some advantage over ancient laptop forensics. Several researchers highlight the provision of computing environment through VM, which might be useful to accumulate the computing setting for rhetorical investigation [32], [34]. We are able to use the VM image to use as a supply of digital evidence. The computation and storage power of cloud computing can also step up the investigation method [33], [34]. Cloud computing will scale back the time for information acquisition, data repeating, and transferring and information cryptanalytic. Forensic image verification times are reduced if a cloud application generates scientific discipline substantiation or hash. Ruan etal highlighted some benefits of cloud forensics, such as, cost effectiveness, information abundance, overall hardiness, quantifiability and flexibility, standards and policies, and forensics-as-a service [27]. If the CSPs integrate rhetorical facilities in cloud environment, or they provide forensics-as-a-service to the client by utilizing the large computing power, then the customers don't got to implement any rhetorical schemes. In that manner, cloud forensics is price effective for tiny and medium scale enterprise. Currently, Amazon replicates data in multiple zones to beat the one purpose failure. In case of information deletion, this information abundance may be useful to collect proof. Amazon S3 mechanically generates MD5 hash of associate object after we store the item in S3, which removes the requirement of external tools and reduces the time for generating hash. Amazon S3 additionally provides versioning Support. From the version log, we

are able to get some crucial information for investigation, such as, World Health Organization accessed the info, and when, what was the requestor's information science, and what was the change in a very specific version. Roussev et al. showed that for large-scale forensics analysis, cloud computing outperforms the tradition rhetorical computing technique [61].

V. Open Issues

We've got seen that researchers have projected several solutions to mitigate some challenges. Sadly, only a number of the projected solutions are tested with planet eventualities. Besides that, to the most effective of the authors' information, CSPs haven't adopted any of the projected answer nonetheless. There are an honest range of open issues. Cloud management plane or API to urge the necessary logs will decrease the dependence on CSP. However, as we have a tendency to don't have physical access, we have a tendency to still want to rely on CSP for numerous rhetorical information acquisition purposes, e.g., aggregation temporary register logs, distinctive deleted files from fixed disk, etc. Therefore, decreasing the dependence on CSP continues to be unresolved. Limited information measure is another vital issue. If the cloud storage is simply too high then information measure are a challenge for time vital case. This issue has not been resolved nonetheless. Several researchers have projected secure information birthplace to mitigate the chain of custody issue. However, no concrete work has been done nonetheless, which might show however we are able to preserve the chain of custody by secure birthplace. To mitigate the cross border issue, researchers have projected international unity, however there's no guideline concerning however this can flip out into reality. Moreover, no answer has been projected for crime scene reconstruction or presentation problems. Modifying the existing rhetorical tools or making new tools to cope up with cloud setting is another massive issue that has not been resolved nonetheless. Several researchers additionally mentioned some open issues of cloud forensics. Concerning work issue in cloud forensics, Open issues Marty projected some open analysis topics in application level work, which are: security mental image, forensic time-line analysis, log review, log correlation, and policy monitoring [37]. Wolthusen known another vital open problem that is distinctive the precise location and jurisdiction under that a precise data point lies.

VI. Conclusion

With the increasing use of cloud computing, there is an increasing emphasis on providing trustworthy cloud forensics schemes. Researchers have explored the challenges and proposed some solutions to mitigate the challenges. In this article, we have summarized the existing challenges and solutions of cloud forensics to answer the question – Where does cloud forensics stand now? Current research efforts suggest that cloud forensics is still in its infancy. There are numerous open problems that we have mentioned in Section. By analyzing the challenges and existing solutions, we argue that CSPs need to come forward to resolve most of the issues. There is very little to do from the customers' point of view other than application logging. All other solutions are dependent on CSPs and the policy makers. For forensics data acquisition, CSPs can shift their responsibility by providing robust API or management plane to acquire evidence. Legal issues also hinder the smooth execution of forensic investigation. We need a collaborative attempt from public and private organizations as well as research and academia to overcome this issue. Solving all the challenges of cloud forensics will clear the way for making a forensics-enabled cloud and allow more customers to take the advantages of cloud computing.

References

1. A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud migration: A case study of migrating an enterprise it system to iaas," in proceedings of the 3rd International Conference on Cloud Computing (CLOUD). IEEE, 2010, pp. 450–457.
2. Market Research Media, "Global cloud computing market forecast 2015-2020," http://www.marketresearchmedia.com/ 2012/01/08/global-cloud-computing-market/, [Accessed July 5th, 2012].
3. Gartner, "Worldwide cloud services market to surpass $68 billion in 2010," http://www.gartner.com/it/page.jsp?id= 1389313, 2010, [Accessed July 5th, 2012].
4. INPUT, "Evolution of the cloud: The future of cloud computingingovernment,http://iq.govwin.com/corp/library/detail.cfm?ItemID=8448&cmp=OTC-cloudcomputingma042009, 2009, [Accessed July 5th, 2012].
5. Clavister, "Security in the cloud," http://www. clavister.com/documents/resources/white-papers/ clavister-whp-security-in-the-cloud-gb.pdf, Clavister White Paper, [Accessed July 5th, 2012].

6. Amazon, “Zeus botnet controller,” http://aws.amazon.com/ security/security-bulletins/zeus-botnet-controller/, Amazon Security Buletin, [Accessed July 5th, 2012].
7. FBI, “Annual report for fiscal year 2007,” 2008 Regional Computer Forensics Laboratory Program, 2008, [Accessed July 5th, 2012].
8. P. Mell and T. Grance, “Draft NIST working definition of cloud computing-v15,” 21. Aug 2009, 2009.
9. Open Cloud Consortium, “Open cloud manifesto,” The Open Cloud Manifestto Consortium, 2009.
10. D. Parkhill, “The challenge of the computer utility,” Addison- Wesley Educational Publishers Inc, US, 1966.
11. A. Michael, F. Armando, G. Rean, D. Anthony, K. Randy, K. Andy, L. Gunho, P. David, R. Ariel, S. Ion et al., “Above the clouds: A Berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.
12. Salesforce, “Social enterprise and crm in the cloud - sales- force.com,” http://www.salesforce.com/, 2012, [Accessed July 5th, 2012].
13. Google, “Google drive,” https://drive.google.com/start#home, [Accessed July 5th, 2012].
14. “Google calendar,” https://www.google.com/calendar/, [Accessed July 5th, 2012].
15. GAE, “Google app engine,” http://appengine.google.com, [Accessed July 5th, 2012].
16. Azure, “Windows azure,” http://www.windowsazure.com, [Accessed July 5th, 2012].
17. B. Grobauer and T. Schreck, “Towards incident handling in the cloud: challenges and approaches,” in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ser. CCSW ’10. New York, NY, USA: ACM, 2010, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/1866835.1866850
18. Amazon EC2, “Amazon elastic compute cloud (amazon ec2),” http://aws.amazon.com/ec2/, [Accessed July 5th, 2012].
19. H. Motahari-Nezhad, B. Stephenson, and S. Singhal, “Out- sourcing business to cloud computing services: Opportunities and challenges,” IEEE Internet Computing, Palo Alto, vol. 10, 2009.
20. Amazon, “Amazon simpledb,” http://aws.amazon.com/ simpledb/, 2012, [Accessed July 5th, 2012].
21. F. Chang, J. Dean, S. Ghemawat, W. Hsieh, D. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. Gruber, “Bigtable: A distributed storage system for structured data,” ACM Trans- actions on Computer Systems (TOCS), vol. 26, no. 2, p. 4, 2008.
22. J. Wiles, K. Cardwell, and A. Reyes, The best damn cyber- crime and digital forensics book period. Syngress Media Inc, 2007.
23. K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” NIST Special Publication, pp. 800–86, 2006.
24. D. Lunn, “Computer forensics–an overview,” SANS Institute, vol. 2002, 2000.
25. J. Robbins, “An explanation of computer forensics,” National Forensics Center, vol. 774, pp. 10–143, 2008.
26. K. . L. Gates, “E-discovery amendments to the federal rules of civil procedure go into effect today,” http://bit.ly/UJU5cs, December 2006, [Accessed July 5th, 2012].
27. 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.
28. D. Birk, “Technical challenges of forensic investigations in cloud computing environments,” in Workshop on Cryptogra- phy and Security in Clouds, January 2011.
29. 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.
30. H. Guo, B. Jin, and T. Shang, “Forensic investigations in cloud environments,” in Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012, pp. 248–251.
31. S. Wolthusen, “Overcast: Forensic discovery in cloud environ- ments,” in proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics (IMF). IEEE, 2009, pp. 3–9.
32. 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.
33. M. D. Ludwig Slusky, Parviz Partow-Navid, “Cloud comput- ing and computer forensics for business applications,” Journal of Technology Research, vol. 3, July 2012.
34. M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, “Digital evidence in cloud computing systems,” Computer Law & Security Review, vol. 26, no. 3, pp. 304–308, 2010.
35. D. Birk and C. Wegener, “Technical issues of forensic in- vestigatinos in cloud computing environments,” Systematic Approaches to Digital Forensic Engineering, 2011.
36. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,” in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 199–212.
37. R. Marty, “Cloud application logging for forensics,” in pro- ceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 178–184.
38. AWS, “Amazon web services,” http://aws.amazon.com, [Ac- cessed July 5th, 2012].
39. J. Vacca, Computer forensics: computer crime scene investi- gation. Delmar Thomson Learning, 2005, vol. 1.
40. G. Grispos, T. Storer, and W. Glisson, “Calm before the storm: The challenges of cloud computing in digital forensics,” International Journal of Digital Crime and Forensics (IJDCF), 2012

