Discussion on the Challenges and Opportunities of Cloud Forensics

Rainer Poisel and Simon Tjoa

Institute of IT Security Research
St. Poelten University of Applied Sciences
St. Poelten, Austria
{rainer.poisel,simon.tjoa}@fhstp.ac.at
http://www.fhstp.ac.at

Abstract. Cloud Forensics refers to digital forensics investigations performed in Cloud Computing Environments. Nowadays digital investigators face various technical, legal, and organizational challenges to keep up with current developments in the field of Cloud Computing. But, due to its dynamic nature, Cloud Computing also offers several opportunities to improve digital investigations in Cloud Environments. Digital investigators may utilize Cloud Computing setups and process complex tasks in cloud infrastructures. Thus they can take advantage of the enormous computing power at hand in such environments.

In this paper we focus on the current State-of-the-Art of affected fields of Cloud Forensics. The benefit for the reader of this paper is a clear overview of the challenges and opportunities for scientific developments in the field of Cloud Forensics.

Keywords: Cloud Forensics, digital forensics, evidence.

1 Introduction

In recent years, Cloud Computing has gained vastly in importance. It has been introduced to optimize the general usage of IT infrastructures. Cloud Computing is a technology that evolved from technologies of the field of distributed computing, especially grid computing [28]. According to NIST [48], "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

There will be substantial market growth in the field of Cloud Computing over the next few years. According to Kazarian and Hanlon [35], 40% of small and medium businesses (SMBs) from different countries are expected to use three or more cloud services and migrate their data into the cloud. In 2010, Gartner [31] released a study which forecasted the cloud service revenues to reach 148.8 billion in 2014 (compared to 58.6 billion in 2009). Carlton and Zhou [18] state that Cloud Computing is, from a technical point of view, a combination of existing

G. Quirchmayr et al. (Eds.): CD-ARES 2012, LNCS 7465, pp. 593–608, 2012.
© IFIP International Federation for Information Processing 2012

technologies. People have difficulties to capture the big picture: for managers and customers of cloud services the idea is similar to exchanging information through web-based user interfaces. Others view the concept as being an extension of the timesharing concept from the 1960s.

Cloud providers sell services based on different business models (also referred to as "service models"): Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [47,26]. With SaaS, the customer uses applications which are provided by the service seller (e. g. web-based e-mail services). With PaaS, the service seller then provides his infrastructure (servers, operating systems, network, etc.). The customer is able to write/use his own applications using the application programming interface made available by the provider. IaaS enables the user to use and run software of his choice (e. g. operating systems). The service seller provides the customer with the necessary infrastructure (servers, network, storage facilities, etc).

Depending on the level of access to the underlying cloud infrastructure the following types of clouds have been categorized [47,39]: private clouds, community clouds, public clouds, and hybrid clouds. In "private clouds" the infrastructure is operated on behalf of a single entity. Usually the infrastructure is located in the premises of the organization. "Community clouds" refer to cloud deployments where the infrastructure is shared by several organizations. In "Public Clouds" one or more providers run the infrastructure and make it available to anybody who wishes to pay for the service. "Hybrid clouds" refer to setups which are formed out of two or more cloud infrastructures. These in turn can be private, community, or public clouds. Of course, the shift in intercommunications and interaction between IT systems poses new challenges for digital forensics investigations. Cloud Service Providers (CSPs) often do not let their customers look behind their "virtual curtains" [15]. Vendor dependent implementations, multiple jurisdictions and proprietary data exchange formats [13] bring digital forensics into a deeper crisis as it is already facing [29]. Ruan et al. [58] defined Cloud Forensics as being a cross discipline between Cloud Computing and digital forensics. It is further recognized as a subset of network forensics [43]. Network forensics deals with investigating private or public networks and as Cloud Computing is based on broad network access it should follow the main phases of the network forensic process. Delport et al. [25] deem Cloud Forensics to be a subset of computer forensics as clouds consist of several nodes which are computers. This means that Cloud Forensics combines both, computer forensics and network forensics [1].

Ruan et al. [58] further extended the definition of Cloud Forensics across three major dimensions: technical, legal, and organizational. The technical dimension describes the set of procedures and tools which are utilized to carry out the digital forensics process in cloud environments. The organizational dimension refers to the fact that Cloud Computing involves at least two parties: CSPs and cloud customers. Further it is possible that CSPs outsource some of their services to other CSPs. The legal dimension refers to multi-jurisdiction and multi-tenancy challenges. Both fields have been exacerbated in cloud environments. Existing agreements and regulations have to be adopted for forensics activities to not breach any jurisdictions or confidentiality measures.

This paper is structured into two parts. First we focus on the current State-of-the-Art of affected fields of Cloud Forensics. In the second part, based on the current State-of-the-Art, related challenges and opportunities are identified in order to derive and describe open research problems.

2 State of the Art of Cloud Forensics

This chapter describes the State-of-the-Art of affected fields of digital forensics investigations in cloud environments.

2.1 Existing Digital Forensics Frameworks

Digital investigations have to consider various perspectives (e.g. legal perspective, technological perspective) in order to be successful. In order to coordinate the efforts between the various stakeholders, there exist a variety of publications dealing with procedures how to handle, analyze, document and present digital evidence. The presented work in this subsection contains well-known and well-established guidelines which are not specifically tailored to Cloud Computing. To some extent the principles introduced are also valid for cloud technology. However, an adaption of the organizational frameworks has to be considered to deal with the new challenges arising from the usage of Cloud Computing.

In the First Responder's Guide for Electronic Crime Scene Investigations [2], the forensic process is split into the four phases, (1) collection, (2) examination, (3) analysis and (4) report. The first phase is dedicated to capture electronic evidence. Thereafter, in the examination phase content and state of evidence is documented and the evidence is examined concerning hidden and obscured information. The last step of the second step is to reduce the information. In the analysis phase the evidence is analyzed concerning the relevance to the case. While examination is a technical task, analysis is usually conducted by an investigation team. Finally, in the last step reporting takes place [2].

NIST SP800-86 [34] shows how digital forensics can support incident handling. This publication focuses tackles digital forensics mainly from an IT perspective, not a legal perspective. The forensics process uses the phases of [34].

Further widely-used digital forensic frameworks include the digital forensics framework of the Association of Chief Police Officers (ACPO) [8] and the DFRWS (Digital Forensics Research Workshop) Investigative Process model [19]. Cohen proposes, in [22], a model consisting of the seven phases: identification, collection, transportation, storage, examination and traces, presentation, and destruction. Ke [36] describes the application of the SABSA model to the digital forensics process to obtain forensically sound evidence. More information on digital forensics frameworks can be found in [52].

2.2 Investigation of Cloud Infrastructures

According to Zimmerman and Glavach [66], the technology of Cloud Computing is not new. It is a new way of providing applications and computing resources on demand. Therefore the technology seems a perfect solution for smaller businesses that do not have the necessary resources to completely fulfil their IT needs [14,51]. Further, it allows private end users to utilize massive amounts of computing resources at affordable prices. However, the introduction of new technologies poses new challenges for the digital forensics investigator [65]. Grispos et al. show "how established digital forensic procedures will be invalidated in this new environment" [32]. They propose research agendas for addressing the new challenges depending on the investigation phase. As mentioned in the previous section there exist several organizational digital investigations frameworks. In the following the different investigation steps: identification, preservation, examination, and presentation are elucidated regarding their implementation for the investigation of cloud environments.

Identification, Preservation, and Acquisition: Grispos et al. outline in [32] the lack of frameworks to determine which elements were affected by IT specific crimes. The usage of conventional intrusion detection systems in the context of Cloud Computing infrastructures has been proposed by several authors [32]. The preservation and acquisition step deals with evidence collection from computer based systems. The increasing storage capacity of devices and computer systems are everlasting challenges in digital forensics investigations [32]. With the introduction of Cloud Computing systems this challenge is still ubiquitous: the elastic ability of Cloud Computing infrastructures allows the user to request additional data storage in a limitless fashion.

The chain of custody documents how evidence was handled in the context of the digital investigations process [20]. The documentation describes how evidence was collected, analyzed, and preserved to be approved in court. Due to the remote nature of Cloud Computing scenarios, assumptions that have been made with the investigation of traditional computer systems are not valid anymore [53]. Investigators usually had physical access to traditional computer systems [66]. Therefore they were able perform a live analysis or to remove storage devices for analyzing them in a forensics laboratory. Storage devices are accessed through a computer network. Digital investigators have to obtain control of cloud services before investigating them [58]. Depending on time an investigator requires to gain control of such a service, relevant evidence can be destroyed (deliberately or accidentially) by both, the service user and the cloud provider [32]. In this regard, IaaS deployments provide much more useful information for digital forensics investigations than PaaS or SaaS setups [15,16]. With PaaS or SaaS deployment scenarios, customers do not have any control of the underlying operating infrastructure. The amount of information from servers is limited and therefore, the client has to contribute to the investigation process. Besides the technical challenges, the lack of regulatory and legal frameworks complicate meeting the chain of custody requirements [63].

In Forensics, 'live' acquisitions and investigations allow to obtain data stored in non-persistent memory such as process information or active network connections [12] as well as temporary data, such as file locks or web browsing caches [15,32], RFC3227 [17] explains several best practices regarding live investigation of systems in case of security incidents.

However, traditional forensics guidelines require storage images to be forensically sound. Therefore bit-by-bit copies including a check sum are made from digital storage devices from instances in “dead” state (the system has been shutdown) to proof the unadulteratedness of digital evidence [8]. Traditional search and seizure procedures may be impractical for performing digital investigations in Cloud Computing environments. Digital evidence is stored in cloud data centres, desktop computers or mobile phones which could be out of physical control by the digital investigator [62]. As it is almost impossible to make a bit-by-bit copy of storage devices [66] the ACPO guidelines are rendered pointless when it comes to complete authenticity of digital evidence in cloud environments. Acquiring all storage devices from such a setup would be too time consuming for investigators and too disruptive for CSPs [32]. Usually cloud users are only offered remote access to the logical representation of their data. In most cases, the underlying physical infrastructure is transparent for the user. In the future, new methods will be needed to allow partial recovery of data from physical devices in accordance with accepted forensic principles. Therefore, forensics tools have to be hybrid of the current live and post-mortem analysis methods [66]. There will be a need for intelligent tools that note and predict artefacts based on heuristics. Delport et al. outline in [25] that it might be necessary to isolate cloud instances in case they have to be investigated. The problem associated with isolating cloud instances is the integrity of data intended for digital forensics investigations [14].

Basically, methods for clearing include moving uninvolved instances or suspicious instances to other nodes. This way the CIA of other instances is protected, but it might result in loss of possible evidence. However, by moving instances, evidence is protected from being tampered by these moved instances. Delport et al. [25] presented different techniques to isolate instances of cloud environments.

Instance relocation means moving an instance inside a cloud environment by moving the data logically or by creating new and destroying old instances. Server farming refers to putting up a spare instance which offers the same functionality as the instance intended for digital investigations. By Sandboxing programs can run in an environment which they cannot escape. Man in the Middle (MitM) refers to placing an entity between a sender and a receiver. In the field of digital forensics this entity is placed between the cloud instance and the hardware of the cloud. Delport et al. [25] conclude that none of their presented approaches fulfils every requirement for the investigation of cloud environments. However, depending on the case techniques may be combined to gain explicit access to a cloud instance.

The usage of cryptography in cloud environments poses additional challenges. CSPs offer encryption as a security feature to their customers. All data is encrypted on the client's side. The key to the encrypted data is never stored in the cloud environment [9].

Deleted data represents another major challenge due to the volatility and elasticity of cloud environments. On one hand, data that has remotely been requested to be deleted can be a rich source of evidence as it can still be physically existing [32]. On the other hand it depends on the CSP how to proceed in the event of a user requesting his data to be deleted [15,66] (e. g. Google's policy includes the deletion of such data from both, its active and replication servers as well as of all pointers to this data).

Reilly et al. [53] also mentioned the lack of tool support for dealing with digital investigations with cloud data centres. Currently, most tools are intended for examining data from traditional computer setups such as office or home computers. Taylor et al. [62] recommended to update existing tool suites such as EnCase or FTK to account for new developments in the field of Cloud Computing.

Examination and Analysis: Forensic tool suites such as The SleuthKit, FTK or EnCase perform "pattern matching" and "filtering" of data that is existing in different types of memory. Evidence in cloud is manifold and will likely be similar to evidence found in traditional computer setups [32]: office application documents, file fragments, digital images, emails, and log file entries [46]. Checksums are used to verify the integrity of objects (disk images, files, log entries, etc.) in the Cloud. Detecting file signatures of files in question or files which should be excluded from a digital forensics investigation are crucial for the filtering process. Hegarty et al. [33] describe a method for adapting existing signature detection techniques for their usage in cloud environments. To detect files with a specific hash value a so called "initialiser" submits the target buckets (storage units of a cloud customer) as well as the hash value to a so called "Forensic Cluster Controller" which in turn distributes the job of finding files with that has value to so called "Analysis Nodes".

In the future investigating cloud infrastructures may be a task performed by cloud deployments. However, cloud customers may access applications offered in the Cloud from a myriad of different computer setups (mobile phones of different make, desktop PCs with different operating systems, etc.) [62].

Presentation: Digital evidence can be utilized in several ways: it can be submitted to court in the form of a report [19] or it may be used by an organization to improve corporate policies and support future investigations [64]. Grispos et al. [32] highlight the need for a standard evaluation method for Cloud Forensics so that Cloud Forensics investigation results pass the Daubert principles [45]. Another challenge arises from explaining the Cloud Computing concept to a jury in court [53]. It may be difficult for a jury member to comprehend the concept as jury members will usually only have basic knowledge of how to use home PCs.

2.3 Digital Investigations Using Cloud Infrastructures

According to cloud security alliance [5], industry is heading forward to create Security-as-a-Service (SecaaS). The authors identified the following ten domains that are likely to interest consumer in the future: (1) Identity and Access

Management Services; (2) Data Loss Prevention; (3) Web Security; (4) Email Security; (5) Security Assessments; (6) Intrusion Management, Detection and Prevention (IDS/IPS); (7) Security Information and Event Management; (8) Encryption; (9) Business Continuity and Disaster Recovery; (10) Network Security. Within one of these domains the authors identify the requirement to "... provide customers with forensics support...". This opinion is also supported by Ruan et al. [58] who derive from the emerging trend to security-as-a-service that forensics-as-a-service will gain importance in cyber criminal investigations by providing massive computing power.

Reilly et al. [53] take the discussion of the usage of cloud technologies for forensic investigations one step further and highlight the benefits delivered by the usage of Cloud Computing for digital investigations. The major advantages identified by the authors include large-scale storage, high availability and massive computing power. Roussev and Richard [55,54] recognized the need for distributed forensics at an early stage. In their paper [56] they formulated the following requirements that should be satisfied by a distributed digital forensic toolkit: Scalability, platform-independence, lightweight, interactivity, extensibility and robustness. As cloud technologies can meet the abovementioned requirements, Roussev et al. evaluate in their paper [56] the feasibility and applicability of MapReduce for forensics applications. Map Reduce [24] was developed by Google in order to facilitate large scale computing. Phoenix [60] and Hadoop [4] are well known implementations of Google's MapReduce model. In their paper, the authors present their prototype, called MPI MapReduce (MMR), which is based on the Phoenix shared memory implementation. In order to test the performance of the prototype they implemented three Hadoop samples (wordcount, pi-estimator and grep) for MMR.

Cohen et al. introduce in [23] their GRR Rapid Response framework which pursues the objective to support live forensics within in an enterprise. The framework is designed to be highly scalable and is available for all common platforms. The proposed architecture is supported by an open-source prototype that is available [23].

Hegarty et al. present in their paper [33] the distributed calculation of file signatures if analyzing distributed storage platforms. Their proposed architecture consists of the three components: initializer, forensic cluster controller and analysis nodes.

Distributed computing power for password recovery or hash cracking is already well established. Various publications (e.g. [67]) and tools (e.g. Distributed Network Attack by AccessData [6,59]) are devoted to this significant subject. eDiscovery applications which are also an important component in an digital investigator's daily business are already available for cloud implementations. An example is the open source eDiscovery software FreeEd [3].

2.4 Digital Evidence in Cloud Computing Environments

The introduction of Cloud Computing provided a change of paradigms to the distributed processing of digital data. In their paper Taylor et al. [61] focuses on the legal aspects of digital forensics investigations. They concluded that due to the increasing number of interacting systems the acquisition and analysis of digital evidence in cloud deployments is likely to become more complex. The data could be encrypted before being transferred to the Cloud or it could be stored in different jurisdictions resulting in data being deleted before investigators have access to it [47].

Flaglien et al. [27] evaluated currently used formats for handling digital evidence against criteria identified in recent research literature. Recent developments with a focus on evidence exchange have been presented. Formats intended for storing evidence from highly dynamic and complex systems are characterized by incorporating additional information which can be processed by data mining tools.

Birk [15] and Wegener [16] mentioned digital evidence to be in one of three different states: at rest, in motion or in execution. Data at rest is stored on storage media. In this case it does not matter if the data is allocated to a file or if it has been deleted. Data in motion is usually data that is transferred over a computer network. Data that is neither in rest nor in motion is referred to as to be in execution. Usually this means process data that has been loaded into memory. In cloud environments evidence can be found on several sources: the virtual cloud instance (where the incident happened or originated), the network layer, and/or the client system [66,15]. Especially in SaaS setups evidence can be found on client systems.

Lu et al. [44] proposed to adopt the concept of provenance to the field of Cloud Computing. As a data object is able to report who created it and modified its contents, provenance could provide digital evidences for post investigations. However, up to now, provenance is still an unexplored area in Cloud Computing. Provenance information would have to be secured in cloud environments as leaking this information could breach information confidentiality and user privacy. Marty [46] follows a similar approach. CSPs and application providers utilize logging facilities to generate and collect relevant data to support the digital forensics investigation process. The sources for logging can be manifold: “business relevant logging covers features used and business metrics being tracked” [46]. Operational logging covers errors that concern a single cloud customer, critical conditions that impact all users, system related problems, etc. Forensics investigations are supported by security logging which focuses on login information, password changes, failed resource access and all activity that is executed by privileged accounts.

Cloud customers lose control over their data and executions in case they outsource the execution of business processes to the Cloud [21]. Accorsi [7] stated that this problem could be overcome with remote auditing. Data analytics perform traditional audits remotely by assess and report on the accuracy of financial data. This requires the introduction of an additional service model: business-process-as-a-service (BPaaS). It is based on the SaaS provision model and provides methods for modelling, utilizing, customizing, and executing business processes in cloud infrastructures. Access to the physical systems is neither possible nor necessary: external auditors will have access to both the auditee's system and the auditee's compartment in the cloud. Then it is possible for the auditors to employ remote auditing, thus addressing the inherent loss of control.

2.5 Hypervisor Forensics

Hypervisors (also referred to as "Virtual Machine Manager" or "VMM") can be understood as a host operating system which performs the allocation of computing resources such as memory, CPU, disk I/O and networking among operating systems that are running as "guest operating systems" [43]. As hypervisors build the bridge between guests and physical computer hardware, all data that is processed has to pass through the hypervisor before it can access physical devices (e. g. network interface cards, CPU ...).

The usage of data from hypervisors to prove various actual situations has been proposed in previous research papers [30,37]. The terminology has been referred to as "virtual machine introspection" (VMI) and data gathered from this level of access supported the operation of Intrusion Detection Systems (IDS). Payne and Lee [50] focused on the development of an abstract monitoring architecture. Their programming library "XenAccess" has been released as an open-source project. Later the source-base has been forked: the project is currently released as another open-source programming library "LibVMI". The library is "focused on reading and writing memory from virtual machines" [41]. Therefore monitoring applications can access the memory state and disk activity of target operating systems in a safe and efficient manner.

Later work which was based on VM introspection and monitoring software focused mainly on the detection of and defence from malicious software. Ando et al. [10] modified Linux as guest operating system to be able to obtain event-driven memory snapshots. Heuristics developed in this project allowed the detection of unknown malware which could not be detected by characteristic signatures.

Kuhn and Taylor [40] focused on capturing exploits in virtualized environments (such as cloud infrastructures). They concluded that there is no common collective base of root-kits, applications, and kernel versions for the forensic analysis of memory in virtualized environments to form a ground-truth for cross technology comparisons. Lempereur et al. [42] presented a framework which could be used to automatically evaluate live digital forensic acquisition tools on different platform configurations. Live digital forensics techniques play an important role in the area of virtualized environments. In their work they describe three classes of digital forensic evidence: stored information (high amount, slow access), information pending storage, and operational information. Operational information can help to narrow down the amount of searches to analyze stored information. This is true for both locally stored information (e. g. within an instance) and information stored on remote systems (e. g. cloud storage).

Krishnan et al. [38] proposed a forensics platform that transparently monitored and recorded data access events within a virtualized environment by only using the abstractions which were exposed by the hypervisor. The developments focused on monitoring access to objects on disk and allowed to follow the causal chain of the accesses across processes even if objects were copied into memory. Transactions of data have then be recorded in a audit log which allowed for faithful reconstruction of recorded events and the changes that they induced. In their work the authors demonstrated how their approach could be used to obtain behavioural profiles of malware.

Current research results demonstrate the feasibility of information acquisition from virtual machine managers (Hypervisors) to support the digital forensics analysis process. However, most work is focused on smaller setups (e. g. single physical machine with several VMs). Therefore we propose that more research should be done to investigate the acquisition of digital evidence across multiple virtualized environments, as given in Cloud Computing.

3 Discussion on Challenges and Opportunities

Beside its opportunities and advantages regarding the general usage of IT infrastructures the introduction of Cloud Computing has brought several challenges for the digital forensics investigator. Ruan et al. [58,57] explained both the challenges and opportunities of digital forensics investigations in cloud environments. Based on this knowledge and the current State-of-the-Art of digital forensics in cloud environments (Section 2) we identify areas for future research. Our findings are visualized in kind of a Venn diagram: a sub-set of challenges can be seen as sub-set of opportunities (see Figure 1).

In the field of digital forensics, tools and procedures have to be used to cope with new technical developments. Garfinkel [29] mentioned that in this regard digital forensics is facing a crisis: advances and fundamental changes in the computer industry will lead to the loss of hard-won capabilities. Cloud Computing and the involved interconnection of computer systems are among the enumerated reasons. The following section breaks down the impacts on digital forensics investigations.

Data Volume and Performance. Appropriate capture and display filters have to be developed and set up in order to make the data volume present in Cloud Infrastructures processible. On the other hand, the elastic nature of Cloud Computing setups also increases the scalability and flexibility [58,53]. Complex tasks can be processed on arbitrary numbers of instances in a distributed fashion.

Complexity. The topic of Cloud Forensics is of multi-dimensional complexity [58]. Different hypervisor vendors provide different application programming interfaces with a short life-cycle to their customers. Different hypervisor architectures influence the structure of instances running in the cloud. The information exchange between multiple CSPs around the world may further complicate the forensics investigation of such systems.

Legal Situation. In cloud setups from different countries, there exists a high probability that multiple jurisdictions may apply. Another problem comes from the easy-to-use feature of most cloud deployments. Weak registration systems allow facilitating anonymity that can be easily abused by criminals to conceal their traces and identities [**?**].

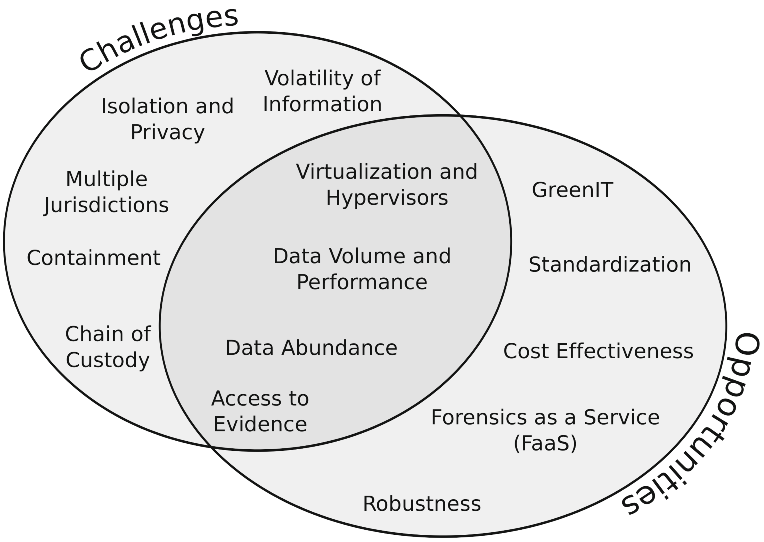

Fig. 1. Challenges and Opportunities of Cloud Forensics

Containment. It is a characteristic for cloud services that interruptions and attacks can have huge effects for a myriad of customers. An example that highlighted the strong dependence of cloud users on their providers was the outages of Amazon's and Microsoft's data centres in Dublin 2011 [49].

Isolation & Privacy. Many cloud service providers provide multi-tenant storage to their customers. Different customers that access the storage units may contaminate therefore the acquisition of forensic data before investigations can take place. Another problem resides in availability issues which can be caused by isolating instances from other instances [32].

Access to Evidence. Due to the impossibility of specifying the storage location at a high level, it may be difficult for investigators to access the data required for conducting forensics investigations [53]. Additionally CSPs intentionally hide the detail of the storage location from their customers to allow for data replication and movement across different service models [32].

Ephemeral Nature of Information in the Cloud. As storage is logical and focused on data allocated to objects (e. g. files), traditional file recovery techniques may not work with acquired images because they may not include file fragments or data from unallocated disk space [33]. Due to the cloud infrastructure being mostly under control of the cloud service provider [21], it may also be difficult to gain remote access to deleted data [58].

Virtualization and Hypervisors. Cloud deployments are often based on virtualization: CSPs implement instances of Cloud Computing in virtualized environments. Running instances are monitored and provisioned by hypervisors. In a cloud setup the hypervisor is the basic module: any successful attack may compromise the security of all systems that are under control of the hypervisor. There are strategies which cope with the detection and elimination of malware in virtual environments but there is a lack of policies, procedures, and techniques on the hypervisor level to facilitate digital forensics investigations. Future tools for the investigation of cloud infrastructures will address this problem further by allowing the correlation of evidence gathered from different hypervisors [38,42,50].

Standardization. The change in technology causes that new standards have to be developed and established [58]. Due to the early stage it is possible that standardized procedures for Cloud Forensics evolve together with the development of Cloud Computing as it matures.

Chain of Custody. At the moment documenting the chain of custody in Cloud Computing environments is an unsolved challenge. Service models such as SaaS only allow accessing a logical view of the data stored in the Cloud. Traditional methods (such as calculating hash values) that prove the integrity of data may be of no use in online scenarios. Best practices and procedures are composed into organizational frameworks. They describe the measures that have to be taken in case digital forensics investigations are conducted [32]. To overcome the problems regarding the chain of custody, an organizational framework that is suitable especially for digital forensics in Cloud Computing environments has to be implemented [22,36,63].

Cost Effectiveness. Forensics-as-a-Service (FaaS) [58] allows to plan and utilize the amount of necessary computing power required by digital forensics investigations [56].

GreenIT. Due to the scarcity of natural ressources for the production of energy required to power IT infrastructures, developments are necessary to optimize the energy consumption of nowadays devices [11]. FaaS may use idle computing resources and thus comes towards the requirements of GreenIT.

4 Conclusion and Outlook

Within this paper the current State-of-the-Art in Cloud Forensics has been presented. The subsequent discussion has shown that research has to be performed in all three subareas (technical, legal, organizational) of Cloud Forensics. Based on the results of this discussion of Cloud Forensics research we intend to focus on hypervisor forensics as both a challenge and an opportunity and the establishment of a solid organizational framework for carrying out digital forensics investigations in cloud environments. Due to the vast amount of data that has to be analyzed we intend to utilize other Cloud Computing setups to overcome the processing limits of single machines.

References

1. Children warned against net predators (2000), http://news.bbc.co.uk/2/hi/uk_news/education/648156.stm
2. Electronic crime scene investigation: An on-the-scene reference for first responders, recommendations of the National Institute of Standards and Technology (2001)
3. Freeeed.org - open-source ediscovery engine (2011), http://www.freeeed.org/
4. Hadoop - mapreduce (2011), http://hadoop.apache.org/mapreduce
5. Security guidance for critical areas of focus in cloud computing v3.0 (2011)
6. AccessData: Decryption and password cracking software, http://accessdata.com/products/computer-forensics/decryption
7. Accorsi, R.: Business process as a service: Chances for remote auditing. In: Proceedings of 35th IEEE Annual Computer Software and Applications Conference Workshops (2011)
8. ACPO: Good practice guide for computer-based electronic evidence. 7safe (August 2007), http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf
9. Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P., Lambrinoudakis, C.: Cryptography Goes to the Cloud. In: Lee, C., Seigneur, J.-M., Park, J.J., Wagner, R.R. (eds.) STA 2011 Workshops. CCIS, vol. 187, pp. 190–197. Springer, Heidelberg (2011)
10. Ando, R., Kadobayashi, Y., Shinoda, Y.: Asynchronous Pseudo Physical Memory Snapshot and Forensics on Paravirtualized VMM Using Split Kernel Module. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 131–143. Springer, Heidelberg (2007)
11. Baliga, J., Ayre, R.W.A., Hinton, K., Tucker, R.S.: Green cloud computing: Balancing energy in processing, storage, and transport. Proceedings of the IEEE 99(1), 149–167 (2011)
12. Barrett, D., Kipper, G.: Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments. Syngress Media, Syngress/Elsevier (2010), http://books.google.at/books?id=QXF1kKX2za8C
13. Beebe, N., Beebe, N.: Digital forensic research: The good, the bad and the unaddressed. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics V. IFIP AICT, vol. 306, pp. 17–36. Springer, Boston (2009)
14. Biggs, S., Vidalis, S.: Cloud computing: The impact on digital forensic investigations. In: Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST) 2009, London, pp. 1–6 (November 2009)
15. Birk, D.: Technical challenges of forensic investigations in cloud computing environments. In: Proceedings of the Workshop on Cryptography and Security in Clouds, pp. 1–6 (March 2011)
16. Birk, D., Wegener, C.: Technical issues of forensic investigations in cloud computing environments. In: Proceedings of the 6th International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA (2011)
17. Brezinski, D., Killalea, T.: Guidelines for evidence collection and archiving. RFC 3227 (Best Current Practice) (2002)
18. Carlton, G.H., Zhou, H.: A survey of cloud computing challenges from a digital forensics perspective. International Journal of Interdisciplinary Telecommunications and Networking 3(4), 1–16 (2011)
19. Carrier, B.D., Spafford, E.H.: Getting physical with the digital investigation process. International Journal of Digital Evidence 2(2), 1–20 (2003)

20. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press (2011), `http://books.google.at/books?id=6gCbJ4O4f-IC`
21. Chow, R., Golle, P., Jakobsson, M., Masuoka, R., Molina, J.: Controlling data in the cloud:outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009), pp. 85–90. ACM (November 2009)
22. Cohen, F.: Digital Forensic Evidence Examination - 2nd Edn. Fred Cohen & Associates (2010)
23. Cohen, M., Bilby, D., Caronni, G.: Distributed forensics and incident response in the enterprise. Digital Investigation 8(suppl.), S101–S110 (2011)
24. Dean, J., Ghemawat, S.: Mapreduce: Simplified data processing on large clusters. In: Proceedings of the 6th Symposium on Operating Systems Design and Implementation. USENIX (2004)
25. Delport, W., Olivier, M.S., Koehn, M.: Isolating a cloud instance for a digital forensic investigation. In: Proceedings of the 2011 Information Security for South Africa (ISSA 2011) Conference (2011)
26. Dillon, T.S., Wu, C., Chang, E.: Cloud computing: Issues and challenges. In: Proceedings of the International Conference on Advanced Information Networking and Applications (AINA 2010), pp. 27–33 (2010)
27. Flaglien, A.O., Mallasvik, A., Mustorp, M., Arnes, A.: Storage and exchange formats for digital evidence. Digital Investigation 8(2), 122–128 (2011); standards, professionalization and quality in digital forensics
28. Foster, I.T., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. Computing Research Repository abs/0901.0131, 1–10 (2009)
29. Garfinkel, S.L.: Digital forensics research: The next 10 years. Digital Investigation 7(suppl. 1), S64–S73 (2010); the Proceedings of the Tenth Annual DFRWS Conference
30. Garfinkel, T., Rosenblum, M.: A virtual machine introspection based architecture for intrusion detection. In: Proceedings of the Network and Distributed System Security Symposium (NDSS 2003). The Internet Society (2003)
31. Gartner: Gartner says worldwide cloud services market to surpass $68 billion in 2010 (2010), `http://www.gartner.com/it/page.jsp?id=1389313` (accessed: December 30, 2011)
32. Grispos, G., Glisson, W.B., Storer, T.: Calm before the storm: The emerging challenges of cloud computing in digital forensics (August 2011), `http://www.dcs.gla.ac.uk/~tws/papers/grispos11calm-rev2425.pdf`, draft published for comment
33. Hegarty, R., Merabti, M., Shi, Q., Askwith, B.: Forensic analysis of distributed service oriented computing platforms (June 2011)
34. Karen, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response, recommendations of the National Institute of Standards and Technology (2006)
35. Kazarian, B., Hanlon, B.: SMB Cloud Adoption Study,- Global Report (December 2010), `http://www.microsoft.com/Presspass/presskits/commsector/docs/SMBStudy_032011.pdf` (accessed: December 30, 2011)
36. Ke, L.: Design of a Forensic Overlay Model for Application Development. Master's thesis, University of Canterbury, College of Engineering (2011)
37. Kourai, K., Chiba, S.: Hyperspector: virtual distributed monitoring environments for secure intrusion detection. In: Hind, M., Vitek, J. (eds.) Proceedings of the

1st International Conference on Virtual Execution Environments (VEE 2005), pp. 197–207. ACM (2005)

38. Krishnan, S., Snow, K.Z., Monrose, F.: Trail of bytes: efficient support for forensic analysis. In: Al-Shaer, E., Keromytis, A.D., Shmatikov, V. (eds.) Proceedings of ACM Conference on Computer and Communications Security (ACM CCS 2010), pp. 50–60. ACM (2010)
39. Krutz, R., Vines, R.: Cloud Security: A Comprehensive Guide to Secure Cloud Computing. John Wiley & Sons (2010), http://books.google.at/books?id=cs6Ox4CHXioC
40. Kuhn, S., Taylor, S.: A survey of forensic analysis in virtualized environments. Tech. rep., Dartmouth College, Hanover, New Hampshire (2011)
41. Sandia National Laboratories: Libvmi (2011), http://vmitools.sandia.gov/libvmi.html (online; Status: January 09, 2012)
42. Lempereur, B., Merabti, M., Shi, Q.: Pypette: A framework for the automated evaluation of live digital forensic techniques. In: Proceedings of the 11th Annual PostGraduate Symposium on The Convergence of Telecommunications Networking and Broadcasting (2010), http://www.cms.livjm.ac.uk/pgnet2010/MakeCD/index.htm
43. Lillard, T., Garrison, C., Schiller, C., Steele, J., Murray, J.: Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data. Elsevier (2010), http://books.google.at/books?id=A4V45b2w27gC
44. Lu, R., Lin, X., Liang, X., Shen, X.S.: Secure provenance: the essential of bread and butter of data forensics in cloud computing. In: Feng, D., Basin, D.A., Liu, P. (eds.) Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010), pp. 282–292. ACM (2010)
45. Marsico, C.V.: Computer evidence v. daubert: The coming conflict. Cerias tech report 2005-17, Center for Education and Research in Information Assurance and Security, Purdue University (2005)
46. Marty, R.: Cloud application logging for forensics. In: Chu, W.C., Wong, W.E., Palakal, M.J., Hung, C.C. (eds.) Proceedings of the 2011 ACM Symposium on Applied Computing (SAC), pp. 178–184. ACM (2011)
47. Mason, S., George, E.: Digital evidence and "cloud" computing. Computer Law & Security Review 27(5), 524–528 (2011)
48. Mell, P., Grance, T.: The nist definition of cloud computing (September 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
49. Miller, R.: Outage in dublin knocks amazon, microsoft data centers offline (2011), http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/
50. Payne, B.D., Lee, W.: Secure and flexible monitoring of virtual machines. In: Proceedings of 23rd Annual Computer Security Applications Conference (ACSAC 2007). pp. 385–397. IEEE Computer Society (2007)
51. Pollitt, M.: Blue skies and storm clouds. Journal of Digital Forensic Practice 2(2), 105–106 (2008)
52. Pollitt, M.M.: An ad hoc review of digital forensic models. In: Proceedings Second Int. Workshop Systematic Approaches to Digital Forensic Engineering SADFE 2007, pp. 43–54 (2007)
53. Reilly, D., Wren, C., Berry, T.: Cloud computing: Forensic challenges for law enforcement. In: Proceedings of International Conference for Internet Technology and Secured Transactions ICITST 2010, pp. 1–7. IEEE (2010)

54. Richard, G.G., Roussev, V.: Next-generation digital forensics. Communications of the ACM 49, 76–80 (2006), http://doi.acm.org/10.1145/1113034.1113074
55. Roussev, V., Richard, G.G.: Breaking the performance wall: The case for distributed digital forensics. In: Proceedings of the 2004 Digital Forensics Research Workshop, DFRWS 2004 (2004)
56. Roussev, V., Wang, L., Richard, G.G., Marziale, L.: Mmr: A platform for large-scale forensic computing. In: Proceedings of the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics (2009)
57. Ruan, K., Baggili, I., Carthy, J., Kechadi, T.: Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. In: Proceedings of the 2011 ADFSL Conference on Digital Forensics, Security and Law (2011)
58. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics: An overview. Advances in Digital Forensics 7, 35–49 (2011)
59. Starcher, G.: Accessdata dna & amazon ec2 (2011), https://www.georgestarcher.com/?tag=amazon-ec2
60. Talbot, J., Yoo, R.: The phoenix system for mapreduce programming, http://mapreduce.stanford.edu/ (accessed: December 30, 2011)
61. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R.: Digital evidence in cloud computing systems. Computer Law & Security Review 26(3), 304–308 (2010)
62. Taylor, M., Haggerty, J., Gresty, D., Lamb, D.: Forensic investigation of cloud computing systems. Network Security 2011(3), 4–10 (2011)
63. Wang, K.: Using a local search warrant to acquire evidence stored overseas via the internet. In: Chow, K.P., Shenoi, S. (eds.) Advances in Digital Forensics VI. IFIP AICT, vol. 337, pp. 37–48. Springer, Boston (2010), http://dx.doi.org/10.1007/978-3-642-15506-2_3
64. Wang, Y., Cannady, J., Rosenbluth, J.: Foundations of computer forensics: A technology for the fight against computer crime. Computer Law & Security Review 21(2), 119–127 (2005)
65. Wolthusen, S.D.: Overcast: Forensic discovery in cloud environments. In: Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics, DC, USA, pp. 3–9 (2009)
66. Zimmerman, S., Glavach, D.: Cyber forensics in the cloud, the newsletter for information assurance technology professionals volume 14(1) (2011), http://iac.dtic.mil/iatac
67. Zonenberg, A.: Distributed hash cracker: A cross-platform gpu-accelerated password recovery system. Tech. rep., Rensselaer Polytechnic Institute (2009)