Cloud Computing and Conflicts with Digital Forensic Investigation

[1]Mohsen Damshenas, [2]Ali Dehghantanha, [3]Ramlan Mahmoud, [4]Solahuddin bin Shamsuddin
[1, 2, 3] Faculty of Computer Science and Information Technology, University Putra Malaysia
Damshenas@gmail.com, {alid, ramlan}@fsktm.upm.edu.my
[4] Cyber Security Malaysia,
solahuddin@cybersecurity.my

Abstract

Unfortunately, the nature of the cloud is in conflict with the characteristic of digital forensic investigation approach since many of the common forensic steps are not possible to follow during the inspection of the case. The distribution of cloud resource location in different countries, utilization of numerous storage devices and very limited physical access to the low-level storage devices and physical memories are just some of the reasons caused this conflict. This paper proposes some basic, yet useful, solutions to conquer the described issues. Implementing multi-factor authentication, utilizing Trusted Platform Module (TPM) in Hypervisor and applying specific changes in the Cloud Service Provider (CSP) contract to provide persistent storage to the customer are parts of suggested approaches, capable of making the current digital forensic investigation practices applicable to the cloud computing environments. This is an absolutely essential requirement for CSP's mainly due to the significance of the clients' trust which demands the ability for being investigated.

Keywords: security; forensics investigation; forensic issue; cloud computing; virtualization;

1. Introduction

NIST, the National Institute of Standards and Technology, defined cloud computing as “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” [1]. Moreover, cloud computing consist of three main models namely IaaS, PaaS, SaaS. The major difference between these models is the user access policy and the way this access become possible; IaaS provides an infrastructure such as a Virtual Machine so the user feels using a real machine on the cloud with all the flexibility a real machine has. PaaS offers a platform for the user's further development which usually is an Application Programming Interface (API). SaaS, as the most limited model, only provides a ready-made system for cloud clients with the least possible access to the cloud while usually the interface can be as simple as a web browser [2].TechNavio [3] report values the Global Cloud Security Software market at US$241 million for 2010 and forecasts the increase up to US$963.4 million in 2014; with the growth rate of %14.4. Knowing the rapid movement of businesses and organizations toward using cloud computing, to take advantage of its eyes catching benefits, the stream of cyber

doi:10.4156/jdcta.vol7.issue9.65

intrusions intensified dramatically as the result of malevolent interest of digital data thefts to these assets of organizations.

Knowing the security risk threatening the cloud computing, the main issue here is not the security of cloud computing as plenty of security organizations such as TrendMicro© have proposed variety of solutions for it; but more about how to investigate the digital crime scene in a forensically sound manner as the cloud computing environment nature is in direct conflict with typical Digital Forensic Investigation (DFI) approaches. Unfortunately with the massive investment on the cloud computing industry [4], so far according to the knowledge of the authors, there is no up to the minute and compatible DFI framework to accomplish forensics investigation. Considering the high demand of the cyber world to DFI studies, doing research on this are requires mastering two main involved areas namely DFI and cloud computing. In this Paper, we propose some simple yet absolutely feasible solutions to help digital forensic investigators conquer the current cloud investigation challenges. In section 2, the necessary literature of the cloud computing and digital forensic investigation approaches will be discussed as well as the difficulties that investigators face while investigation cloud computing cases. Furthermore, in section 3 the proposed model to address abovementioned challenges will be illuminated and analyzed.

2. Literature Review

The section explains necessary digital forensic investigation concepts and associated challenges with cloud computing in more details. We will discuss issues in evidence collection and preservation as these topics are the most challenging stages of digital forensic investigation process; the final section would be the existing issues of cloud computing digital forensic investigation.

2.1. Common Digital Forensic Practices

RFC 3227, Guidelines for Evidence Collection and Archiving [5], [6], provides a basic guideline for collecting digital evidences. Identifying suspicious devices which might contain digital evidences is the very first stage of an investigation (regardless of usual forensic investigations ethics such as earning suitable search and seize warrant). After identification of the target devices, while the crime scene is precisely protected from any threat to the integrity of the evidence, obtaining appropriate order of volatility is vital. The order of volatility is the order in which sensitivity of potential evidence are prioritized (i.e. CPU register, RAM, running processes, network connections, system settings and hard disk). Utilizing proper tools to collect evidences is the next step which involves knowing variety of tools developed for different platforms and tasks. Below are some of the suggested tools in the guideline:

- Programs to examine processes (e.g., ‘ps’ and ‘tasklist’)
- Programs to examine the system state (e.g., ‘uname’, ‘ver’, ‘netstat’, ‘ifconfig’, ‘ipconfig’, ‘iwconfig’, ‘arp’ and ‘route’)

- Programs to create a bit to bit copy of available memories on the target machine (e.g., ‘dd’)
- Programs to generate hash checksum of the image (e.g. ‘md5sum’, ‘sha1sum’, ‘dd’)

It is vital to note that digital evidence collection from a live system is different from a powered-off system. Collecting digital evidences from a live machine involves collecting data at rest, in execution and in motion. Investigating such systems is utterly sensitive because preserving data in volatile memory can be compromised by any power cottage. The most necessary action in such investigations is to create a forensic image of all volatile memories with minimum change in the memory [7], [8]. Once the forensic imaging is done, the integrity of the image should be verified by generating and comparing the hash checksum of the storage device and the image. The generated image then can be duplicated for being analyzed [9]. The last stage of the digital forensic investigation guideline covers documentation and reporting of every detail of the investigation. At this section, there would be a demand for producing the temporal analysis (time-line analysis) which basically is the time map of the incident. Generating temporal analysis strongly requires the recording of the system clock relativity through observing the evidences time stamps (i.e. every file has a time stamp saved as metadata). In continue, to preserve the chain of custody, it is indicated that only a known reliable medium should be used to store the evidence; and the evidence should be kept in a safe place while only specific persons will get access to it. Meanwhile, all permitted accesses should be logged and documented for the final report [5], [10], [11]. Figure 1 indicates the common digital forensic approach.

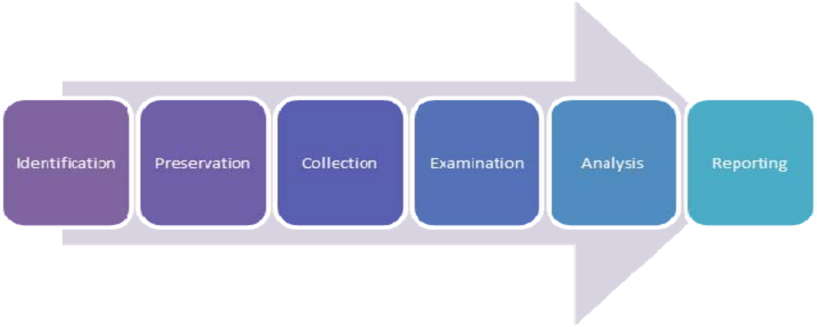

Figure 1. The general digital forensic investigation approach

2.2. Conflicts of Cloud Computing with Digital Forensic Investigation

Now that the common digital forensic investigation approaches are illuminated, in continue the conflicts of these techniques with cloud computing environment will be discussed in detail. For instance, preserving the original evidence is not applicable because the data might be stored in different servers and the storage device that contains the evidence is also being used by many other cloud clients [12]. Table 01 indicates an overview of the known challenges in cloud computing.

Cloud Forensic Issue	Stage

Access to the tracks of the evidence on non-volatile memory	Identification
Access to volatile memory in Cloud	Identification
Accessing “date on rest” on the persistent storages	Identification
Securing the hard disk from further changes	Identification
Obtaining evidence from client side	Identification
Seizing the physical evidence	Collection
Generating forensic image of the evidence	Collection
Recovery of deleted files and cloud privacy policies	Collection
Verification of virtual machine manager integrity	Collection
User claiming that his credentials were stolen	Preservation
Wiping user data after contract is finished	Preservation
Third party access to the evidence	Preservation
Analyzing petabytes of data	Analysis
Failure to properly generate the temporal analysis	Analysis
Reconstruction of the crime scene	Reconstruction
Identifying the right jurisdiction	Reporting

Table 01: overview of the discussed challenges in cloud computing

2.2.1. Identification

Identifying potential evidences in “data in execution” demands for access to volatile memory (i.e. CPU register and physical memory) [13]. The very first issue of investigation of cloud based cases is inspecting resources which are not accessible to the client. This issue may cause failure in identifying system network status or running processes at the time. Again, this issue has minimum effect on IaaS clients as the investigator can simply use the virtual machine and access those resources. Another issue here, regardless of the access issue, is that the cloud service providers do not keep the clients data on the physical memory when the client`s session is closed. The reason might be to save resources from being wasted by data that are not in use. This problem get even worst in cases where the cloud service provider do not offer persistent storage device and all client`s data are stored on a volatile memory. Obviously, closing the session might cause major data loss and consequently loss of evidences. The situation can get even more complicated when the client intentionally close the session to hide his tracks of malicious activities [14].

Data in rest, which refers to the stored data in storage devices, may contain important evidences such as log files, metadata and configuration files. In this case, IaaS model investigation does not limit the investigator as it provides all accesses to persistent storages. Yet another issue rises during investigation of cloud models which do not provide full access to the employed persistent storages. Inspecting usual computer crimes would let the investigator to unplug the power supply of the system (after making an image of volatile memories), so the temporary files on the system would remain in the persistent storage; as proper shutdown of the system will definitely remove some cashed data. Retrieving temporary file automatically created by applications is a necessary step which cannot be done in PaaS and SaaS since the client access is absolutely restricted by the provided API of the cloud service provider or a simple limited interface [15], [16], [17]. Regarding the data in rest identification issues, not all evidences are in the cloud side of the crime; in fact there might be evidences at the client side which usually is missed to be identified. The reason could be the lack of proper logging capability in client side application [18].

2.2.2. Collection

Seizing the physical evidence is an inevitable action in forensic investigation; which is not feasible in cloud computing environments as the nature of the cloud (sharing resources) is in conflict with it. In order to seize the resources like hard disk that is used to commit the crime, the physical hard disk have to be collected and kept in a safe place; but due to the face that the hard disk is being used by numerous clients, it is not applicable. In addition, the client's data might even be distributed in different hard disks of different servers which make it very hard track and seize all of them. Yet another problem rises here, that concerns the privacy of cloud's other clients. The problem is that seizing and inspecting the whole hard disk may lead to exposure of other clients' private data. Clearly, no organization accepts unauthorized access to their confidential data by a third party [16], [19], [20]. Furthermore, in forensic investigation as noted before, making a forensically sound image of the potential evidence is vital due to the demand of preserving the integrity of evidence and avoiding data lost. Obviously, creating a bit by bit image of a storage device require access to every single bit of the storage device that unfortunately is not offered in PaaS and SaaS cloud models. Accordingly, the investigator will not be able to access, identify and collect the evidence which leads to the loss of data in execution (i.e. data in physical memory) or in rest (i.e. data in hard disk). It is notable that the IaaS cloud model not only offers access to utilized storages devices, but it also provide the feature of snap shot which can help preserving the state of the machine [14], [21].

Additionally, recovering evidences is a necessary part of the evidence collection which can be interrupted by the storage policy of most of the cloud service providers. In computer forensic investigation the collection stage concerns about the deleted data and the approaches to recover the deleted data. As the forensic image of the storage device contains hidden partitions, lost data, slack spaces and other parts, it might be possible to recover the data if it is not over written. However, the cloud file system might overwrite the deleted file of a user by a file of another one. A simple calculation shows that with the very high rate of data travel on the cloud, there is a good chance of losing the data in rest located in slack space [17], [22]. And finally, compromised Virtual Machine Manager (VMM) is another issue in cloud forensic investigation process as VMM has the right to control and moderate virtual machines and their specified resources. Obviously, a compromised VMM can challenge the entire investigation by questioning the integrity of evidences as it has the access to add/update/delete any data on the virtual machine. Without a proof to the integrity of the VMM, all the evidences on the virtual machine can be considered as compromised [17], [23].

2.2.3. Preservation

One of the most common challenges of investigators in preserving the evidence is that the malicious client can ignore any connection to the crime. Basically, this issue is rooted in the nature of digital environments as the discovered evidence is not directly related to the client and the only connection might be the logs proving that the client has been logged in; however in the case of cloud computing, the client can even deny the logs by claiming that his authentication credentials were taken and used for malicious activities [21], [24]. Yet another issue of collecting evidence in cloud environment might be the capability of a malicious cloud client to compromise the evidences. If the client himself uses the cloud for malicious purposes, according to the provided service policy it can be possible for the client to finish the contract which will force the CSP to wipe all clients' data immediately. The behavior of CSP facing such situations (finished contracts) is one of the challenges caused mainly due to the clients' privacy conflicts with keeping clients' data after the contract is finished [14], [17], [25]. Furthermore, one more common issue in preserving the evidence is the possibility of access from a third party, regardless of being human or machine. Investigating cloud computing carries the challenge of preserving the evidence while the cloud service provider or the hypervisor (the virtualization software that allow multiple operating systems running on a computer at the same time) is able to access data as a third party. Therefore, in order to prove the integrity of the evidence, the trustworthiness of the hypervisor or cloud service provider should be assured [22].

2.2.4. Analysis

The main challenge in analyzing evidences in cloud environment rises due to the nature of the cloud computing. Utilizing huge amount of resources in cloud computing, make the complicated time consuming task of analyzing even more complicated and time consuming. A cloud can utilize Petabytes volumes of storage devices which require very accurate low level inspection; which even for computer aided analysis it takes very long time [26], [27]. Moreover, generating the temporal analysis of the case is one of the necessary primary tasks required for reconstruction and reporting of the investigation. In cloud computing environment this task becomes a serious challenge for the inspectors as the cloud do not provide sufficient access to investigators. This restriction leads to the failure of regenerating the logical sequence of event; as it strictly requires discovering data provenance of files involved in the crime. Notably, the IaaS cloud model provides sufficient access for investigators to extract time-stamp of the files from their meta-data [21].

2.2.5. Reconstruction

This step of investigation helps to logically recreate the crime scene for the court of law; while it requires identifying the exact location and time of the incidents according to the temporal analysis. Unfortunately, in case of cloud computing the identified time or even the location might be relative mainly due the nature of the cloud. The cloud environment consists on widely distributed resources in term of time zone and location; which may cause difficulties in putting all pieces of the incidents together to generate a big picture of the committed crime [18], [28].

2.2.6. Reporting

One of the challenges of forensic investigator in this stage is choosing the right jurisdiction, which might be extra challenging in cloud computing investigation. Common forensic investigation practices suggests taking the case to the country in which the crime is happened; but the crime is distributed as the cloud is distributed. It means that the suspect could utilize shared resources and facilities in different locations to commit the crime [26], [29], [30]. This problem specifically disused in [24] as transition of data through the cloud where the data might be transferred across a number of countries when a person accesses the data. In the state of transition, the data might be stored in different devices it pass through or deleted after the process is done. These devices might reside in countries that share different judiciary system and possibly lengthen the process of digital investigation when a cloud-related cybercrime happened.

3. Proposed solution and analysis

Previously, most of significant conflicts of digital forensic investigation and cloud computer environments have been discussed. The big picture of these conflicts would clarify that most of these issues are deeply rooted in the weakness of common digital forensic investigation practices in dealing with new technologies; which are changing even on daily basis. The nature of these changes is the base of the technology so it requires basic alternation in the current digital forensic investigation approaches. In continue, some basic and simple suggestions are proposed which can help adapting and utilizing the current digital forensic investigation methods in investigation.

3.1. Identification

The first solution would concern the issue of storing data only on physical memory which causes data lost when the client’s session is expired, requires cloud service providers additional service. Regardless of the costs, providing persistent storage device for storing client’s data is absolutely vital. Implementing a persistent storage would bring the benefit of having a more reliable storage while it would be possible to recover data in case of data lost. Moreover, in case of a forensic investigation it would be feasible to identify the evidence even if the contract in finished and the data is erased from physical memory. Furthermore utilizing a persistent memory could lead to unsatisfactory of clients, regarding the privacy matters concerning the accessibility of data after the contract is finished. In such case, there should be noted in the contract that after specific time (i.e. one month) the data will be wiped securely while the data will be securely encrypted to prevent any unauthorized access.

On the other hand, solving the challenge of accessing to evidences in logs, which can solved in PaaS model by developing an additional API to be executed along the main API of every client. This API can log specific data and in case of an inspection, reveal the data in logs for the investigator. Meanwhile, in SaaS cloud model, the solution could be slightly more complicated in term of implementation as the client has the least access to the resources. Therefore, it is possible for cloud service provider to offer the feature of logging different types of data as long as it does not invade client’s privacy. Additionally, [31], [32] suggest using XML and formal methods to avoid privacy conflicts. Moreover, the proposed solution for the problem of identifying evidences on the client side of the cloud involves applying changes in the client side application. Depends on the cloud model used, it might be necessary to embed the functionality of saving the logs of the client’s activities. This feature is separate from operating system audit mechanism as it is going to be able to record specific data like login/logout time stamp of the client.

3.2. Collection

The challenge of creating a forensically sound imaged of the storage device was one of the basic problems in cloud environment forensic investigation as the accesses to storage devices are very limited expect the IaaS cloud model. Implementing a mechanism to record the track of all clients' accessed data can address this issue; while the recording process involves logging full address of the hard disk sectors by using a suitable addressing schema like Logical Block Addressing (LBA) or CPU registers addresses with their value of last access. Obviously, addressing method of different storage devices are varying on different platforms and choosing the proper addressing method is totally depends on the device and platform being used by cloud service provider. Having all these records, will make it feasible to make a bit by bit image of all addresses the client has accessed. On the other hand, to solve the issue of a compromised virtual machine manager or hypervisor which question the integrity of the evidence; it is applicable to integrate Trusted Platform Module (TPM) or even a virtual TPM as mentioned in [33], [34]. These security models insure the confidentiality of data by providing encryption (Needham-Schroeder public-key protocol for web authentication) and integrity of the data by proposing the concept of Security Aware Could (SAC).

3.3. Preservation

The proposed solution is embedding multi-factor authentication besides utilizing virtual private network with extra authentication which guarantee data integrity, confidentiality, authenticity and non-repudiation; this can simply benefit the investigator for preserving the evidence trustworthy by preventing the malicious client claims about a leaked authentication data. Especially the virtual tunneling over the internet can help preventing questioning the IP address or identical information of the client. Additionally, it is possible to use the previously proposed solution involving logging of the client side data. This way by referring to the logged data on the client side it would be revealed whether the client is trying to compromise the evidence usability by denying any connection. Addressing the issue of malicious cloud clients who try to compromise remained evidences by finishing the contract; as briefly mentioned before, demands for keeping client's related data (i.e. logs or documents) for a period of time after the contract finished. Besides, dealing with the privacy issues of this solution, it is possible to encrypt client's data securely and keep data only for specific period of time according to the contract and service provider's policy.

3.4. Analysis

Regarding the issue of analyzing vast amount of data, which is actually one of the advantages of cloud, the new approach of using a parallel digital forensics system (PDF) for terabyte size data sets can help the analyzing and even imaging of the huge data size possible. In this method which is proposed by "L.M. Liebrock" [35], PDF can break up the analyzing process into two or even more parallel processes. Imaging the RAID drives for simultaneous analysis, utilizes a parallel end-pint device to increase the string analysis of the images. Moreover, as the rate and amount of transaction to save and retrieve the information of the discovered evidences might be extremely high, this method uses a light weight with high performance database. In order to solve the "Identifying time-stamp" issue of cloud computer investigation challenges, it is feasible to log all normal meta-data in a separate file, instead of the usual header file. This provides clients' privacy as each user only can see the related records of the client; full meta-data of the file which contains all clients' records that can be retrieved later by the client's request.

3.5. Reconstruction

This solution comes from the very basic idea of using a global timing system like GMT as a standard which has to be used in all cloud resources, traffics and log files. Being able to recreate the event based on the time pattern generated is an advantage of implementing this idea. It might even being used in generating the time-line analysis itself as the problem could be conquered better if the temporal analysis of the even follows a standard time. Obviously, tracking and recreating the events happened on different locations with different time zones can make the process too complicated. This rule should also be applied to virtual machines in some way, or else all the evidences timing should be converted to the specified timing pattern.

3.6. Reporting

A research conducted in [24] provided a solution for the issue of different jurisdiction; as demonstrated on how to perform investigation based on the judicial system in the United Kingdom and how to obtain evidence from other jurisdictions as well. As a conclusion, the legislation is urged to consider that evidence obtained from the cloud environment should be admissible due to the popularity of cloud computing.

4. Conclusion and future works

Obtaining digital evidence in cloud computing, analyzing the evidence, choosing the right court to take the case and the privacy of clients are some of the main issues of cloud computing forensic investigation. This paper discussed about the concept of cloud computing, as well as forensic investigation practices; knowing both, brings the cloud forensic investigation issues to light. This article illuminated some of the conflicts of digital forensic investigation and cloud environment; and then continued with discussing some of the possible solution. Most of the issues of investigating in cloud environment such as security of data in cloud, privacy concerns of clients and hardships of investigators during identification of the evidence can be solved by providing a standard cloud deployment framework for cloud service providers to follow while developing and setting up the cloud services.

References

[1] P. Mell and T. Grance, "The NIST Defnition of Cloud Computing." NIST Special Publication, 2011.

[2] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, 2012, pp. 877 –880.

[3] "Global Market Share Report: Trend Micro #1 in Cloud Security," *Trend Micro*. [Online]. Available: http://www.technavio.com/content/global-web-security-market-2011-2015. [Accessed: 06-Jul-2012].

[4] T. Pan and L. Zheng, "Trust Network Modeling for Virtual Enterprise Cloud Manufacturing," *JDCTA: International Journal of Digital Content Technology and its Applications*, vol. 6, no. 5, pp. 115–123, 2012.

[5] D. Brezinski and T. Killalea, "Guidelines for Evidence Collection and Archiving." [Online]. Available: http://www.ietf.org/rfc/rfc3227.txt. [Accessed: 07-Jul-2012].

[6] W. Harrison, "The Digital Detective: An Introduction to Digital Forensics," in *Advances in Computers*, vol. Volume 60, Elsevier, 2004, pp. 75–119.

[7] J. Okolica and G. L. Peterson, "Windows operating systems agnostic memory analysis," *Digital Investigation*, vol. 7, Supplement, pp. S48 – S56, 2010.

[8] B. D. Carrier and J. Grand, "A hardware-based memory acquisition procedure for digital investigations," *Digital Investigation*, vol. 1, no. 1, pp. 50–60, Feb. 2004.

[9] W. S. van Dongen, "Case study: Forensic analysis of a Samsung digital video recorder," *Digital Investigation*, vol. 5, no. 1–2, pp. 19 – 28, 2008.

[10] E. E. Kenneally and C. L. T. Brown, "Risk sensitive digital evidence collection," *Digital Investigation*, vol. 2, no. 2, pp. 101–119, Jun. 2005.

[11] L. E. Daniel and L. E. Daniel, "Chapter 4 - The Foundations of Digital Forensics: Best Practices," in *Digital Forensics for Legal Professionals*, Boston: Syngress, 2012, pp. 25–32.

[12] M. Damshenas and A. Dehghantanha, "Forensics Investigation Challenges in Cloud Computing Environments," presented at the The International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Kuala Lumpur, Malaysia, 2012.

[13] J. Wang, F. Zhang, K. Sun, and A. Stavrou, "Firmware-assisted memory acquisition and analysis tools for digital forensics," *Proceedings of the Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2011.

[14] C. Yan, "Cybercrime forensic system in cloud computing," in *Image Analysis and Signal Processing (IASP), 2011 International Conference on*, 2011, pp. 612 –615.

[15] D. Bem, "Virtual Machine for Computer Forensics – the Open Source Perspective," in *Open Source Software for Digital Forensics*, E. Huebner and S. Zanero, Eds. Springer US, 2010, pp. 25–42.

[16] S. Ahmed and M. Y. A. Raja, "Tackling cloud security issues and forensics model," in *High-Capacity Optical Networks and Enabling Technologies (HONET), 2010*, 2010, pp. 190 –195.

[17] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on*, 2011, pp. 1 –10.

[18] H. Guo and B. Jin, "Forensic Investigations in Cloud Environments," presented at the International Conference on Opto-Electronics Engineering and Information Science (ICOEIS 2011), Xi'an, China, 2011.

[19] A. Dehghantanha and A. Seddon, "Investigating Privacy Issues in Forensics Investigation," *International Journal of Computational Intelligence and Information Security*, vol. 2, no. 11, pp. 27–31, Nov. 2011.

[20] K. Zhang, Q. Li, and Y. Shi, "A Novel Non-Deterministic Data Privacy Preservation Mechanism for Software as a Service," *JDCTA: International Journal of Digital Content Technology and its Applications*, vol. 6, no. 7, pp. 181–189, 2012.

[21] S. Biggs and S. Vidalis, "Cloud Computing: The impact on digital forensic investigations," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2009, pp. 1 –6.

[22] G. C. Kessler, "Anti-Forensics and the Digital Investigator," in *5th Australian Digital Forensics Conference*, Mt. Lawley, Western Australia, 2007.

[23] Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," *Journal of Systems and Software*, vol. 85, no. 5, pp. 1083–1095, May 2012.

[24] S. Mason and E. George, "Digital evidence and 'cloud' computing," *Computer Law &amp; Security Review*, vol. 27, no. 5, pp. 524 – 528, 2011.

[25] C. Wright, D. Kleiman, and S. Sundhar R.S., “Overwriting Hard Drive Data: The Great Wiping Controversy,” in *Proceedings of the 4th International Conference on Information Systems Security*, Berlin, Heidelberg, 2008, pp. 243–257.

[26] D. Reilly, C. Wren, and T. Berry, “Cloud computing: Forensic challenges for law enforcement,” in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, 2010, pp. 1 –7.

[27] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, “Forensic investigation of cloud computing systems,” *Network Security*, vol. 2011, no. 3, pp. 4 – 10, 2011.

[28] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, “Digital evidence in cloud computing systems,” *Computer Law &amp; Security Review*, vol. 26, no. 3, pp. 304 – 308, 2010.

[29] S.-J. Wang, D.-Y. Kao, and F. F.-Y. Huang, “Procedure guidance for Internet forensics coping with copyright arguments of client-server-based P2P models,” *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 795–800, Jun. 2009.

[30] H. Chung, J. Park, S. Lee, and C. Kang, “Digital forensic investigation of cloud storage services,” *Digital Investigation*.

[31] A. Dehghantanha, “Formal Methods for Analyzing Privacy Policies: Techniques for Formal Representing, Analyzing, and Processing Privacy Policies,” 2011.

[32] A. Dehghantanha, N. I. Udzir, and R. Mahmod, “Towards a pervasive formal privacy language,” in *Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on*, 2010, pp. 1085–1091.

[33] H. Sato, A. Kanai, and S. Tanimoto, “A Cloud Trust Model in a Security Aware Cloud,” in *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*, 2010, pp. 121 –124.

[34] D. Liu, J. Lee, J. Jang, S. Nepal, and J. Zic, “A Cloud Architecture of Virtual Trusted Platform Modules,” in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 804 –811.

[35] L. M. Liebrock, N. Marrero, D. P. Burton, R. Prine, E. Cornelius, M. Shakamuri, and V. Urias, “A preliminary design for digital forensics analysis of terabyte size data sets,” in *Proceedings of the 2007 ACM symposium on Applied computing,* New York, NY, USA, 2007, pp. 190–191.