Forensics Investigation Challenges in Cloud Computing Environments

[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

Cloud computing discusses about sharing any imaginable entity such as process units, storage devices or software. The provided service is utterly economical and expandable. Cloud computing attractive benefits entice huge interest of both business owners and cyber thefts. Consequently, the "computer forensic investigation" step into the play to find evidences against criminals. As a result of the new technology and methods used in cloud computing, the forensic investigation techniques face different types of issues while inspecting the case. The most profound challenges are difficulties to deal with different rulings obliged on variety of data saved in different locations, limited access to obtain evidences from cloud and even the issue of seizing the physical evidence for the sake of integrity validation or evidence presentation. This paper suggests a simple yet very useful solution to conquer the aforementioned issues in forensic investigation of cloud systems. Utilizing TPM in hypervisor, implementing multi-factor authentication and updating the cloud service provider policy to provide persistent storage devices are some of the recommended solutions. Utilizing the proposed solutions, the cloud service will be compatible to the current digital forensic investigation practices; alongside it brings the great advantage of being investigable and consequently the trust of the client.

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

I. INTRODUCTION

Nowadays, organizations are learning the benefits of cloud computing and moving toward transferring their data to the cloud; which gains cyber thefts' interest to the cloud resources with a higher level of endangerment. A recent FBI research indicates that the size of the average digital forensic case is growing at the rate of 35% per year indicates the wild increase in digital crimes [1]. Thus, this is absolutely significant to pay more attention to cloud computer security and consequently cloud computing forensic investigation. Obviously, in order to discuss about the digital forensic investigation and cloud systems, having a basic knowledge of both area is crucial.

Cloud Computing as defined by the US National Institute of Standards and Technology (NIST) 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" [5]. The cloud computing with current technologies, involved three common models of services as — Infrastructure as a Service (IaaS) which provides a virtualized machine (an environment like a physical machine but with some limitations) to the clients, — Platform as a Service (PaaS) that usually provide an Application Programming Interface (API) to the client so it will be possible to utilize the API and develop customized applications; and — Software as a Service (SaaS) with providing an interface (usually web based) to the client for using the intended service [2].

Unfortunately, the current forensic investigation practices do not match the cloud computing characteristics. This paper will discuss the forensics aspects of cloud computing by pointing out the forensic investigation issues in cloud computing and recommending solutions to the problems. By doing so, forensic investigators are able to conduct forensics investigations on cloud computing machines with higher accuracy and integrity. This paper is organized as follow: A deep literature of current status cloud forensic standards and issues in section 2. In section 3 a model is proposed to address clarified difficulties, while the proposed model's analysis discussed in the same section.

II. LITERATURE REVIEW

The section clarifies involved topics related to forensic investigation issues in cloud environments in details. We will discuss evidence collection techniques, then evidence preservation and finally current challenges of cloud digital forensic.

978-1-4673-1677-4

A. Digital Forensic Investigation

According to RFC 3227 [7], collecting digital evidences, at the very first step, requires identification of all machines suspicious of containing related evidence. Once the target machine detected, the task is to obtain pertinent order of volatility and then protect the area from any change that might affect the evidence. Going along order of volatility, collect potential evidences with appropriate tools depends on the operation system architecture. The next stage would be recording the machines clock drift, which will be used to generate temporal analysis of the incident; and finally documentation and reporting. Temporal analysis or Time-Line analysis is the logical sequence of incidents that leads to the crime.

On the other hand, collecting digital evidences can be done from a live system, which contains data in motion, data at rest and data in execution, or from a storage device or a powered-off system, which usually contains data on rest. The important point in investigating live systems is to preserve volatile information, which can be found in storage Medias that any power disturbance will lead to complete loss of data. The first step in investigating a storage media is to connect it to a forensic system which mounts the media as read-only. Afterward, making a forensic image of the storage media. Imaging a storage device is different from copying the content as the imaging will make an exactly same bit-by-bit copy of the content. The next important stage is to check the integrity of the image through hash checksum generation. In continue, preserving the original evidence, mounting the forensic image and finally investigation of the image [6].

Preservation of the digital evidence is an utterly vital task, as it defines the effect of the evidence in the court of law. Obviously, the integrity check of altered evidence is condemned to failure, simply because the court of law strictly measures the evidence to make sure it is not fake and not just made by the investigator [4]. RFC 3227 [7], strictly indicates that the evidence have to be archived in a secure manner according to the specified procedure while the chain of custody is clearly documented. Preferably, use a trustable archiving medium instead of a vague device never used before. Moreover, the evidence has to be stored in safe place with strict access control to the location of the evidence, while all granted accesses should be logged [7].

B. Challenges of Forensic Investigations in Cloud Computing Environments

By knowing the usual digital forensic investigation practices, now, it is vivid that the nature of cloud computing is in direct conflicts with digital forensics investigation. Except in the IaaS cloud model that provides an environment logically similar to a machine, none of the programs and approaches for digital data collection is feasible for the cloud computing models. For instance, collecting the system processes and observing system status is not possible because SaaS and PaaS do not provide any access to the operation system commands. Based on the type of problem occurred in forensic investigation stage, the following are problems investigators face.

1) Identification

The distributed nature of cloud make identification of possible sources of evidences a comparatively difficult task. In this section we are making a deeper look on issues that investigators could face in this stage. Access to evidences in logs, is the first issue in evidence identification stage. Checking system status and log files are a part of collecting evidences, which is not feasible in SaaS and PaaS because the client access is completely limited to the API or the pre-designed interface. It is just partly applicable in IaaS cloud model as it provides the Virtual Machine which behave almost same as an Actual Machine [3].

Data loss in volatile storage is next challenge of forensic investigation when there is no evidence remains to be identified. Usually, the CSP does not provide a persistent storage media for the clients and all the clients' data is volatile unless the client request for additional package with higher cost; as the demand for storage is very high in cloud computing architectures. Such data storage policy in cloud computing may lead to loss of evidence in case the person who committed the crime restarts or force power-off the machine [11].

Client side evidence identification is another necessary step in computer forensic investigation that is usually not applicable especially in SaaS and PaaS models as there are always some vital parts of evidence data can be found on client side interface (e.g. web browser temp data). Depends on the type of the interface, it might be absolutely essential to collect these data due to the possibility of being sensitive evidence. The mentioned data usually get lost as the client side interface does not log and keep them properly [13].

2) Collection

Not only in computer forensic investigation, but in every forensic investigation methodology collecting evidence is a significantly vital task, which it is not completely feasible in cloud computing. In continue some of the challenges are pointed out.

Collecting evidence is the main issue in this step. Computer forensic investigation requires seizing the physical evidence in the collection stage. This is not possible due the sharing nature of the cloud. Every resource is shared simultaneously between numerous of cloud clients; apart from being used all the time, the privacy of other clients' data is another issue of seizing the physical evidence [8].

Making forensic image, one of the necessary steps of data collection, is to make bit-by-bit image of the storage Medias. Making a forensic copy of the system is not applicable for SaaS and PaaS as the client do not have any direct access to the storage media, which may lead to loss of data in rest, in motion and in execution. In case of IaaS model, using the snap-shot feature of the VM can help to freeze the status and investigate the system [22, 20].

Evidence integrity verification is another issue in cloud computing environments as it could be challenged by the chance of the data being compromised through the CSP or the hypervisor. Besides the possibility of the evidence being compromised after the integrity checksum has been generated, the Hypervisor has the ability to modify the hash checksum generation procedure [12].

3) *Preservation*

The evidence, in forensic investigation is the proof to a crime and any offence to the trustworthy or relation of the evidence can make it of no use. Usefulness of evidences: In cases that the client is involved with the malicious activities, it is possible for the client to claim that his/her authentication credentials were stolen and misused by other person. As the client can also connect to the cloud anonymously, there is no way to prove that the claim is wrong [9].

4) *Analysis*

Data analysis is another essential step of the forensic investigation; especially in computer forensic investigation it demands for a more delicate examination as the quantity of objects to be inspected is wildly increased. In cloud computing, this can be even called a disaster as the nature of the cloud computing involves utilization of massive amount of resources with a good chance of containing an evidence. This is an additional issue of cloud forensic investigation mainly due the limitations in processing and examining the vast data [10].

5) *Reconstruction*

Data reconstruction step of the forensic investigation produces different types of analyses. The digital forensic practices demands for generation of temporal analysis to logically recreate the crime, as part of data collection steps. In cloud computing, each piece of crime might have happened in separate country due to the nature of cloud computing which involves utilizing distributed and shared resources; this brings an issue which interrupt the generation of the temporal analysis since the time difference makes it hard to make the logical order of crimes took place [28].

6) *Reporting*

The last step, and the last challenge of forensic investigators involves in choosing the right court for reporting the case. In usual computer forensic investigation it is not difficult to decide about the court and the case would be brought to the court in the country in which the crime has been committed; but in distributed networks and particularly in cloud computing it is absolutely complicated due to the characteristic of the cloud computing. It is not clear that where the crime has committed and where evidences are physically located since usually the cloud resources are shared between multiple clients in multiple countries. This obviously confuses the investigator in deciding where and what legal system the suit should be heard [10].

III. PROPOSED SOLTION AND ANALYSIS

All the issues discussed before, are the result of the huge difference in cloud computing characteristic by the originally designed model, Single Personal Computer or Server. A new framework for computer forensic investigation, alone, cannot address all these issues; instead it demands for a framework for cloud computing. Some of the suggested keys for cloud computing framework and analysis are as follow.

1) *Identification*

In continue some of the proposed approaches to avoid challenges in identifying the evidence are discussed. As the first suggested solution for addressing the challenge of “Access to evidences in logs“, in PaaS cloud model, it is possible to prepare an API to extract relevant status data of the system, limited by the data related to the client only. In SaaS, depends on the interface, it might be possible to implement the feature to check the basic logs and status of the client's usage. All above features should provide read-only access only and demands for specific log and system status manager running as a cloud service. It is notable that the domain of provided data should be stated in the client-CSP contract.

In addition, to address the forensic investigation challenge described before as “Data loss in volatile storage”, no matter of the cost, it should be globalized between cloud service providers to offer persistent storage device for clients data; which will brings the advantage of data-safety and data-recovery opportunity for clients, and the ease of evidence collection from a forced powered-off cloud machine. On the other hand, to insure the clients' privacy of data, it should be indicated in the client-CSP's contract that for instance the clients data will be triple wiped after a week the contract finished. In addition, to insure the confidentiality of data it is possible to encrypt all users' data, so it will not be readable by unauthorized person.

Designing, implementing or configuring the client side application to log all potential evidences on the client's machine can be a solution for the issue described as "Client side evidence identification". The client side application which communicates with cloud services can be used to collect evidences as it might be a part of the crime. Built-in logging feature of sensitive data in client side application can help preserve potential evidences such as user communication logs and other sensitive data.

2) Collection

The solutions recommended here, are related to the challenges of the collection step in common computer forensic investigation methodology.

Regarding challenge of "Making forensic image", with current limitations of cloud computing and digital forensic investigation, it is not applicable to create a forensic copy of the storage media containing the evidence. Yet it might be possible to generate a track record of all clients' activities such as all file accesses, data transmission, live processes and any other useful forensic record with full physical address of the accessed area. Later on, to generate a forensic image of specific clients all it requires is to check the track record of the client and then copy bit-by-bit stream of all the area the client has accessed to. Obviously, the applicability of this approach mostly relies on the generation of the track record of the client, which can be implemented by the cloud.

3) Preservation

Following is the proposed solution for the problem clarifies as "Usefulness of evidences". Using multi-factor authentication methods plus cryptographic tunneling protocols such as Virtual Private Network (VPN) to authorize the client and guarantee the confidentiality and integrity of data can simply solve the challenge. Having a multi-factor authentication can prevent the user to claim about stolen authentication credentials. In the court of law, proving that the user account was not compromised and malicious activities have been done by the owner is not simple if the IP or other identical information has been faked.

4) Reconstruction

In continue, a simple solution is proposed to solve the issue mentioned before as "Data Reconstruction" challenge. Using a specific time system (e.g. GMT) on all entities of the cloud can simply address the challenge of different time zone as it brings the benefit of having a logical time pattern. This can be used later to demonstrate a time-line (temporal) analysis of a crime or even tracking multiple log records in different physical locations. In IaaS cloud models, the VM time is under the user's control; so all the date and times used in logs and other records should be converted to the specific time system.

IV. Conclusion and Future Works

The cloud computing with the pleasant offer of computer as service and not a product brought lots of hopes to companies and businesses with limited computing resources problems. Currently those hopes are realities thanks to Cloud Computing (CC) and Cloud Service Providers (CSPs). However, cloud computing nature do not allow many of computer forensic investigation practices to be done properly as it simply utilized variety of computing resources shared between numerous clients without sufficient access to logs and system status.

In this paper, we discussed challenges of cloud computing investigation and proposed solutions addressing clarified challenges. The common cause between all these challenges is mainly the lack of an inclusive global cloud computing standard, which leads to cloud security and privacy issues, absence of a proper cloud deployment framework and confusion of computer forensic investigators about collecting/preserving evidences in such environments. Furthermore, there is a huge demand for updating current computer forensic investigation methods, as the day by day technology improvements will make it completely out of day and useless in near future.

References

[1] Federal Bureau of Investigation (FBI), "Regional Computer Forensics Laboratory (RCFL)", Program Annual Report for Fiscal Year 2007, Washington, DC, 2008

[2] Ben Kepes, "Understanding the Cloud Computing Stack SaaS, Paas, IaaS", Diversity Limited, 2011, [URL] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

[3] Dominik Birk, Christoph Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments", Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE Sixth International Workshop on , vol., no., pp.1-10, 26-26 May 2011, [URL] http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=6159124

[4] ACPO E-Crime Working Group, "Good Practice Guide for Computer-Based Electronic Evidence", 7safe information security website, [URL] http://7safe.com /electronic_evidence/index.html

[5] Peter Mell, Timothy Grance, "The NIST Defnition of Cloud Computing", NIST Special Publication, Spetember 2011, [URL] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[6] Hyunsang Kim, Sangjin Lee, Jongin Lim, "Digital evidence collection process in integrity and memory information gathering", Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on , vol., no., pp. 236- 247, 7-9 Nov. 2005, [URL] http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=1592536

[7] Brezinski, .D, Killalea, .T, “Guidelines for Evidence Collection and Archiving”, RFC-3227/BCP-55, The Internet Engineering Task Force (IETF), Feburary 2002, [URL] http://www.ietf.org/rfc/rfc3227.txt

[8] Shaftab Ahmed, M. Yasin Akhtar Raja, “Tackling cloud security issues and forensics model”, High-Capacity Optical Networks and Enabling Technologies (HONET), 2010 , vol., no., pp.190-195, 19-21 Dec. 2010 [URL] http://ieeexplore.ieee.org /search/srchabstract.jsp?arnumber=5715771

[9] Stephen Biggs, Stilianos Vidalis, “Cloud Computing: The impact on digital forensic investigations”, Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for , vol., no., pp.1-6, 9-12 Nov. 2009, [URL] http://ieeexplore.ieee .org/search/srchabstract.jsp?arnumber=5402561

[10] Reilly .D, Wren .C, Berry .T, “Cloud computing: Forensic challenges for law enforcement”, Internet Technology and Secured Transactions (ICITST), 2010 International Conference for , vol., no., pp.1-7, 8-11 Nov. 2010 [URL] http://ieeexplore.ieee .org/search/srchabstract.jsp?arnumber=5678033

[11] Cheng Yan, “Cybercrime forensic system in cloud computing”, Image Analysis and Signal Processing (IASP), 2011 International Conference on , vol., no., pp.612-615, 21-23 Oct. 2011, [URL] http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber =6109117

[12] Gary C. Kessler, “Anti-Forensics and the Digital Investigator, Champlain College Burlington”, 5th Australian Digital Forensics Conference, December 2007, [URL] http://ro.ecu.edu.au/adf/1/

[13] Hong Guo, Shang, Bo Jin, “Forensic Investigations in Cloud Environments”, International Conference on Opto-Electronics Engineering and Information Science (ICOEIS 2011), December 23-25, Xi'an, China, 2011, [URL] http://www.asaas.org/ICOEIS2011/N774.pdf