Isolating a cloud instance for a digital forensic investigation.

Conference Paper · January 2011

Source: DBLP

CITATIONS
70

READS
1,413

3 authors, including:

Waldo Delport
University of Pretoria
4 PUBLICATIONS **85** CITATIONS
SEE PROFILE

Michael Kohn
Johannesburg Society of Advocates
9 PUBLICATIONS **348** CITATIONS
SEE PROFILE

Isolating a Cloud Instance for a Digital Forensic Investigation.

Waldo Delport
Information and Computer Security Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa
Email: wdelport@cs.up.ac.za

Martin S. Olivier
Information and Computer Security Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa
Email: molivier@cs.up.ac.za

Michael Köhn
Information and Computer Security Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa
Email: mkohn@cs.up.ac.za

***Abstract*—Cloud Computing is gaining acceptance and increasing in popularity. Organizations often rely on Cloud resources to effectively replace their in house computer systems. In a Cloud environment an instance is typically accepted to be a virtual system resource established within that Cloud. Multiple instances can be contained a single node. The Cloud itself consists of multiple nodes. The Cloud structure has no predefined or fixed boundaries.**

Digital Forensics (DFs) can be considered the science of finding a root cause of a particular incident. Isolating the incident environment is generally accepted within the Forensic Community to be an integral part of a Forensic process. We consider this isolation is also needed in a Digital Forensic Investigations (DFIs). The isolation prevents any further contamination or tampering of possible evidence.

In order to isolate the incident the Cloud instance is isolated. The node instance is effectively placed in a controlled environment to enable a controlled DF investigation to be conducted. This paper will introduce possible techniques to isolate these Cloud instances to facilitate an investigation. The techniques include, but are not limited to Instance Relocation, Server Farming, Address Relocation, Failover, Sandboxing, Man in the Middle (MITM) and Let's Hope for the Best (LHFTB). A discussion of each of these techniques will be given. This discussion will include a description of each techniques, the advantages and disadvantages of using the techniques and the visibility of the techniques.

***Index Terms*—Cloud Computing, Digital Forensic.**

I. Introduction

As long as people are involved there will be crime. The need for Digital Forensics exists because some of these crimes or other incident is taking place on computer system [1]. The introduction of clouds complicated the digital forensic process. There is a belief that a digital investigation a cloud can be difficult to do. The need to have formal and proven methods to conduct a digital investigation on a cloud became apparent.

As computer related technologies continuous to expand a logical expansion in online technologies was cloud computing [2]. Cloud computing enables service providers to provide virtual systems to their clients. It enables the service providers to maintain a large number of independent services in a single cloud infrastructure.

In a cloud an instance must be isolated when it becomes apparent that an incident happened on that particular instance. This isolated helps preserve the integrity of the evidence collected from the instance. One of the problems to preserve the integrity of an instance is an attribute of clouds [1]. In a cloud the data from instance may share the storage of multiple instances and may not be in a constant place in the cloud. To preserve the integrity of the evidence the location on the cloud must be known and must be protected from tampering and contamination. Another complexity is that other instances on the same node may belong to other users. Users expect at least availability and privacy of their instance provided by the service provider [3]. The Digital Forensic process must be done in a manner that will not result in the privacy of other instances being lost and the availability of the instance must be effected in the smallest manner possible.

This paper intends to introduce new techniques to isolate instances on a cloud. These techniques are Instance Relocation, Server Farming, Address Relocation, Failover, Sandboxing, MITM and LHFTB In Section 2 a brief description of Digital forensics is provided. It also provides information about Computer, Network and Cloud Forensics. Section 3 provides a description of Cloud Computing. In Section 4 we discuss why there is a need to isolate the instance on a cloud. Section 5 introduces the techniques to isolate an instances and compares them to each other. A summary and the conclusion are given in Section 6.

II. Digital Forensics

To define digital forensics one first needs to define forensics. Forensics is a formal and proven approach to the gathering of evidence and processing of a crime scene. Sometimes used in the court of law [4]. From this definition it can be said that digital forensics must be based on sound scientific methods and techniques. It can be added that digital forensic can aid in the court of law. The digital forensic process helps in answering the who, what, when, where and how of an investigation [1].

In a digital forensics process a live or dead analysis can be followed [1]. The normal computer forensic process uses dead analysis, in a dead analysis the system is turned off as soon as the examination team acquires it and images are made of

the storage mediums, the analysis is then conducted on the images [5]. The other approach is a live analysis where the computer is kept on and evidence gathered from the computer in the environment that is on the system. There are advantages and disadvantages of both. The main disadvantage of a dead analysis is the fact that some information may be lost because it is in a buffer or the RAM. The problem with a live analysis is that the evidence can be destroyed or modified without the intent to do so.

In order to obtain admissible evidence a well defined forensic process needs to be followed. Cohen [6] proposes a model for the digital forensic examination that consists of seven phases. The phases are Identification, Collection, Transportation, Storage, Examination and traces, Presentation and Destruction.

Identification : In the identification phase possible evidence is identified as evidence.

Collection : Once the evidence is identified it is collected. The integrity of the evidence must be preserved while the evidence is gathered.

Transportation : The collected evidence must be transported. The evidence is collected at a crime scene and the rest of the digital forensic examination will happen at a different location. The evidence is moved to an examination lab where there is the necessary equipment to do a digital forensic examination. The normal manner to ensure that the evidence integrity is kept is to copy the evidence and keep the original in a safe place and move the copy.

Storage : The digital forensic proses may be a lengthy process, while the examination is on-going or even done the evidence needs to be stored in a manner so that the evidence will not degrade and become inadmissible.

Examination and traces : The Examination and traces phase consist of four sub categories, they are Analysis, Interpretation, Attribution and Reconstruction [6]. The Examination phase will try to explain route of evidence, from creation to state it is in now. The last step is to try and create the same output from the original evidence.

Presentation : The next step is to present the findings. The presentation can take various forms. A report containing the outline of the examination proses and the evidence that was found can be created. In some cases the examiners should be able to testify in the court of law. The report and the testimony content will be summaries of the previous phases. If a presentation contains faults or inaccuracies it will have a negative effect on the evidence that was gathered even making the evidence inadmissible.

Destruction : The last step in the digital forensic examination is the demolition of the gathered evidence. The period can range from immediate destruction to seventy years after the case. The time period is influenced by various factors including data sensitivity and case severity.

Documentation is a continuous process and needs to happen in all phases of the digital examination. One of the main aids to help preserve the integrity of the evidence is documentation. The documentation should at least include the name of the evidence, the place the evidence is gathered. The documentation should also include the processes followed in identifying, retrieving, storing and transporting the evidence. The documentation should also mention the chain of custody when the examination was in progress. There have been several cases where the outcome of the case was influenced by the documentation.

A. Computer Forensics

Computer forensics is related to the forensics of computer components and their content [7]. The field of computer forensics attempts to narrow the search for evidence to the computer itself, the content on the computer and devices attached to the computer.

B. Network Forensics

Network forensics was introduced to help solve attacks on networked systems. The evidence of a Network Forensic investigation is collect from the data sent over the physical network consisting of a network containing at least two computers [7]. One method of gathering possible evidence is by captured and analysing network traffic. Other sources of network forensic evidence are logs from servers, users browsers settings and router information. Network Forensics can be done live. The problem with live network forensics is that significant hardware resources on a network consisting of more nodes than a typical home network [8].

C. Cloud Forensics

Cloud forensics is Digital Forensics applied on Cloud Computing [9]. Cloud Forensics is a subset of Computer Forensics as a cloud runs on a network and consists of network equipment. Cloud Forensics also entails Computer Forensics as a cloud consists of nodes that are computers. A cloud also consists of instances which are a special case of a computer instance. This means that Cloud Forensics ties Computer and Network Forensics together. This does not mean it is Digital forensics. Cloud Forensics is also a sub category of Digital Forensics.

III. Cloud Computing

Cloud computing is a relative old term but has been adopted quickly the last couple of years [2]. Cloud Computing builds on different forms off distributed computing. It ties the distributed computing together with virtualization. Cloud Computing enables a service provider to provide a flexible, cost effective and on-demand infrastructure to its clients instead of the clients running their own infrastructure. There is no standardized definition for cloud computing [10]. For the purpose of this paper Cloud Computing will be defined as a distributed computing architecture providing flexible, cost effective and on-demand infrastructure to users over some form of network by using virtualization to create virtual resources on the abstracted hardware.

The users of cloud infrastructure are provided a virtual computer with which can be interacted usually throw the

Internet [1]. This virtual computer can also be known as an instance. Normally an instance can be accessed from anywhere in the world depending on the security setup. The instance can be a small instance used by a single user to store backups of files or it can be a server running the website and database of a company. A client only pays the service provider for services rendered. If the requirements of the client change it is an easy process to change the scope of the instance to accommodate the new requirements of the client. If a new instance is required the task of stating and setting up an instance is trivial. On most Cloud systems an instances can be launched from an image that contains most of the needed software. This images were created with a specific task that it needs to perform. An image might be created that serves as a basis for a web server and another image for home computers.

The service provider is responsible for maintaining the Confidentiality Integrity and Availability (CIA) of the instances on a hardware level. The user is responsible for protecting the CIA on a higher level e.g. the content of files [11].

The value that can be added from Cloud computing is significant primarily to small and medium sized businesses [12]. It enables businesses to have access to servers without the initial start-up cost and they have no maintenance cost on hardware level. As the businesses grows their infrastructure can easily be changed to adapt to the growth.

Cloud Computing is growing and is estimated to become a billion dollar industry this year [9]. The reason for this is that some of the largest IT related companies has implemented or is implementing cloud computing. Some of the large companies are Google, Microsoft, IBM and Amazon [11], [1]. These company state they will provide CIA to their customers by using various techniques.

IV. The need to Isolate a Crime Scene

In a "real word" forensic process the crime scene is isolated [13]. The isolation helps protect the possible evidence from contamination and loss of continuity. If any contamination happens or the continuity is lost all the evidence gathered from the investigation admissibility might get lost. To help protect the admissibility of the evidence a crime scene is dived into separate parts to aid in the isolation. These parts can only be entered by authorized personnel using authorized manner. A path is sent out where the personnel can walk in and around the crime scene. A log is kept of where personnel are and what they are doing.

Multiple instances can reside on a single cloud node. A user of an instances expect that there is confidentiality in place to protect the data on that instance [11]. When a Digital Forensics Investigation is done on a cloud there must be methods in place to prove that the privacy and confidentiality of the users has been protected. We prove to users that their instances CIA was protected by using tested method that are accepted and known to protect clients CIA. To have proven methods to follow in an DFI the methods must be based on reliable technique to collect and preserve evidence.

In the cloud environment we want to protect the instance that we are going to investigate from tampering and contamination. In order to provide admissible evidence the evidence needs to be protected. Gathering evidence is one of the aims of a DFI. If the evidence is suspected to be invalid by any means it will not be able so serve as admissible evidence. In order to add the evidence admissibility the evidence needs to be protected from contamination and tampering.

Is a normal DFI it is accepted that assets may be seized. As stated above in a cloud environment there can be multiple instances running on a single cloud node. This makes it improbable that assets my be seized [2].

We feel it is necessary to isolate an instance on a cloud node. The controlled environment will aid in protecting the instance from contamination and tampering. This controlled environment where an instance is isolated is going to be used for the DFI.

V. Isolation of a Crime Scene in a Cloud

As stated a cloud node can contain multiple instances and the nodes needs to be cleared when doing an DFI. The methods for clearing include moving the suspicious instance to another node or moving the uninvolved instances too other nodes. The CIA of the other instances is protected when moving the suspicious instance. This can result in the loss of possible evidence. When we move an instance data may get lost or the instance might realize it is being moved and tamper with evidence. To protect the evidence the other instances are moved from the node. Care must be taken when moving the instances in order to protect their CIA.

When isolating a cloud instance the investigator must consider a we live or dead analysis is applicable. The techniques that are suited for each type of analysis may differ. When doing a live forensics analysis we want to stop the instance from tampering with evidence. If a dead analysis is chosen the other instances must be protected from the consciousness of the power outage. It must be decided what looses and risks are acceptable before staring with an DFI in a cloud.

The techniques that are proposed are Instance Relocation, Server Farming, Failover, Address Relocation, Sandboxing, Man in the Middle (MITM) and Let's Hope for the Best (LHFTB).

A. *Instance Relocation*

Instance relocation means that an instance is moved inside the cloud. This is done by moving the instance from one node to another. This can be done manually or automatically. When it is done manually the administrators of the cloud will usually move the instance by some means. Automatic relocation is done by the cloud operating system. When the instance is moved it can be done in three possible ways. The existing instance can be ended and a new one created. Another option is where a new instance is created and the old instances is destroyed once the new instance is created. The other option is where the instance is logically moved. This entails that the

data is moved from one node to another without the instance being destroyed.

To move an instance we divide an instance in three units that must be moved. These units include data on secondary storage, the content of the virtual memory e.g. swap memory and the running processes.

1) Manual Instance Relocation: When an instance is moved manually it is up to an administrator or investigator to move the instance. The possible methods to manually relocation an instance is a subset of the methods giving above. Either the existing instance can be ended and a new one created or a new instance is created and the old instance is destroyed once the new instance is created. When an existing instance is ended all of the units must be protected or saved. There is a verity of methods available. The storage can be copied to an image file using tools including dd_rescue [14]. The content of the virtual memory can also be written to files also using dd_rescue. Once all the files are created the original instance is removed and a new instance created. The new instance will receive all the content of the old instance. The new instance can be created with the same network address as the old instance but on a different node. One problem is the process. It is hard to store process in a manner that can restore the instances later to the new instance. The other method involves creating a new instance and moving all of the units to the new instance and then removing the old instance. Once the new instance is created the storage content can be moved to the new instance. The running process can be moved using methods designed to move processes between computers [15]. Some of the proposed methods by Milojíčić have been testes and proven as valid process moving methods. The virtual memory is harder to move and care must taken to move it. It is difficult to move because while the instance is being used the virtual memory is in a constant state of change. When the new instance has all the units of the original instance the original instance is removed. The new instance must then be set to have the same network addresses as the old instance to receive the network traffic.

2) Automatic Instance Relocation: The cloud operating system will move the instance in the Automatic Instance Relocation technique. The methods used to move is implemented by the creators of the cloud operating system. The creators must insure the method can be proven and is reliable. The means it uses may be the same as described above or be other methods. The reasons for an instance to be moved by the system includes, but is not limited to, the administrator or investigator asking the system to move an instance and load balancing. The administrator or investigator asks the system to move an instance for the purpose of an DFI other possible reasons might include conflict of interest between instances on a singe node. The load balancing functionality might be implemented in cloud operating systems. When the systems notices that instances on a node are extremely resource dependent and other nodes have lost of resources available it might try to balance the load of the nodes. This functionality can be used by an investigator. The investigator forces an instances to be resource intensive then the system will move it away from the node. The node is cleared by the system itself.

These instance relocation techniques enables a node to be cleared for an DFI. The way in which they are moved can be controlled and monitored. The service provider can prove to its customers that it is protecting their CIA. The cloud operating system manufactures can implement reliable methods to do a successful DFI on their cloud system.

If the instances are moved in a manner that violates their CIA the service provider may be influenced negatively. The customers may experience downtime of their instance or loss of data. They can then leave the service provider or charge for down time. If the cloud operating system moves the instances it might be hard for the investigator to prove they are using reliable methods. This adds reliance from the manufactures to be involved in an DFI.

These techniques can be hard to implement. As discovered by experimentation the storage media can be easily be copied but it is a non trivial task to send it to the new instance and keep that instance running. The hard drives where copied as a whole and the process of overwriting system files can result in the new instance failing. The process can be moved if the operating system of the instance supports the functionality. This can be an effective method to clear a cloud node if there is no build in functionality if implemented correctly.

B. Server Farming

A server farm is a multi-node system [16]. In web server farms the web-site is split over two or more nodes. The user interacting with the website only sees the functionality of a single server. In the server multiple nodes are used to deal with the website. The server farm uses some form of routing to route request between nodes from users. The server farms use distribution technologies to enable this service. This distribution aids in the Quality of service of the website. There is no single point of failure. When a node fails the router will stop sending request to that node.

In a cloud multiple instances can be created that is logically the same instance but over multiple nodes. Multiple instances work together and appears as one instances. The load for the logical instance is spread over the actual instances. When a single node fails the remaining instances will continue to function. This enables examiners to terminate instances on the same node and to isolate the suspicious instance on a node. Small server farms of the uninvolved instances needs to be created at the start of the investigation. They can be created by adding just one instance to the farm. This means there will be two instances in the farm. Once the server farm is working the original instance can be removed.

To enable Server farming on clouds it needs to be implemented by the cloud operating systems creators. The cloud infrastructure must provide for the rerouting of network traffic. The cloud infrastructure must also allow multiple instances to exist over multiple nodes that can interact. The process of creating a server farm for the sole purpose of an DFI might

put unnecessary load on the cloud. If the cloud provides the functionality to provide availability to its clients it can just be used to aid an DFI.

Although Server farming can be resource expensive it can aid the service provider manage their clients CIA. The instances can be removed from the node without a loss of availability.

This technique relies on cooperation from the cloud operating system creators. If the implementation is wrong the DFI can result in the loss of CIA of other users on the cloud.

C. *Failover*

In a failover environment there is at least one server replicating an other server [17], [18]. The replicating server is commonly known as the backup server. If the primary server fails the backup server can immediately take over. This means that all the data and processes of the primary server is replicated on the backup server. Failover was introduced to provide high availability for websites. In 1999 E-Bay lost an estimated 5 million dollars when there servers failed [19]. If there where failover technology implemented this problem could have been prevented. Failover can be provided in several ways. Possible methods are Client-based failover, DNS-based failover and IP-address take over [17]. In Client-based failover the client knows of both the primary server and the backup server. If the primary server is unresponsive the client communicates with the backup server. When using DNS-based failover the DNS server redirects traffic to the backup server when the primary server fails. In IP-address take over the backup server takes over the IP-address of the primary server when the backup server notices the primary server has failed.

To implement failover an adaptation of the IP-address take over will be used. The original instance is replicated creating a backup instance. Once the original instance is killed the backup instance will take over the IP of the original instance. The method in which the instance is replicated is open to the DFI team. To replicate the same units as for Instance Relocation needs to be moved. The units include data on secondary storage, the content of the virtual memory e.g. swap memory and the running processes.

The failover technique will result in virtually no availability loss of the instance. The failover can be implemented by the DFI team. There is almost reliance on the cloud operating system manufacturers. This technique also does not use a lot of resources of the cloud.

There will be a loss in availability and some data may get lost. This loss can cause loss of CIA. If the loss is acceptable the method may be used.

D. *Address relocation*

Address relocation can be seen as when network traffic is relocated to other computer. The network traffic is directed by either the router or DNS server to other computer because of some reason. A network packet is sent so a specific IP address. The computer which has the IP address might be unavailable and the packet is sent to other computer without the sender being aware of the change. The rerouting mechanism also makes it appears as if the packets that are returned to sender are sent from original computer. The Address relocation can be seen as a special case of the DNS-based failover method. A backup server is maintained in some or other form. When it is detected that the main computer has failed the traffic is routed to the backup server.

Create a replica instances of the uninvolved nodes. Once they are created use the clouds internal network DNS server or other method to redirect all traffic to the new instance. If the clouds DNS server cant be changed use an extra instance. This instance will serve as a middle ground to the instance and the internal DNS. The instance is another level of DNS. The instance can be used to interact with multiple instances but is controlled by the administrator of the system and not the system. The top level DNS can be configured when an DFI is in progress to redirect all the traffic to a replica created. The primary instance can then be removed.

The switch overtime from primary instance to replica instance can be insignificant if the replication is correctly implemented.

This method relays on replication working correctly. If the replication is incorrect the Address relocation is inefficient. The replication will help keep the instances CIA. This method also adds the complexity of two DNS server running on the cloud. The Service Providers might argue this technique is a waste of cloud resources.

E. *Sandboxing*

In program security a sandbox is a controlled environment where a program can execute [20], [21], [22]. A program cannot escape the sandbox and cannot effect other programs outside the sandbox. It is used to stop malicious programs from harming other programs on the same computer by limiting the interactions between the programs. A sandbox is created by software controlling the interaction of the program with other programs.

In terms of a cloud we will isolate an instance by placing it in a sandbox. The sandbox will prevent it from interacting with other instances. The other instances will then be protected from harm. To enable this functionality two approaches can be followed. The cloud operating system can launch a sandbox application. The other option is where the investigator launches an application on the instance. This application will monitoring all communication channels. It creates a virtual box around the instance. The instance can do what it wants inside the box but will not be able to do anything outside the box. This application will run on the network of the instance. Networking is the communication method an instance has with the rest of the cloud. The sandbox application will monitor network traffic and block were needed.

The sandbox techniques aids the service provider in protecting the CIA of the other instances. The other instances are protected while the DFI is being done and the instance that is being investigated is boxed in and continues as normal.

Information can be lost while the instanced is sandboxed. The instance might realize that it is placed in a sandbox and try to tamper with possible evidence. It might be difficult to block the network traffic in a manner that can be proven to be accepted in the field of DF.

These techniques helps the service provider in the CIA of other instances but evidence loss can occur. The instance can be sandboxed while the other instances are moved from the node. Once they are removed an DFI can be performed. This DFI can be a live or dead investigation. Once all other instances are off it can be decided which method is preferred. The sandbox may add a live forensics as the instance is kept in a controlled environment.

F. Man in the Middle

The term MITM can be used in network security to describe an Man in the Middle Attack (MITMA) [20]. An MITMA is a combination of potential threats in computer security. These threats include interception, interruption, modification and fabrication. Interception is where an other entity gains access to an assist. Usually the interception is unknown to the sender and receiver. The assist is delivered to the receiver and a copy to the entity. Interruption is where an assists is lost. The assist my be blocked, deleted or any other form of destruction of the assist. Modification is where the assist gets modified in some why. The receiver receives a changed version of the assist. Fabrication is where a new assisted is created. The senders sends the original assist and the receiver receives the assist created by the entity. An MITMA is where the entity places itself between the sender and receiver. It receives all the assists from the sender and sends assists to the receiver. The assists are vulnerable to interception, interruption, modification and fabrication.

To allow an MITM to be used in clouds to assist in an DFI an entity will be created that exits between the cloud instance and the hardware of the cloud. This entity can be part of or use the virtualization software of the cloud. The data going from the instance to the hardware and from hardware to the instance can be analysed. The hardware includes but is not limited to the network, CPU, RAM and hard drive. This enables a forensic process to be done on all the data being used in an instance. The forensic process will be a live forensic investigation.

The entity can be kept inactive when there is no suspicion of wrong doing on an instance. This minimizes cost of being ready for an DFI in term of computation cost. When there is a suspicion of an instance the MITM entity can be activated. Ones activated the MITM entity will analyse all actions of the instance and the data going from and to the instance. It will stop the instance from deleting data on storage media and RAM. The MITM entity will allow an investigator to access the resources of the instances without the instance being aware of the analysis. The investigator can also observe the actions the instance is or trying to perform. To enable the MITM to exist between the instance and hardware it must be added by the creators of the cloud software or by a using company. To aid in the evidence admissibility the MITM must be implemented using proven methods.

An advantage of this method is that the instance does not know it is being analysed. It can prevent the instance from destroying evidence also from doing the suspicious activity. Other advantages include hat the instance can function as expected and other instances will not be affected by the DFI. The techniques also aids in the protection of other instances. The instances that are being investigated can logically be blocked from communicating with other instances.

A potential problem is implementing it. There is a reliance on the cloud operating system manufactures. The cloud operating system manufacturers might not feel the need to add this functionality. To enable a company to add the functionality the software must be reversed engineered. Once the software is reversed engineered the MITM must be added. Both of these approaches has problems. The cloud operating systems creators might not make the functionality available to only its own employees or might create the functionality sub standard. The admissibility of evidence might be lost because of bad implementations. The problem with reverse engineering is the reverse engineering. Most software packages have a term of use. This term usually permits the revere engineering of the software. This opens a change that the company using an MITM they added might be sued. There is also the problem that proving the implemented as correct can be challenging because it was not implemented in a normal manner.

We believe that these techniques has the potential to be a valid techniques to do an DFI in clouds if the cloud manufacturers agrees to implement a reliable and proven MITM functionality in their software. The MITM might also be used to with other techniques. The other techniques clear the node of instances and a controlled live forensic process can be followed on the instance.

G. Let's Hope for the Best

The usual procedure is followed for doing an DFI [5] in the LHFTB technique. The node is turned off and taken to a controlled environment. Images of the hard drives of the node are made. These images are then analysed. A potential difficulty is that a node can contain multiple instances. The hard drives of the node can contain multiple virtual hard drives. The investigator must know how the cloud operating systems stores information. Information from other instances may not be used. This violates the CIA of the other users. It can be difficult to piece together the original virtual hard drive and credible evidence may get lost.

A possible advantage for LHFTB is that a suspicious instance has no warnings. This means that the instance possible will not interfere with possible evidence.

A potential problem is that on a single node can contain multiple instances. These instances can be lost. This violates the agreement between the service provider and the client. Uninvolved client lost their availability. Another problem is that running information is lost. The information in RAM and the network is lost and cannot be used.

We propose that this technique is not used on its own and that the other technique must be combined. Fist an MITM must be started on the instance that needs to be investigated. The RAM and other information can be acquired from the MITM. Other instances must then be moved from the node. The MITM also aids in the instance moving process it protects the instances being moved and keeps the investigated instance in a controlled environment. Then the power must be removed and images made. This creates a controlled and monitored DFI.

VI. Conclusion

Cloud computing is a rapid growing technology [11]. A DFI might be hard to do in a cloud because of various reasons [1]. On a cloud one node can contain multiple instances. The possible evidence can share a drive with several other instances data. The evidences needs to be protected. In the "real word" a crime scene is isolated to protect the evidence. If a digital crime scene on the cloud is isolated it can aid the evidences admissibility.

This paper introduced possible techniques to isolate an instance on a cloud. The techniques introduced where Instance Relocation, Server Farming, Address Relocation, Failover, Sandboxing, MITM and LHFTB. A brief discussion of each of these techniques where given.

It can be seen from the discussion that no one technique proposed a perfect solution. The techniques may be combined to provide a feasible method to isolate a cloud instance. The differences between some of the techniques are small and may be seen as the same. The differences of the techniques allows them to be used in different environments.

We want the implement the techniques in the future to test them in an experimental environment.

References

[1] 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*, November 2009, pp. 1 – 6.

[2] M. Vouk, "Cloud computing - issues, research and implementations," in *Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on*, June 2008, pp. 31 – 40.

[3] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 85 – 90. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655020

[4] "Definition of Forensic," April 2011, oxford Dictionary. [Online]. Available: http://www.oxforddictionaries.com/definition/forensic?view=uk

[5] M. A. Caloyannides, N. Memon, and W. Venema, "Digital forensics," *Security Privacy, IEEE*, vol. 7, no. 2, pp. 16 – 17, March 2009.

[6] F. Cohen, *Digital Forensic Evidence Examination*, 2nd ed. Livermore, CA: Fed Cohen & Associates, February 2010.

[7] B. Fei, "Data visualisation in digtial forensics," Master's thesis, University of Pretoria, 2007.

[8] V. Corey, C. Peterman, S. Shearin, M. Greenberg, and J. Van Bokkelen, "Network forensics analysis," *Internet Computing, IEEE*, vol. 6, no. 6, pp. 60 – 66, Novenber 2002.

[9] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: an overview," *IFIP International Conference on Digital Forensics*, vol. 7, 2011.

[10] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, nov. 2008, pp. 1 –10.

[11] R. Lu, X. Lin, X. Liang, and X. S. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 282–292. [Online]. Available: http://doi.acm.org/10.1145/1755688.1755723

[12] G. Reese, *Cloud Application Architectures : Building Applications and Infrastrucure in the Cloud*, 1st ed., A. Oram, Ed. O'Reilly Media, 2009.

[13] P. White, *Crime Scene to Court: The Essentials of Forensic Science*, 3rd ed., P. White, Ed. Royal Society of Chemistry, 2010.

[14] K. Garloff, "dd_rescue," Computer Program, vertion 1.23. [Online]. Available: http://www.garloff.de/kurt/linux/ddrescue/

[15] D. S. Milojíčić, F. Douglis, Y. Paindaveine, R. Wheeler, and S. Zhou, "Process migration," *ACM Comput. Surv.*, vol. 32, pp. 241–299, September 2000. [Online]. Available: http://doi.acm.org/10.1145/367701.367728

[16] E. Casalicchio and S. Tucci, "Static and dynamic scheduling algorithms for scalable web server farm," in *Parallel and Distributed Processing, 2001. Proceedings. Ninth Euromicro Workshop on*, 2001, pp. 369 –376.

[17] K. Singh and H. Schulzrinne, "Failover, load sharing and server architecture in sip telephony," *Computer Communications*, vol. 30, no. 5, pp. 927 – 942, 2007, advances in Computer Communications Networks. [Online]. Available: http://www.sciencedirect.com/science/article/B6TYP-4KYY4GT-1/2/4faf31d97db80455a5a5eb986648fcf6

[18] I. Kuzminykh, "Failover and load sharing in sip -based ip telephony," in *Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2008 Proceedings of International Conference on*, February 2008, pp. 420 – 422.

[19] R. Zhang, T. Abdelzaher, and J. Stankovic, "Efficient tcp connection failover in web server clusters," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 2, march 2004, pp. 1219 – 1228 vol.2.

[20] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th ed. Prentice Hall, 2006.

[21] C. Greamo and A. Ghosh, "Sandboxing and virtualization: Modern tools for combating malware," *Security Privacy, IEEE*, vol. 9, no. 2, pp. 79 –82, April 2011.

[22] M. Smith, T. Friese, M. Engel, and B. Freisleben, "Countering security threats in service-oriented on-demand grid computing using sandboxing and trusted computing techniques," *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1189 – 1204, 2006, security in grid and distributed systems. [Online]. Available: http://www.sciencedirect.com/science/article/B6WKJ-4K66F0M-1/2/5ec06dfeedd5b7fa56fb84ba4b6fef39