International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

A Survey About Impacts of Cloud Computing on Digital Forensics

Farid Daryabar[1], Ali Dehghantanha[1], Nur Izura Udzir[1], Nor Fazlida binti Mohd Sani[1], Solahuddin bin Shamsuddin[2], Farhood Norouzizadeh[1]
[1]Faculty of Computer Science and Information Technology
University Putra Malaysia
farid0fx@gmail.com, {alid, izura, fazlida}@fsktm.upm.edu.my,
farhood1990@gmail.com
[2]Cyber Security Malaysia
solahuddin@cybersecurity.my

ABSTRACT

Nowadays, digital storage of computer data is moving toward cloud computing which is a set of infrastructure provides data storage for organizations and individuals. Due to this large scale, in case an attack occurs in the network of a cloud it would be a big challenge to investigate the cloud. Therefore, digital forensics in cloud computing is a new discipline related to the increasing use of computers, networks and digital storage devices in numerous criminal activities in both traditional and Hi-Tech. This study reviews the literature on some challenges in cloud computing forensic investigation, and it is followed by evaluation and analysis of all types of information on cloud computing and its impacts on computer forensic investigations in publishing alliances with the survey was carried out in the field.

KEYWORDS

Cloud computing, Digital forensics, Digital investigation

1 INTRODUCTION

Recently, cloud computing has become a new paradigm in information technologies. It grants several promising technological and economic opportunities that have a prospective to become an evolutionary point in the new era of computing environment. The evolution of this technology creates various challenges mostly in cybercrime investigations and digital forensics. Therefore, there is a need for digital forensics experts or investigators to extend their knowledge and tools into cloud forensics environments and establish their capability in order to reduce the risks of cloud security. Apart from that, some characteristics of cloud computing such as multi-jurisdiction, different service models, different deployment models and multi-tenancy have created a new setting for cloud forensics dimensions.

Fundamental and technical background of cloud computing and digital forensics with the related works is included in Section 1 and 2. The analysis of forensic investigation and implication of digital evidence in cloud computing environment including focus on the technical issues, law enforcement of cloud forensics and privacy issues are presented in section 3. The conclusion with recommendations of future works is provided in section 4.

1.1 Cloud Computing Concept

Cloud computing which is also known as ‘Internet computing’ generally is seen as collection of clouds on the web.

It provides technology enabled services to the people and organizations by utilizing the internet [1]. People can just access to the web anywhere and at any time without to think about the physical management as well as the maintenance issues. Most of the cloud computing resources are very dynamic and scalable because they are independent computing which is free from maintenance cost. The most widely used definition of cloud computing is made by NIST [2] where they define Cloud Computing as a pool of computing resources such as servers, networks, services and applications that provide convenience, flexibility and more performance on demand network access which is consisting of five essential characteristics, three service models and four deployment models.

These five essential characteristics of cloud computing are on-demand self-service, broad network access, rapid elasticity, resource pooling and measured service [3]. Cloud computing composed of three service models that are Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). SaaS is where the application is hosted and delivered online through a web browser, PaaS is where the cloud provides the software platform for systems while IaaS is a set of virtualized computing resources [4].

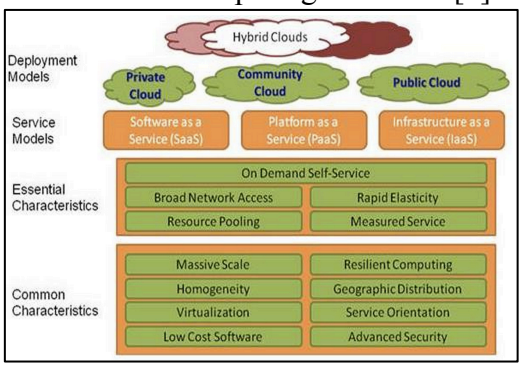

Figure 1. The NIST Cloud Definition Framework.

The four cloud deployment models are the Public Clouds, Community Clouds, Private Cloud and Hybrid Cloud. Figure 1 below is the overall picture of the cloud computing definition given by NIST [4].

Based on the standard definition given by the NIST, cloud computing aim to make a better use of distributed resources and combine them to achieve higher throughput as well as to be able to solve large scale computation problems [5].

1.2 Digital Forensic Concept

Digital forensics is also known as computer forensics or computer forensics is the process of preparing, acquisition, preserving, examining and analyzing and also reporting of digital data. The purpose of this digital forensics is to improve and to acquire legal evidence found in digital media [6].

According to the NIST, the current definition of digital forensics is the scientific procedures used to recognize and classify, collect, evaluate, and analyze the data while maintaining the level of integrity of the information throughout the forensics process. The purposes of digital forensics are including forensic computing, forensic calculations and computer forensics. Being called into judicial proceedings is one of the digital forensics risks. Thus it must have a correct procedure in conducting the forensic investigation and doing the inspection setup where this procedure or methodology must basically base on the scientific principles [7].

Although several studies had been done and the objectives more focused on the technical issues, challenges and the opportunities, but there is still a needed to do further research and find the most effective methods to evaluate particularly the uncertainty of the evidence or any forensic findings in the cloud forensics processes. Forensic

investigators need to fulfill themselves with a multiple disciplines of knowledge in order to investigate the digital evidence in a cloud environment. They need to master specific areas such as mobile, hard disk, registry and others that can be presented in court as legal evidence since all these evidences are in a virtual manner, not as others physical evidences. In order to ease the tasks of identifying before the extract to analyze the evidences, a reliable and specialize frameworks, tools, applications and other forensic requirements are needed. This paper will focus on the cloud forensics environments including the basic framework and architecture, the challenges and opportunities and also the security issues. It will further discuss the forensic investigations when it include into the cloud computing environment that covers from the digital evidence, the framework, the implications of digital investigations to the cloud computing environment and others.

1.3 Limitation of the Study

In this survey, the statistical analysis is based on trends from 2004 until present. Most of the papers are from Elsevier journals, IEEE and magazine articles. Based on these research papers it is not possible to help in developing a holistic picture of the current issues associated with cloud forensics. This is due to the technicalities of each paper in specific research field and insufficient information about cloud forensics is given. Based on the provided journals, most of the researchers are focus on the benefits of cloud computing system which limits us to find the scope and interest in this research. Among the other limitation it can be mentioned that some topics fit into more than one main category like journals with a topic keywords of concepts and architecture often overlap with a category in security and privacy issues. It can be admitted that the existence of journals that unclear or ambiguous about the topic of the journal and the content of it.

1.4 Data Collection

Implementation a number of steps are encapsulated in two key phases as follows:

1. Brainstorm. This first step is important to identify all related topics exist in 42 journals published from 2004 that need to be analyzed. Labelling while scanning a keyword is applied to all journals in order to categorize and generalize all the journals into few main topics.
2. Analysis. In this step we detail the resulted main category into a number of subtopics. Method of analysis is based on the keyword in order to investigate each journal.

It has been classified into four main categories which are framework and architecture, challenges and opportunities, security and privacy issues and cloud forensic investigations as shown in Figure 2. Within 8 years, 28 journals focusing on the area of the cloud forensic investigation area. This followed by 9 journals in security and privacy issues. For the rest two main categories are concepts and architecture contributed by 4 journals and 3journals in challenges and opportunities.

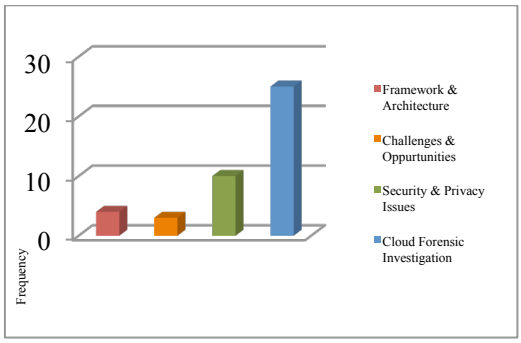

Figure 2. Main categories across the all papers.

In analysis step, keyword analysis plays a main role to extract the detail topic discuss. The four main categories in digital forensic analysis in the cloud computing environment study are further details in 23 subtopics as in Figure 3. However, the keywords used may vary in different papers, thus these keywords are grouped based on the author's understanding. For example the word forensic investigation challenge will be grouped together with a technical challenge as they represent a similar meaning of acting. This result of the listed subtopics doesn't reflect exactly the precise standard categories but purely from our perspective. However the keyword analysis portrays techniques and theories that are being emphasized within the timeframe of this research paper.

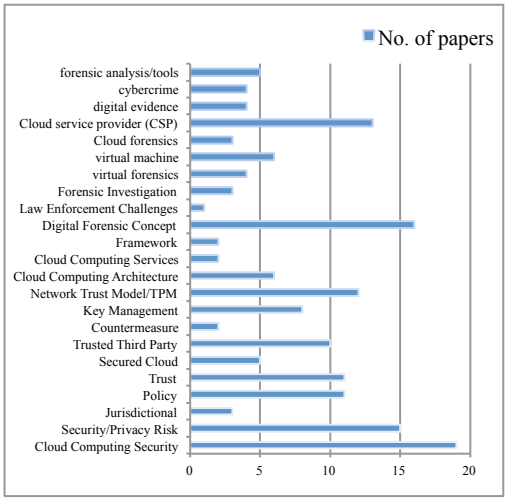

Figure 3. Details topics throughout the cloud forensic topic.

In some cases, the keyword analysis alone is not sufficient to determine journals belong to which subtopics or categories. This is where the analytical method needs to be implemented. The understanding of the whole picture of the journal is a must, and then the extraction of the proof concept of the journal will ease the case. For example a journal of 'An integrated conceptual digital forensic framework for cloud computing', according to the keyword can be categorized in both categories of cloud forensic investigation AND conceptual and architecture. With our analytical method, this journal suit best in conceptual and architecture category because the focus is on the academic concept rather than the application of the forensic investigation. Furthermore, the summary of the overall journals in this research is briefly explained in the next part.

2 DIVING INTO THE WORLD OF CLOUD COMPUTING AND DIGITAL FORENSICS

As mentioned earlier, in this section we will touch some related works and technical background on cloud computing and the role of digital forensics in preserving digital evidences in a cloud environment that become a major challenge particularly when involved with the different levels of challenges based on the complexity of the cases. This section is divided into 4 parts by. Part 1 briefs a basic architecture and framework of cloud computing the concept of cloud computing while focusing on the characteristics of the cloud computing including the service model and cloud deployment model. Part 2 discusses the challenges and opportunities when comparing with the traditional server-based system and hosting provision for security. While part 3 describes all privacy and security issues that need to be focused in order to strengthen and guarantee a security in cloud computing.

These issues include the topics of threat, data and privacy, also trusted and customers risk. The last part which is part 4 covers forensic investigations in a cloud computing environment mainly in digital evidence, framework and structure of digital forensic analysis. At the end of this section we give two case studies, SAMSUNG

Digital Video Recorder storage format and The Great Wiping Controversy, about overwriting hard drive data, based on the specimen's review regarding on forensic analysis.

2.1 Basic Framework and Architecture

As in the NIST Cloud Definition Framework in the previous section, the common characteristics of the Cloud Computing are Virtualization, low cost software, service orientation, massive scale, geographic orientation and others. It also contributes as an advantage by using this technology where cost is reduced to a substantial level because the infrastructure is provided by the third-party and the computing tasks do not need any intensive.

There are two main sections in the cloud computing system that is the front end, what the client sees and the back end, the cloud of the system. Both of them are linked and connected to each other usually through a network. The central server will monitor the traffic and also administered the system and client demands by using special software called middleware which allows networked computers to communicate between each other [5]. According to [5], there are four different layers of cloud computing architecture as Figure 4.

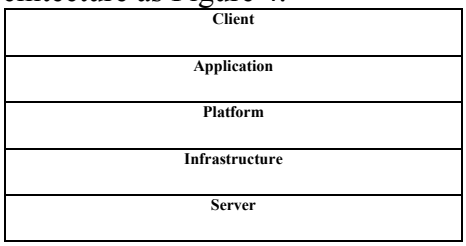

Figure 4. The Different Layers of Cloud Computing Architecture.

The top layer is the Client layer consists of the hardware and software which relies on cloud computing for application delivery. The second layer from the top is the Application layer which delivers SaaS over the web and eliminates the installation process on the user's system. Platform layer is the middle layer which provides the platform for the cloud infrastructure and it normally has all the applications required by the client. The second layer from the bottom is the Infrastructure layer which provides the required infrastructure as a service. This layer benefits more to client where they do not need to buy and installed by themselves. And here, the last layer in the above figure is the Server layer. This server level consists of the characteristic both computer hardware and software.

In one of the international conference papers by Liu et. Al 2010, the authors proposed the cloud architecture of virtual trusted platform modules (TPM). This virtual TPM is to facilitate the development of trusted system where it lies in its capabilities for secure key management and storage as well as reporting of platform configuration measurements. This cloud architecture of Virtual TPM is embodying the concept of Infrastructure as a Service (IaaS) in cloud computing environments. Figure 5 below is the cloud architecture of Virtual TPMs that been proposed by the authors from Australia [8].

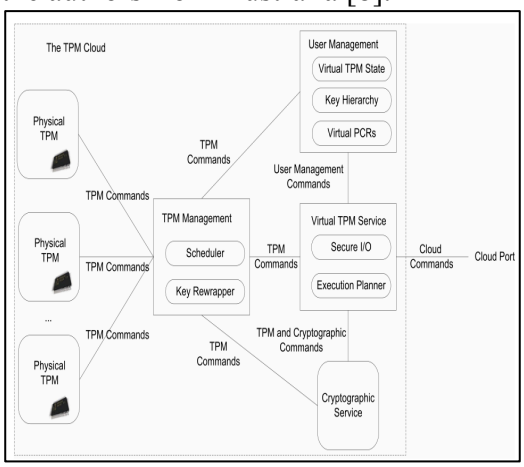

Figure 5. The Cloud Architecture of Virtual TPMs.

2.2 Challenges and Opportunities

Cloud computing has the potential to become one of the most transformative developments in the history of computing, following the footsteps of mainframes, minicomputers, PCs (Personal Computers), and smart phones. It has drastically moved the way how information technology services are generated, transported, accessed and managed. According to [9], a conclusion obtained from 2008 to 2009 survey regarding the implementation of the cloud computing is that cloud computing is gaining critical figure among large enterprises: 82% of the respondents said they are "in some stage of trial, implementation or use of public clouds" and 83% said the same for the use of private clouds. The move to cloud computing is the next stage of an inevitable trend in the breakdown of the enterprise perimeter, both technically and organizationally.
As the world has been moved from traditional computing system to this cloud computing environment, there are a lot of new challenges and opportunities that need to be taken into consideration by the people surrounding it. Below are three main challenges listed by [10] and the challenges are:

- Governance Aspect
  This governance aspect is that the people need to understand what is the main requirements are at the present stage and what will be in the future. People also need to justify what is the model that they need to employ the system in order to meet specific IT requirements.
- Risk Factor
  The main important thing here is that to understand who the owner of the risk is and the means for each risk to the main business and operations.
- Control
  When we are moving forward from the traditional paper-based risk register, we need to focus on how to mitigate the risk from our site. Without proper planning, it will bring such negative implications for the reputation in the marketplace for example loss of confidence after data leakage where it can be harmful to a brand.

All of the activities in a cloud computing system must be ensured that they are on the right security track. This is the biggest challenge to each company or organization where they must know their storage requirements must be able to associate with cloud computing environments.

2.3 Security and Privacy Issues

Security and privacy issues are divided into 3 sections as follow.

2.3.1 Threat and Security Issues

The term security means protection against something that may danger to another thing such as threats or attacks that can harm the network. A threat is an object, person or other entity that represents a constant danger to an asset. In our context here, an asset is the cloud computing itself. There are a lot of threats that present danger to an organization's people, to the information and also the overall network. Some of the common threats are as below:

- Acts of human error or failure

This threat includes acts performed without the intent or malicious purpose that cause by inexperience, improper training and also incorrect assumptions. Human failure can cause trouble with the overall network.

- Deliberate acts of trespass

This act happens when an unauthorized individual gain access to the network that's been protected by the owner. It means that the network is now not confidential for the owner.

- Deliberate acts of sabotage

This category of threat involves an act of sabotage or vandalism to either destroy the network's assets or damage the connection. Examples of this threat are an activist or cyberactivist operations and also cyberterrorism.

- Deliberate acts of theft

The threat of theft means that the illegal taking of another's property. This is a dangerous threat where sometime the owner's network may not know until the crime is far too late.

When the users of the web are rapidly increased from time to time, the security problems are also increasing. The high speed of communication has led to the growth development in information distribution and the cloud architecture is designed in order to address the issues regarding trust management in a cloud computing environment. The security issues are still there but the cloud architecture helps to reduce the complexity [11].

In an international conference paper by [1], the collected 11 journals as their literature review and they come out with a list of security problems in cloud computing environments and the problems are for example the loss and leakage of data, the client's trust and a user's authentication, the malicious users handling, the wrong usage of cloud computing and its services and also hijacking of sessions while accessing data.

Responses to the above security problems, one way to overcome the problems is by implementing the race factor. To ensure a good performance, there are some features need to be taken into consideration that meet with the management features in order to improve the RaS parameters and the features are as below [12]:

- Availability management
- Access control management
- Vulnerability and problem management
- Patch and configuration management
- Countermeasure
- Cloud system using and access monitoring

In cloud computing system, the main security issues are basically on the data communication between the client and the service provider as well as the vulnerabilities in the domains of both parties. The concept of cloud computing is that they transferred the responsibilities of data management and security to the service provider. Thus, users do not need to worry about the problem arises in this field.

2.3.2 Data Security and Privacy Issues

In the security world, there is one structure known as CIA Triad which are consisted of Confidentiality, Integrity and also Availability and this structure is purposely meant for ensuring that each organization or a system must be secured enough to run their operations. They become the building blocks that must be used in designing a secure system which applies to three categories of assets that are data, software and also hardware resources.

Confidentiality means that the data or information only can be used or accessed by the authority person. With cloud computing system, the resources are being shared including the memory, programs, network and data.

Although all the users are being separated, the hardware is not isolated to each other. In cloud computing, the data confidentiality is correlated to user

authentication. The main issue here is when the authentication is lacking, it can lead to unauthorized access to the user's account in the cloud [13].

Data integrity is an action to protect the data from unauthorized modification such as adding, deleting or editing the data. Thus, the security of cloud services depends heavily on the security of the interfaces. Other than data integrity, the software integrity, hardware integrity and the network integrity are also the main concerns topic.

One of the steps to avoid the security risks, [14] recommends to use the audit services because it is critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. According to Zhang et.al, 2012, encryption is also one of the most general data privacy preserving approach where it has been adopted to a lot of related areas such as SaaS, IaaS and PaaS [15].

Availability is meant for the accessibility of a system when the users request. It includes the availability of a system to continue operations. The network nowadays is full and burdened with data retrieval and processing at all time. The arise an issue in cloud computing is that the cloud computing services present a full reliance on the resource infrastructure and network availability at all-time [13].

According to Svantesson and Clarke, 2010, some privacy issues in cloud computing environment are such as whether the data is used appropriately, whether it has been stored and transmitted safely, how long the data will retained for and is the collection of data is carried out in an appropriate manner or not. These issues must be considered in all cloud computing environments [16].

2.3.3 Trust and Customer Risks Issues

In a cloud computing environment, a question of trust must be answered clearly, especially about the need of assurance and how to manage a secure business-to-business collaboration [17].

In [18], the authors listed out several problems regarding the trust issues that are the multiple stakeholder problems, the open space security problem and the mission critical data handling. They proposed a hierarchical trust model to overcome these three main problems. Other than obtain a secure aware cloud, users or clients also had minimal risks to be faced when they are in the cloud environment. This hierarchical trust model consists of two main layers that are internal trust layer and the contracted trust layer.

Internal trust layer is a platform that guarantees the operation is under the usual internal control while the contracted trust layer is the trust given by some contract. Figure 6 shows the cloud trust model proposed by [18]:

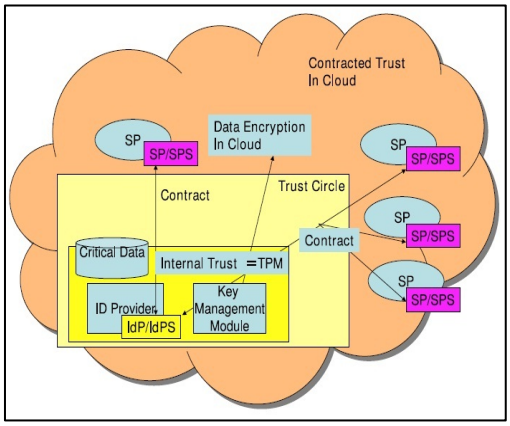

Figure 6. A Cloud Trust Model.

2.4 Forensic Investigations in Cloud Computing Environment

The main purpose of digital forensic investigation to step into the cloud computing environments is to find evidence against the criminals

throughout the web. Because of overflow technologies in cloud computing, the digital forensic analysis have to deal with some difficulties such as the security issues, the limited access and other issues that we had discussed before.

As we know, digital forensics is a structured investigation that is done in the past or ongoing of the data transmission and processing occurrences while still maintaining the chain of the document as the evidence where it can be used and validated in cases [19].

What makes it challenging in the cloud computing environment is that the source of the evidence is everywhere and the connection to the source is very complex and complicated. Moreover in applying digital forensic toward the cloud computing environment, the investigators will have to involve a lot of people whether inside of the country or even outside of the country where the processes of retrieving the evidence in cloud storage is not a simple as copying file from one folder to another folder. It may cost a lot of time which will cost us a lot of money in parallel to the time spend in doing the investigations.

Investigators have to discover the computational structure, attribution of data, the integrity of the data, and stability of evidence and also how to present and visualize the evidence which may bring to the aspect of cross-jurisdictional [19].

2.4.1 Digital Evidence in Cloud Computing Environment

Everything that an individual did in his life is kept somewhere as a record of what he's been doing and sometimes it is good and sometimes it is bad. As a Muslim, we learnt that there are two guardian angels named Raqib and Atid that will always keep recording our good and bad behavior.

The evidences are everywhere even if we want to deny it. In scientific angle, the evidence can be our fingerprint, DNA, human witnesses, CCTV, the residue of gun explosion, tools used, alibis, and also cloud computing environment.

As in the law, the enforcers have a warrant to be used to enter and search premises, this also applies if the constable required information stored in the electronic form where it includes that the electronic devices are with the suspect such as a laptop, mobile phone, compact disc or external hard disk and the devices is on the property as amended by the Criminal Justice and Police Act 2001, Schedule 2, para 13 (2) [20]. Other than that is the evidence from other jurisdictions such as answering questions or producing articles and information where it also include evidence in digital format. In seizing evidence, for example enforcers enter a premise to inspect and search the premises, if they found that the computers inside the premises are connected and on-line to a cloud storage server, that server is considered as a part of the computer hardware even if the server is out of the country. Thus, the enforcer or investigator may copy the data and information on to the computer of the suspects or they can have the remote access to the server thus they can download the data to any other computer they wish for [20].

In order to avoid the defendant from accusing that the enforcer change the data in the process of transferring the data to other devices, the enforcer may record what they have been doing using any types of recording instruments such as a video recorder or screen recorder software.

Problem when seizing evidence in cloud computing is when the cloud is managed by other organizations or

company that provide cloud computing services moreover if the cloud server is outside of the country because of a lot of procedure must be taken that involve government, politics, law enforcement agencies and also the time where the longer the time taken to seize the data and information from the cloud server, the longer the time for the suspects to safely erase and delete the data and information that is related to the cases [21].

In terms of the confidentiality of the data, in the cloud storage, there are also other personal data with other people and for the organizations and companies; their mission is to protect those personal datum from an unauthorized individual including the enforcer themselves. Thus, an act is written in 1998 to cater about personal data which is the Data Protection Act, 1998 [21].

Another problem is that there are a lot of data and information in the cloud storage, to find the information that related to the case might get hard such as finding a needle in the haystacks. Thus, cloud storage such as Google Docs is a good example where it recorded information relating to the use of the storage such as IP address, number of logins, date and time access and storage usage. The investigators can get the information related faster without having to look at the information in the cloud storage one-by-one [21].

In the United Kingdom (UK), RIPA which stands for the UK Regulation of Investigatory Powers Act, 2000 is the body that monitors most of all the investigation process in the UK. With this act, the process of transmitting the information is more secure and faster where a party without lawful authority cannot intercept the communication in the transmission process [21].

In the examination of cloud forensic especially in cloud based crime, [22] defined layers of trust based on the real situation where for example an evidence is brought to the court and the judge or jury have to decide whether they can trust the evidences presented to them in order to determine if the evidence is accurate or vice versa. Thus, both researchers came out with layers of trust in cloud environment such as in Table 1. By looking at the table, the investigators can choose where they want to conduct the forensic investigation based on the layers mentioned. All of the above also been agreed by a paper in [23] while focusing towards only personal computer (PC) and Smartphones that is commonly used in this world of technology.

Table 1. Six Layers of the IaaS Cloud Environment.

Layer	Cloud Layer	Trust Required
6	Guest Application/data	Guest OS, hypervisor, host OS, hardware, network
5	Guest OS	Guest OS, hypervisor, host OS, hardware, network
4	Virtualization	Hypervisor, host OS, hardware, network
3	Host OS	Host OS, hardware, network
2	Physical Hardware	Hardware, network
1	Network	Network

2.4.2 The Framework and Structure of Digital Forensic Analysis

There is also another method of file sharing which can be included in the cloud computing environment that called peer-to-peer connection where some parties claim it as copyright infringement. Means that as a user, we make our computer to become a host in sharing files with the other computers around the world (usually called as ‘Seeder’) and at the same time we also

get other files from other persons' computers (usually called as 'Leecher'). In this case, [24] proposed a spiral model in conducting the action research as in Figure 7.

According to [24], Phase I is the normal operation of the system where it includes plan in understanding the process, action in running the Expeer Program, observation where the host provides the IP address of the clients connected to it and the reflection which focus on designing the system to record, filter and block unauthorized files. While phase II is the suggested examination of management technicians which also includes plans in investigate the server role, action to block server connection, observation in finding a red herring and finally the reflection of the limit to circumstances.

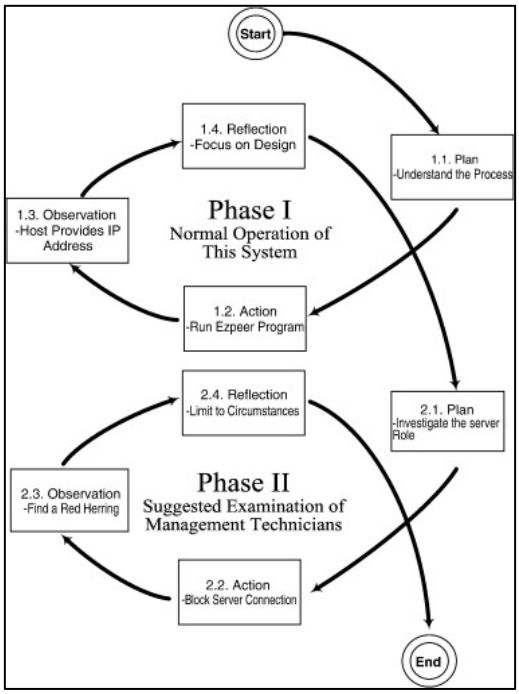

Figure 7. Action research on the commercial Ezpeer P2P model.

Every examination comes with the cost in parallel with time, thus [25] come out with architecture to reduce the time taken in examining the cloud storage and they called it as PDF architecture stands for the parallel digital forensics system. More computers can be used at the same time to examine the cloud storage. Figure 8 shows the visualization of the PDF architecture.

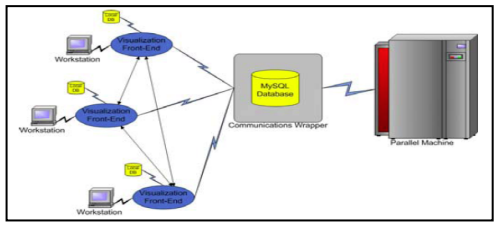

Figure 8. PDF Architecture.

In [26], they also come out with their proposed framework to support digital forensics investigation in the environment of cloud computing better than before and the way they proposed it is by integrating two digital forensic frameworks by NIST in 2006 and McKemmish framework in 1999. Thus, their framework is as below:

1. Evidence sources identification and preservation
2. Collection
3. Examination and analysis
4. Reporting and Presentation

Another method is by hardware based memory acquisition where a device call proof-of-concept is developed to read the system memory through the PCI interface while maintaining the integrity of the contents and it is called as 'Tribble' [27]. The writers claim that their method is more reliable than just using software in term of maintaining the data integrity because the risk of modifying the procedure in producing false data and the data being overwrite in doing the analysis can be reduced.

In addition there were several works on analysis of cloud and virtualized environments [42-44], privacy issues that may arise during forensics investigation [45-50], mobile device investigation [51].

3 ANALYSIS AND DISCUSSION

By looking at different angles, cloud computing environment actually makes the process of investigation easier and faster because without using the cloud

computing, the investigators may have trouble with cross platform software, multiple operating system in a different computers or mobile phone and there is also a lot of devices to be examined and that may cost time and also money. This paper will further discuss on the analysis on forensic investigations and the implication of digital investigation, both in a cloud computing environment.

3.1 Analysis on forensic investigations in cloud computing environments

The authors of [30] from Electronics and Telecommunications Research Institute, South Korea proposed a forensic service concept named as Forensic Cloud to enable the investigators focus more on the investigation process while does not have to think much about the technology used which means that they do not have to learn much about the latest technology but they still can continue with the process of investigation. In order to achieve this, they need a high speed processing of basic investigation which includes hacking, cracking, analyzing and many more and the needs of intuitive presentation and lastly to support user mobility while data access is secured.

Another analysis is proposed by [31], where he embedded the analysis software in the cloud to monitor the dynamic data network stream in real time. Thus, all of the incoming connections, outgoing packet, logging, time and date and others is recorded and monitored just like what have been done by Google in Google Doc storage or it is like anti-virus software that monitors any malicious data connection to the user's computer.

The software also recorded the temporary files, deleted files, exchanging files, system log files, backup medium, system buffer, registered information software, boot sector, allocated and unallocated space and slack space which also considered as a type of concealed evidence [31]. Most of this can be recorded and traced even if the system is shut down. Figure 9 shows the framework of the engine is placed.

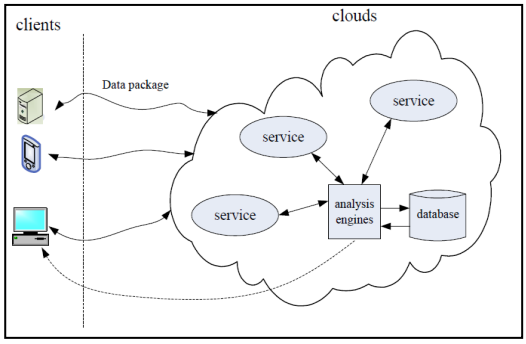

Figure 9. Framework of Analysis Engine.

Another analysis that can be used is the regeneration event where a snapshot is done toward for example every attack occurs. It is proposed by [32] where they classified the documented attacks as partition clustering which organized category wise as disjoint sets of attacks and also hierarchical clustering which divide the organized category sets. By doing the snapshot, they can replay the event of the attack as for their experiment and also restore the system to the state before the attack. It goes to the forensic analysis where the investigators can visualize the incoming and outgoing data through the cloud storage.

In [33], the authors have proposed a windows OS agnostic memory analysis. It is because of the tools used could not generalize a specific version and OS they were developed for. This kind of analysis has been described in the form of different processes.

As we see in the process flow, the first step is just to recognize whether it is a 32-bit system or 64-bit system and by doing this, they can find the kernel page directory table, thus the virtual

addresses can be parsed to physical addresses. After that, base address of the kernel executable and tcpip.sys are acquired where we can extract and use GUID (Globally Unique Identifier) to download the correct program to be used with this system from the cloud storage. Thus, from all the information, process, configuration information and registry are possible to be extracted using the techniques described in the paper [33].

3.2 Analysis of the Implication of Digital Investigation to Cloud Computing Environment

Cloud computing environments are now in their own level of IT world. The opportunity to save cost by having outsourced computing services and also the ability to exploit related competence make the cloud computing in a comfort zone. Amazon, Microsoft and Google are some of the service providers that have built successful cloud computing platforms especially in the economic benefits. But in the other hand, they do not know the location of their data and the service provider did not provide them with a guarantee for their data security [34]. Thus, the embedded of digital forensic analysis is needed to overcome the security problems and to provide the evidences when it is required.

One of the potential elements in digital investigation is the virtual environments. When the collection of data becomes larger, it leads to threat the storage because it is not only limited to any location. Thus, the need of virtual environments in the digital computer investigations arises because they bring positive implications to the system with a good performance level, excellent and also high stability [35].

From [6], the authors defined Virtualization process as "an abstraction layer that decouples the physical hardware from the operating system to deliver greater IT resource utilization and flexibility". Virtual environments make the digital forensics changed a lot. The virtual machines can be used either as evidence or as a tool. The implications of this fertilization process have added the vast level of difficulty to an already difficult field. Thus, digital forensic analysis may need an additional approach during the investigation process in the cloud computing environment such as memory forensic analysis or data carving method. The purpose of these two approaches is to recover any files that have been damaged when performing the analysis. This will raise an issue to few parties involves. Those issues are technical issues, law enforcement and private and confidential issues.

3.2.1 Technical Issues

Digital investigations are basically about the control of forensic digital data were in term of technical viewpoint, all of the data are available in three different states that are at rest, in motion or in execution [36]. Data at rest is presented by allocating disk space, data in motion is when the data is transferred from one to another while data in execution is where the process information and allocated data can be analyzed by creating a snapshot on the current system.

3.2.2 Law Enforcement Issues

Currently, the law enforcement agencies such as polices are conducting the computer forensics work. The Association of Chief Police Officers (ACPO) Guidelines for Computer Investigations and Electronic Evidence is a thorough complete document, which specifies the procedures and steps that officers should take in

dealing with a variety of situations associated with computers and digital evidence. This guideline provides the necessary information to ensure that each investigation is performed to the highest level of standards [37]. According to [38], the computer forensic process is basically consists of six stage model that are as below:

• Identification: determine items, components and data possible associated with the allegation or incident
•Preservation: ensure evidence integrity or state
• Collection: extract or harvest individual data items or groupings
•Examination: scrutinize data items and their attributes
• Analysis: fuse, correlate and assimilate material to produce reasoned conclusions
•Presentation: report facts in an organized, clear, concise and objective manner.

These six stage process models form the basis of the majority of computer forensic investigations. Through this paper they have considered cloud computing as a notable step change which will affect future practices in computing and IT. They also considered computer forensics as a process used largely by law enforcement agencies to acquire digital evidence associated with some alleged crime or incident.

3.2.3 Private and Confidential Issues

According to [39], private and confidential issues are one of the main concerns of digital forensic analysis in a cloud computing environment. Thus to tackle the problems related to these two issues, the authors make two groups of the major existing world that are private database search and public database search. The private database search includes the searching processes on private-key-encrypted data and also the public-key-encrypted data. While in public database search, the scheme of information retrieval allows user to retrieve records from the database without exposing about the record itself. It is the same topic and same author in another article that discussed about these two issues where in the second article, the authors agree that both privacy and confidentiality of irrelevant server data need to be protected [40].

Based on the revision of the specimens provided and the analysis that have been done, we suggest that cloud forensics issues can be separated into three different points of view. There are from the end users, trusted third parties and the service providers' perspectives.

3.2.3.1 From End User's View

Nowadays, cloud service provider affords to offers wonderful various packages with an eye catching prize, thus it is the end user's responsibility to determine the purpose of their requirement, identify the suitable cloud services and background technology used to best suit their business offers. The confidentiality, integrity and availability of the data should be the main focus in aiming for a security rather than the ease of use only. According to [11] from their experience, the end users are advised to engage with a cloud provider that able to qualify the standard ISO 27001 within the framework of the Statement on Auditing Standard (SAS 70), that will provide a document of gaps between governance, risk and control.

It is important to insecure the privacy of data by fully indicated in the Client-CSP contract with an additional clause of providing forensic capability. Appropriate terms in the SLA (Service Level Agreement) have to add to

enable general forensic readiness in the cloud. It is important because a low level of end users accessing to forensic data reflect that the end users have to control over the exact location of their data which depend on the cloud model choose.

3.2.3.2 From Third Parties' View

In terms of the third parties, the authors include the characters of the investigator of the forensic and as well as the auditors for the cloud computing. This is due to the nature of cloud computing service that is difficult to investigate due to the uncertain logging and data for multi tenants exact co-located at a specific time frame and potential spreading changing of host or data center depending on the cloud service provider. Thus in every forensic investigation case, it is important to lock a contractual commitment to support any form of investigation and discovery else any request from the investigator will be impossible to be fulfilled whether from neither the CSP nor the clients. Thus it is important to any investigator to have the knowledge of law to ease their job and protect themselves. For example, the digital investigators in UK abide by the guidelines enforce by the Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence [9].

3.2.3.3 From Cloud Service Providers' View

The Cloud Services Provider (CSP) means that whoever had provided the data storage services should have enough storage spaces and computation resources. From this view, the data owner and third party need to interact with CSP to gain an access or update their data for various application purposes. However, neither we assume that CSP is trusted to guarantee the safety of stored data, nor assume that the data owner has the ability to collect the evidences of CSP's fault after errors occur. Based on that, the cloud forensic investigations in cloud computing environments always involve of these two parties i.e. CSP and cloud customer. We found that when the CSP outsources the services to the other parties, the possibility of investigation occur is higher. Therefore, the services security will be guaranteed by the CSP, not from the users. The usability and reliability is then worth paying more attention highly.

4 Conclusion and Future Works

From analysis part, we identify that cloud forensics is a cross-discipline between digital forensics and cloud computing. Various aspects of forensic in cloud computing in terms of security and privacy issues, conceptual and architectural, challenges and opportunity and the cloud forensic have been reviewed.

Additionally, security and privacy in cloud forensics issues, most journals focus on the need for better understanding a potential risk involve if the breach of data in cloud computing happen and what the countermeasure need to be available for the ease of the forensic investigation need to be done. Thus it will lead to the involvement of the trusted third party, where most of the times can offer a more secured solution for the end users rather than the CSP.

This paper analyses the reviews of the related works and based on our view of the end users, trusted third parties and the cloud service providers' perspectives. From the end user's point of view this paper has discussed whether the availability is preserved so that they can get an access to their own data. From the trusted third parties' view, this paper has explained whether

they can gain the authority to get access to the evidence. And finally, for service providers' point of view this paper has summarized whether they able to guarantee the safety of the data.

The discussion above is basically on the security problems when digital forensics analysis is embedded into cloud computing environments. In the future, these security problems can be transferred as a solution in order to have a secured network. There must be some ways to have an improved security by migrating the cloud services. Three proposed ways by [41] are a progression of connectivity, the flat corporate network and the social engineering path. This may be one of the future works in the cloud computing field.

5 REFERENCES

1. F. B. Shaikh and S. Haider, "Security Threats in Cloud Computing," Sixth International Conference on Internet Technology and Secured Transactions, pp. 214-219, December 2011.
2. D. Chen and H. Zhou, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, pp. 647-651, 2012.
3. S. Mason and E. George, "Digital Evidence and Cloud Computing," Journal of Computer Law and Security Review, vol. 27, pp. 524-528, 2011.
4. H. Guo, T. Shang and B. Jin, "Forensic Investigations in Cloud Environments," International Conference on Computer Science and Information Processing (CSIP), pp 248-251, August 2012.
5. Y. Jadeja and K. Modi, "Cloud Computing- Concepts, Architecture and Challenges," International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 877-880, March 2012.
6. H. Sharma and N. Sabharwal, "Investigating the Implications of Virtual Forensics," International Conference on Advance in Engineering, Science and Management (ICAESM-2012), pp. 617-620, March 2012.
7. B. Martini and K-KR Choo. An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Elsevier- Digital Investigation, volume XXX, pp. 1-10, 2012.
8. D. Lin, J. Lee, J. Jang, S. Nepal and J. Zic, "A Cloud Architecture of Virtual Trusted Platform Modules," International Conference on Embedded and Ubiquitous Computing, pp. 804-811, 2010.
9. K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud Forensics: An Overview," IFIP Advances in Information and Communication Technology, vol. 361, pp. 35-46, 2011.
10. R. Morrell and A. Chandrashekar (Red Hat). Cloud Computing: New challenges and opportunities. Network Security, October 2011.
11. S. Ahmed and M.Y Akhtar Raja," Tackling Cloud Security Issues and Forensics Model," Conference on High-Capacity Optical Networks and Enabling Technologies (HONET), pp. 190-195, December 2010.
12. F. Sabahi, "Cloud Computing Security Threats and Security," pp. 245-249, 2011.
13. D. Zissis and D. Lekkas, " Addressing Cloud Computing Security Issues," Future Generation Computer System, volume 28, pp. 583-592, 2012.
14. Y. Zhua, H. Huc, G.J. Ahnc and S. S. Yauc, " Efficient Audit Service Outsourcing for Data Integrity in Clouds," Elsevier -The Journal of Systems and Software, vol. 85, pp. 1083– 1095, 2012.
15. C. Wright, D. Kleiman and R. S. S. Sundar, "Overwriting Hard Drive Data: The Great Wiping Controversy," ICISS 2008, pp. 243-257, 2008.
16. M. Taylor, J. Haggerty, D. Gresty and R. Hegarty, "Digital Evidence in Cloud Computing Systems," Elsevier- Computer Law and Security Review, vol. 26, pp. 304-308, 2010.
17. C. Everett. Cloud computing- A question of trust. Computer Fraud & Security, June 2009.
18. H. Sato, A. Kanai and S. Tanimoto, "A Cloud Trust in a Security Aware Cloud," 2010 10th Annual International Symposium on Applications and the Internet, pp. 121-124, 2010.
19. S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," Fifth International Conference on IT Security Incident Management and IT Forensics, pp. 3-9, 2009.
20. S. Mason and E. George, "Digital Evidence and Cloud Computing," Journal of Computer Law and Security Review, vol. 27, pp. 524-528, 2011.

21. M. Taylor, J.Haggerty, D. Gresty and R. Hegarty, "Digital Evidence in Cloud Computing Systems," Elsevier- Computer Law and Security Review, vol. 26, pp. 304-308, 2010.
22. J. Dykstra and A. T. Sherman, "Acquiring Forensic Evidence form Infrastructure-as-a-Service Cloud Computing: Exploring & Evaluating Tools, Trust and Techniques," Journal of Digital Investigation, vol. 9, pp. S90-S98, 2012.
23. H. Chung, J. Park, S. Lee and C. Kang, "Digital Forensic Investigation of Cloud Storage Services," Journal of Digital Ivestigation, pp. 1-15, May 2012.
24. 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," Journal of Computer Standard and Interfaces, vol. 31, pp. 795-800, 2009.
25. L. M. Liebrock et, "A Preliminary Design for Digital Forensics Analysis of Terabyte Size Data Sets," SAC'07, pp. 190-191, March 2007.
26. B. Martini and K-KR Choo, "An Integrated Conceptual Digital Forensic Framework for Cloud Computing," Elsevier, Digital Investigation, volume XXX, pp. 1-10, 2012.
27. B. D. Carrier and J. Grand, "A Hardware-based Memory Acquisition Procedure for Digital Investigations," Journal of Digital Investigations, vol. 1, pp. 50-60, 2004.
28. W. S. V. Dongen, "Case Study: Forensic Analysis of a Samsung digital video recorder," Journal of Digital Investigation, vol. 5, pp. 19-28, 2008.
29. C. Wright, D. Kleiman and R. S. S. Sundar, "Overwriting Hard Drive Data: The Great Wiping Controversy," ICISS 2008, pp. 243-257, 2008.
30. S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," Fifth International Conference on IT Security Incident Management and IT Forensics, pp. 3-9, 2009.
31. C.Yan, " Cybercrime Forensic System in Cloud Computing," International Conference on Image Analysis and Signal Processing (IASP), pp. 612-615, October 2011.
32. A. Belorkar and G. Geethakumari, "Regeneration of Events using System Snapshots for Cloud Forensic Analysis," Unpublished Thesis.
33. J. Okolica and G. L. Peterson, "Windows Operating System agnostic memory analysis," Journal of Digital Investigation, vol. 7, pp. S48-S56, 2010.
34. A. Induruwa, "Hidden in the Clouds: The Impact on Data Security and Forensic Investigation," The International Conference on Advances in ICT for Emerging Regions, vol. 77, 2011.
35. T. Pan and L. Zheng, "Trust Network Modeling for VirtualEnterprise Cloud Manufacturing," International Journal of Digital Content Technology and Its Applications (JDCTA), vol. 6, no. 5, pp. 115-123, March 2012.
36. D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), pp. 1-10, May 2011.
37. S. Biggs and S. Vidalis, "Cloud Computing: The Impact on Digital Forensic Investigations," International Conference for Internet Technology and Secured Transactions (ICITST), pp. 1-6, November 2009.
38. D. Reilly, C. Wren and T. Berry, "Cloud Computing: Forensic Challenges for Law Enforcement," International Conference for Internet Technology and Secured Transactions (ICITST), pp. 1-7, November 2010.
39. S. Hou, T. Uehara, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers," Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 378-383, 2011.
40. S. Hou, T. Uehara, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics," Third International Conference on Multimedia Information Networking and Security, pp. 595-599, 2011.
41. P.G Dorey and A. Leite, "Commentary: Cloud Computing- A security problem or solution?," Elsevier- Information Security Technical Report, vol. 16, pp. 89-96, 2011.
42. M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Bin Shamsuddin, "Forensics investigation challenges in cloud computing environments," Cyber Warfare and Digital Forensics (CyberSec), pp. 190-194, 2012.
43. S. H. Mohtasebi, A. Dehghantanha, "Defusing the Hazards of Social Network Services," International Journal of Digital Information, pp. 504-515, 2012.
44. A. Dehghantanha, R. Mahmod, N. I

Udzir, Z.A. Zulkarnain, "User-centered Privacy and Trust Model in Cloud Computing Systems," Computer And Network Technology, pp. 326-332, 2009.

45. A. Dehghantanha, "Xml-Based Privacy Model in Pervasive Computing," Master thesis- University Putra Malaysia 2008.
46. C. Sagaran, A. Dehghantanha, R Ramli, "A User-Centered Context-sensitive Privacy Model in Pervasive Systems," Communication Software and Networks, pp. 78-82, 2010.
47. A. Dehghantanha, N. Udzir, R. Mahmod, "Evaluating user-centered privacy model (UPM) in pervasive computing systems," Computational Intelligence in Security for Information Systems, pp. 272-284, 2011.
48. A. Dehghantanha, R. Mahmod, "UPM: User-Centered Privacy Model in Pervasive Computing Systems," Future Computer and Communication, pp. 65-70, 2009.
49. S. Parvez, A. Dehghantanha, HG. Broujerdi, "Framework of digital forensics for the Samsung Star Series phone," Electronics Computer Technology (ICECT), Volume 2, pp. 264-267, 2011.
50. S. H. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, "Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone," International Journal of Digital Information and Wireless Communications (IJDIWC),volume 1, issue 3, pp. 651-655, 2012.
51. Y. TzeTzuen, A. Dehghantanha, A. Seddon, "Greening Digital Forensics: Opportunities and Challenges," Signal Processing and Information Technology, pp. 114-119, 2012.