ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (47-58), Month: April - June 2016, Available at: www.researchpublish.com

# Cloud Forensics

[1]Haitham Ennajah, [2]Dr. Edward Chow

University of Colorado at Colorado Springs, School of Engineering and Applied Science

***Abstract:*** **The purpose of this paper is to explore and evaluate techniques and tools utilized in the world of Cloud Forensics. The main focus will be on how to acquire evidence from a cloud computing structure in a sound forensic manner, so as to preserve integrity and authenticity of the forensic evidences. Furthermore, the challenges facing investigators in acquiring data off of a cloud structure that could be out of their jurisdiction area will be discussed as well, along with recommendations based on this report's findings in order to overcome some of the critical challenges in Cloud Forensics.**

***Keywords:*** **Techniques and Tools, Critical Challenges in Cloud Forensics.**

***Terms and definitions:***

***CSP*** – Cloud Service Provider

***ISACA–*** Information Systems Audit and Control

***SANS –*** A US based Information Security training organization

***NIST*** – National Institute of Standards and Technology

***SLA*** – Service Level Agreement

## I. INTRODUCTION

Cloud computing has become one of the hottest topics which has changed the way of providing IT infrastructure to organizations, promising simplicity and delivering utilities based on virtualization technologies. Cloud computing provides convenience, availability, elasticity, large storage capacity, speed, scalability, and on-demand network access to a shared pool of configurable computing resources while reducing the cost based on pay-as-you-go basis for consumers **[1]**. Companies are realizing that cloud computing is offering a fast access to best-of breed business applications and is drastically boosting their infrastructure resources. However, there are some concerns about how security and compliance integrity can be maintained in this new environment **[2]**.

Cloud Forensics is different than the traditional computer forensics (i.e, acquiring evidence from a PC, laptop, handheld device, etc,). In these mentioned devices, the size of data storage isn't a huge problem to deal and work with to the investigator who is carrying the data acquisition process.

"*Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data."* NIST 2011 – The NIST Definition of Cloud Computing.

**Cloud forensics** is a cross discipline of cloud computing and digital forensics, **[10]**

Cloud computing is a shared collection of configurable networked resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law. Cloud forensics can also be considered as a subset of network forensics, since network forensics deals with forensic investigations in any kind of network, private or public. Cloud computing, in turns, is based on broad network access, and thus follow the main principles found in the network forensic process with some techniques custom tailored for the cloud computing environment.

Cloud computing is an evolving paradigm with complex aspects. Its essential characteristics have dramatically reduced IT

costs, contributing to the rapid adoption of cloud computing by business and government. To ensure service availability and cost-effectiveness, Cloud Service Providers (CSPs) maintain data centers around the world. Data stored in one data center is replicated at multiple locations to ensure abundance and reduce the risk of failure. Also, the segregation of duties between CSPs and customers with regard to forensic responsibilities differ according to the service models being used. Likewise, the interactions between multiple tenants that share the same cloud resources differ according to the deployment model being employed.

Multiple jurisdictions and multi-tenancy are the default settings for cloud forensics, which create additional legal challenges. Sophisticated interactions between CSPs and customers, resource sharing by multiple tenants and collaboration between international law enforcement agencies are required in most cloud forensic investigations. In order to analyze the domain of cloud forensics more comprehensively, and to emphasize the fact that cloud forensics is a multi-dimensional issue instead of merely a technical issue, both will be discussed in this paper.

Next, the following sections will be discussed in more details to point out some of the important aspects and challenges within the area of Cloud Forensics which are:

**I. Digital Forensics**

**II. Cloud Computing**

**III.Cloud Forensics**

To give a better insight, the next section explains some of the issues and challenges in digital forensics in respect to evidence and procedure. Then, cloud computing and its security concerns are discussed before moving onto cloud forensics and the related findings.

**I. Digital Forensics:**

Digital forensics is a process of analyzing digital data while preserving its integrity to be admissible in the court of law which includes: collection and preservation of sized media at the crime scene, validation, analysis, interpretation, documentation and courtroom presentation of the examination results. It is worth mentioning that the evidence contained within the media (obtained in traditional ways) is in the control of law enforcement where in the cloud environment such controls over the digital evidence are not feasible, **[3]**. Digital evidence is any information of probative value which is stored or transmitted in a digital form based on **(SWGDE)1** definition which presents many challenges due to its characteristics. Some of these challenges can be listed as follows:

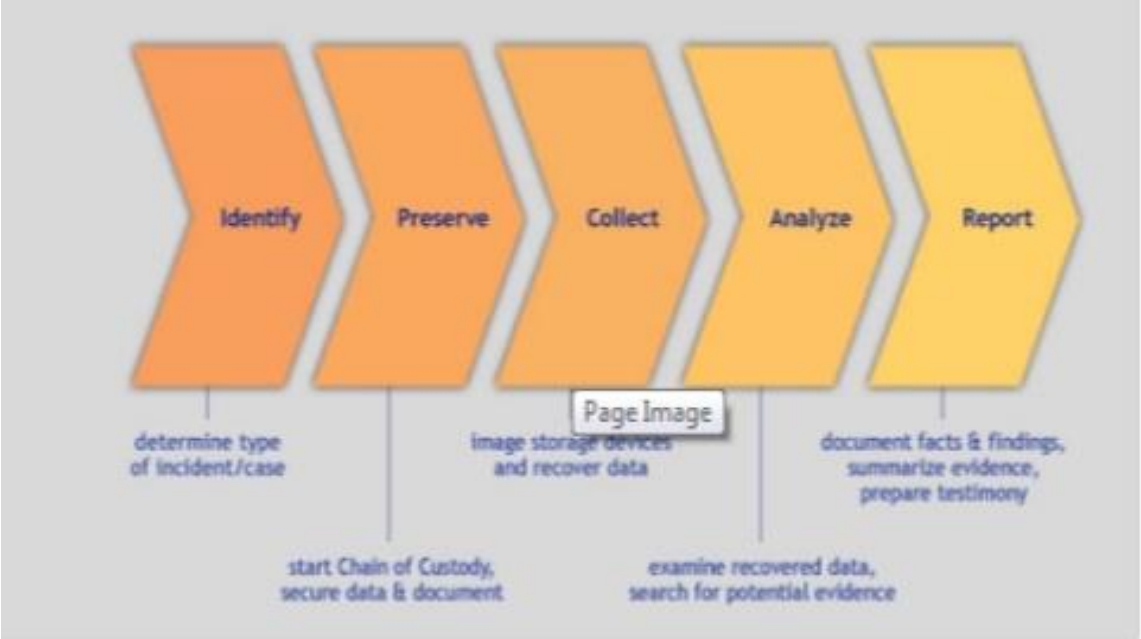
1. The quantity of potential evidence
2. Easy contamination
3. The number of suspects
4. Authenticity and integrity
5. Reliability
6. Completeness
7. Convincement (to Juries)
8. Admissibility, **[4]**

The procedure to carry out a digital forensics process, **(Figure 1) [25]**, requires precision due to the importance of its role in the presentation to the court which includes:

- **Identification**: determining the items or data associated with the allegation
- **Preservation**: ensuring integrity of evidence
- **Collection**: extracting data items

1 Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence standards and principles (1999), <https://www.swgde.org/documents.html >

- **Examination**: scrutinizing data and analyses
- **Presentation**: providing an organized report in a clear, non-technical and objective manner, **[4]**.




**(Figure 1)**

**II. Cloud Computing:**

Cloud computing is a fast growing technology which has attracted many organizations' attention towards the advantages that can offer including the reduction of the energy costs by outsourcing servers which reduces cooling cost, minimizes the number of IT related human resources, reduces the change management to the minimum, and minimizes cost of computer replacement. In cloud computing, software, hardware, and the configured system are purchased as a service. Cloud computing service is often delivered through virtual machines due to their flexibility and ready-to-go nature. The computing can scale up and down via the cloud computing application software in charge, **[5]**.

Cloud computing has five essential characteristics as follows, **[1]**:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

Cloud Computing has three models comprising of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These models have different limitations and provide different capabilities to the consumers. For example; SaaS provides browser-initiated application software for consumers and cloud providers take the responsibilities over security and application licensing, (suitable for public users) whereas IaaS allows to rent processing, storage, and networks, (suitable for enterprises). Four deployment models are defined in cloud computing as follows:

- Public
- Private
- Community
- Hybrid

The public cloud is available to general public whereas the private cloud is solely for a single organization. The

community cloud is used when several organizations are involved to support a specific community, and the hybrid cloud is a composition of private and community clouds.

**Security Issues in Cloud Computing:**

There are potential security threats associated firstly, with the fact that data in cloud are stored and processed remotely and secondly, the usage of virtualization and sharing of platforms between consumers whereby makes the ownership boundaries of digital items blurry. Gregg **[7]** presented a possible list of security threats in cloud computing indicating that the traditional security threats still exist in the cloud but they are more pronounced such as SQL-injection in platform level, phishing cloud provider, and expanded network attack surface. Further more, examples of the attacks in the cloud could be any of these as well : Side Channel attacks, Authentication attacks, and Man-in-the-middle cryptographic attacks.

Side Channel attacks happen when an attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. There were more threats listed by Jamil and Zaki **[8]**, being related only to the cloud environment. Some of these threats are listed below:

- **The loss of governance:** where there is a gap of commitment between cloud providers and Service Level Agreement(SLA)
- **Lock-in:** which is the difficulty in data portability within the cloud and introduces cloud provider dependency for service provisions
- **Data Protection:** cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification, **[8].**
- **Insecure or incomplete data deletion:** when the consumers are not sure whether their data have been deleted completely or partially (i.e. other copies) based on their request. It is worth mentioning that there are other security threats which could be happening from the inside of cloud environment such as attacks from one virtual machine to another which are difficult to detect. There is no doubt that cloud computing is a great technology which present IT organizations with a fundamentally different model of operation however, security is one of the main issues and in a case of security breach, the major concern is the safety of the stored data. This particular concern can be addressed in the following:

**1. Service Level Agreement (SLA):**

SLA represents an understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation that is available to the cloud subscriber. This also includes the terms of service covering other important details such as limitation on liability and accountability.

**2. Multi-Location:**

Cloud systems offer huge computer resources to consumers therefore; the produced data are stored in the cloud in different locations along with the mirror copy produced by the cloud providers for recovery situations. One of the obvious problems in this scenario is that the data may be stored in multi-jurisdictions where different rules apply. It is possible that one action is legal in one jurisdiction whereas it is illegal in another and this will seriously affect any forensic investigations regarding data acquisition.

**III. Cloud Forensics:**

Cloud forensics can be defined as the application of digital forensics in cloud computing. The cloud computing benefits are the reasons that are making forensic community concerned. The scalability of the cloud means at one point, data from different sources can occupy the same sectors within the storage media which creates a dilemma during e-discovery, while a company is being investigated; the investigator unknowingly acquires residual data from another company, **[9]**. The growth of storage capacity in cloud computing is a disadvantage for digital forensics since there would be more forensic

data and more time consumption to analysis the data, of course, if nothing goes wrong. There are other insufficiencies and incompatibilities of the traditional digital forensics methods (e.g. encryption, multi-jurisdiction, & proliferation of endpoints) in cloud computing. Therefore it is necessary to adopt digital forensics knowledge and tools specific to cloud computing in order to establish a forensic capability toward reducing cloud security risks **[10]**.

Cloud computing is a new model and the digital forensics community is still exploring what difficulties this new technology creaks for them. There have been many published papers stating the potential encountered difficulties in the process of maintaining the chain of custody. Even leading private or public organizations like SANS, ISACA or NIST have not yet presented a set of recommendations or best practices to follow when there is a security incident inside of the cloud or guidelines on how to implement the cloud in organizations, **[11]**.

In some cases, cloud computing could be able to assist network forensics in their online investigations for cybercrimes. Criminals may abuse professional anonymous communications systems such as Tor and Anonymizer which were originally designed for protecting network users form identity theft and profiling. Therefore, law enforcement may purchase tens of Amazon EC2 Vms, joining the Tor network as sentinels which can act as entry & exit nodes for Tor circuits and would be able to determine the attack sources.

## 2. TECHNICAL CHALLENGES AND IMPACT OF CLOUD FORENSICS

Compared with traditional forensics, it is challenging to capture complete events and related data within the cloud computing environment.

Here are some unique difficulties as compared to traditional forensics:

- Potential loss of data during an image process for different reasons, such as shut down virtualized server, can cause parallel or unrelated services to be interrupted.
- Lack of access to network routers, load balancers and other networking components
- No access to large firewall installations
- Challenges in mapping known hops from instance to instance which will remain static across the cloud routing schema
- Challenges in log analysis of cloud applications
- Consolidation and consistency of logs
- Accessibility of logs
- The velocity of attack factor
- Malicious insider
- Data deletion
- Hypervisor-level investigation

In order to address the technical challenges in the cloud, a variety of studies were carried out by researchers such as Ruan, 2011 **[14]** who published a paper proposing a new definition for cloud forensics after conducting a survey among digital forensic experts and practitioners from around the world in United Arab Emirates, hosted by Zayed University. The survey was aiming to indicate a better understanding of some concepts such as the cloud forensics definition, the most challenging issues, most valuable research directions, and the critical measures for cloud forensic capability. Based on Ruan's definition, **[10]**, cloud forensics is a cross-discipline between cloud computing and digital forensics. Also, it is a subset of network forensics which deals with forensic investigations in any kind of public or private networks with extended or novel techniques tailored for the cloud computing environment.

Cloud forensics can be expanded in three dimensions: technical, organizational, and legal, **[10]**.

**Technical Dimension:**

The technical dimension encompasses the procedures and tools that are needed to perform the forensic process in a cloud computing environment. These include data collection, live forensics, evidence segregation, virtualized environments and

proactive measures. This dimension includes a set of tools and procedure to carry out the digital forensics process in cloud computing environments and its main key aspects are as follows:

- **Forensic data collection:**

It is the process of identifying, labeling, recording, and extracting data from other possible sources of data in the cloud either the client-side or provider-side artifacts. Due to the different cloud service and deployment models, duties vary from one service or deploy model to another in the cloud. Therefore, different tools and procedures are to be applied. For example, in public clouds, forensic data might be collected from multiple tenants in the cloud environment. Other considerations regarding data collection in the cloud are prioritizing the collection of highly volatile data while preserving the integrity of data without breaching any laws and regulations under the jurisdictions where the data are collected.

- **Elastic, static and live forensics:**

It is essential for cloud forensics tools to be elastic in order to compete with rapid elasticity of cloud computing. Large scale static and live forensic tools are required to deal with most cases such as e-discovery, data recovery, data acquisition, and evidence analysis tools.

- **Evidence segregation:**

Cloud forensics involves the reverse process of evidence segregation from various shared resources in multi-tenant environment but the underlying cloud infrastructural components such as CPU caches and Graphic Processing Units (GPU) were not designed for strong compartmentalization in a multi-tenant architecture. Therefore, it is necessary to develop tools and procedures in order to be able to segregate evidence among multiple tenants in different deployment models with different service models in the cloud.

- **Investigations in virtualized environments:**

tools and procedures are required to be developed for investigations in virtualized environments such as hypervisor investigations and evidence retrieval from physical locations of data at a given time stamp.

- **Pro-active preparations:**

pro-active measures can be taken to facilitate the forensic investigation such as designing forensic-aware cloud applications, tools which pro-actively collect forensic data in the cloud, and conducting regular snapshots to remote storage.

It should point out that the technical dimension encompasses some challenges one might face during an investigation in a case that is associated with a cloud environment.

The main challenge to forensic investigations is the scope and diversity of operations in a cloud computing environment.

These challenges can be addressed as follows:

**Discovery of Computational Structure:**

The identification of computing and storage systems to be analyzed for evidence is time-consuming at larger scales and cannot be readily ascertained in the case of distributed computing systems. In addition, in many cases the systems and services cannot be duplicated or sized due to sharing resources among the servers and third parties which causes unreasonably infringements or crossing jurisdictional boundaries. There is a need to develop a mechanism for describing the scope of the computations, services, or documents to be captured which includes several aspects such as temporal extent, spatial extent, and dependency analysis. Temporal extent is related to the fact that data may be present for a limited time or to be staged through different levels of storage hierarchies so the establishment of a consistent (e.g. snapshots) of state related to the data and process is required. Spatial extent is related to the location transparency of cloud computing which represent a significant challenge in accessing the evidence in multi-jurisdictions and it is crucial to establish an understanding of the location on which relevant data is stored. Dependency analysis is the need to establish a complete understanding of processes' dependencies and their distribution across different systems in a cloud environment. These three issues merely serve as an abstract outline of some of the issues in capturing forensic data in the cloud environment.

**Attribution of Data:**

The utility as forensic evidence of any data depends on the ability to ascertain the provenance of the data and, where possible, have clear attribution in place.

**Semantic Integrity:**

The semantics of a data set representing a snapshot of a system which, is limited in scope both temporally and in the extent captured, must be ascertained with the same level of confidence as the data itself. It is highly important to establish mechanisms for gaining semantic information such as data dictionaries and to infer information with sufficient, demonstrable, or provable confidence. This is not just limited to the collection and analysis of evidence, but also to its presentation as the reasoning and analysis should be performed in a transparent way when incomplete or inferred data is applied.

**Stability of Evidence:**

It is not always possible to obtain the individual specifications and data dictionaries for distributed data sets and partial data sets collected from distributed systems and it is also difficult to retain the operational instances on which one can rely for isolated data. Thus, it is crucial to establish the maximum extensional information of a given data sets upon capture as well as mechanisms for describing such semantic information which may need the creation and derivation of extra data sets to aid in deducing the extensional semantic of data set in question so as to permit longer-term preservation of data sets. Another issue relates to time-sensitive ephemeral data such as streaming media or control systems data flow.

**Presentation and Visualization of Evidence:**

This may involve documents or linked sets of documents containing substantial challenges as a large number of different formats and presentation mechanisms may be required since the data sets may have a considerable temporal extent and extensional semantics as well as representational specifications may change across data items forming a set of digital evidence.

**Cross-Jurisdictional Aspects:**

Modern distributed systems and the data processed that are likely to transcend national borders in at least some of their constituting elements during the processing or storage data sets. This presents a considerable challenge and must be tackled so not to jeopardize the investigative process. There is a need for research to be conducted from different areas to converge and collaborate to affect the desired outcomes in digital forensic investigation in cloud computing environment, **[16]**.

In a research carried out by Delport **[17]**, the use of some cloud isolating techniques were suggested in order to prevent any contamination or tampering in the evidence while forensics investigations are taking place in the cloud environment. These techniques include Instance Relocation, Server Farming, Address Relocation, Failover, Man in the Middle (MITM) and Let's Hope for the Best (LHFTB). They interpreted a virtual computer in the cloud as an instance which can be accessed from anywhere in the world depending on the security setup. A cloud node can contain multiple instances where the node is required to be cleared during a forensics investigation by moving the suspicious instance to another mode or moving the uninvolved instances to other nodes. Instance relocation can be done by moving an instance inside the cloud either manually or automatically. Cloud administrators can move an instance manually whereas in automatically movement, operating system is able to perform the movement. Any instance movement includes transferring three parts of an instance; data on secondary storage, the content of the virtual memory and the running process.

## 3. CLOUD FORENSICS TOOLS

There is no fool-proof method of acquiring data forensically in the cloud which requires a combination of computer forensics and network forensics. The active data can be collected by traditional forensic tools, while its integrity is preserved, and for additional data over the network such as activity logs, network forensics tools are used. E-discovery by, (Access Data), can be useful in cloud computing which refers to any process in which electronic data are sought, located, secured, with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or performed on a network, e.g. Encase have launched their own version however; avoidance of multi-jurisdictions problem is a major concern.

Another useful tool is OWADE, (Offline Windows Analysis and Data Extraction). It is an open source cloud forensics tool developed by a Stanford University team, provided and launched at the BlackHat 2011 security conference, (http://owade.org). It is able to extract information from cloud services that a user accessed in his computer; reconstruct Internet activities and search for the online identities that were used however; Encase and FTK (The Forensics Toolkit) would be able to perform this. One of OWADE advantages is its ability to decrypt files ciphered using various Microsoft built-in encryption schemes and it combines this ability with traditional data extracting techniques in order to access Skype chat history, decrypt Internet Explorer stored logins and passwords, by cracking the windows user password, or access historical Wi-Fi location data stored by windows, delivering a list of access points with dates and times.

**Log analysis Challenges:**

Some of the most useful information in digital forensics is within the log files which can also assist the application developers for fault monitoring, assessing feature usage, and monitoring business processes. There are challenges associated with cloud-based log analysis and forensics such as, decentralization of logs, volatility of logs, multiple tiers and layers, archiving and retention, accessibility of logs, nonexistence of logs, non-compatible or random log formats, and absence of critical information in logs.

**Organizational Dimension:**

Forensic investigation in the cloud computing environment involves the consumer, the cloud provider, and sometimes the third party. An organizational structure is needed in order to carry out cloud forensics activities efficiently and effectively **[10]**.

**Cloud Organizational Structure:**

Each cloud organization is required to define a structure of internal staffing, provider-consumer collaboration, and external assistance satisfying the following roles:

- **Investigators:**

The investigators not only are responsible to carry out a collaborative investigation of allegations of misconduct in the cloud, but also, assist law enforcement when is needed. Also, they need to know the forensic capabilities of the involved parties and their segregation of duties.

- **IT Professionals:**

Such as networking staff, security staff, administrators, ethical hackers, cloud security architect, and technical support staff who assist the investigators with their expertise in the cloud organization.

- **Incident Handlers:**

They are responsible for incidents such as unauthorized data access, inappropriate system usage, accidental data leakage and data loss, insider attacks, and malicious code infections.

- **Legal Advisors:**

It is necessary to include legal advisers, who are familiar with multi-jurisdiction and multi-tenant issues, in forensic staffing in order to prevent any violations in regulations under respective jurisdictions or confidentialities of other tenants who sharing the same resources. It is also recommended, Service Level Agreements (SLAs) to include the related responsibilities and procedures to follow in a case of forensic investigation while an internal legal advisor is involved.

- **External Assistance:**

It is recommended that cloud organizations involve external parties to perform forensic tasks such as e-discovery, investigations on civil cases, and investigations on external chain of dependencies. It also helps to determine in advance which actions should be performed by the external parties **[10]**.

**Chain of Dependencies:**

Cloud providers and most cloud applications often have dependencies on other cloud providers therefore, an investigation may depend on one of the links in the chain and level of complexity of the dependencies. Essential communications and

collaborations through this chain need to be facilitated by organizational policies and SLAs. The chain of cloud provider and consumer also has to communicate and collaborate with law enforcement, third parties, and academia in order to facilitate effective and efficient forensic activities **[10]**.

## 4. OPPORTUNITIES AND CHALLENGES IN FORENSICS FOR DIFFERENT MODELS

Data centralization in the cloud can be a benefit to forensic readiness which leads to a quicker coordinated response to incidents and also a dedicated ready to use forensic server can be built in case of need. Some of the other advantages to the computer forensic investigators are the high availability of compute-intensive resources and potentially petabytes of storage. Moreover, inbuilt hash authentication for authentication of disk images shortens the time needed in generating MD5 checksums. However, the main difficulties of cloud computing from a forensic perspective are maintaining the principles for forensic procedures in the cloud such as remote data centers, evidence authenticity and integrity **[4]**.

**These models are represented as follows:**

**Infrastructure as a Service (IaaS)**

Cloud Computing's Infrastructure as a Service (IaaS for short) is the foundation of cloud computing. Rather than purchasing or leasing space in an expensive datacenter, labor, real estate, and all of the utilities to maintain and deploy computer servers, cloud networks and storage, Cloud buyers rent space in a virtual data center from an IaaS provider. They have access to the virtual data center via the Internet. This type of cloud computing provides the "raw materials" for IT, and users usually only pay for the resources they consume, including (but not limited to) CPU cores, RAM, hard disk or storage space, and data transfer – example IaaS providers include ProfitBricks and Amazon EC2 .

**Platform as a Service (PaaS)**

The consumer deploys application packages to a runtime environment that is hosted by a cloud provider so the consumer owns the core application, and programmatically dictates how it would interact with other dependencies.

For example, in case of Microsoft Windows Azure, the application would be built in Visual Studio, compiled and published through Azure developer portal. The advantage is the core application is controlled by the organization. Therefore, log information can be customized in a way that by invoking the custom code, the system state can be interrogated and logs be pulled. The disadvantage is that the provider may confine the access to logging information **[21]**.

**Service as a Service (SaaS)**

In SaaS, the provider invokes an instance of an application and the consumer can apply basic configurations or may be able to interface with the application via an API, however, no deep programmatic control is involved in order to modify the core application of the system.

The advantage is that high level application logs might be available either success logs and failure logs, or the actual activities within the environment which depends on the provider's decision.

**Crime in the Cloud:**

CA Technologies (Internet security business unit), reported that an emerging trend is now happening towards the creation of Cimeware-as-a-Service with almost all Trojans (96%) developed as a result of this tactic. It also claimed that cyber criminals are increasingly reliant on cloud-based web services and applications, such as Google Apps, Flickr and Microsoft Office Live, as well as real-time mobile web services to target general users. Criminals have already started to develop exploit kits such as Incognito which is a web-based application represented as MaaS (Malware as a Service), and it is located in the cloud providing services to underground communities, **[22]**. Cloud computing could still suffer from traditional attacks such as DDoS, attacks targeting parts or the entire cloud. In addition, a cloud can be used as a tool to conduct or plan a crime and attack another cloud.

**Mobile Cloud Forensics:**

Most of the existing mobile applications use cloud computing such as Facebook and Google Mail. Mobile commerce is a new innovation which is causing a concern in the digital forensic community. For instance, wave and pay is a new method of payment where consumers no longer need to pay by bank card and the bill will automatically be paid with a swipe of a

mobile. Some of the studies have been dedicated to improve mobile cloud forensics. In 2011, Zhu **[24]** carried out a research to find out whether the existing forensic tools are able to extract all the information within smartphone devices. Different digital forensic tools (e.g. XRY v5.5 & Oxygen) were used as well as the open source tools. Zhu's findings indicated that the current forensic tools and methodologies could not extract data from cloud storage based applications such as Dropbox and also have difficulties extracting cloud based emails such as G-mail. Cloud based emails can only be extracted if the phone is jail-broken or has a root access right. However, the cloud service provider would be able to collect the emails, but the integrity of the data would not be 100% **[24]**.

**Legal Dimension:**

Traditional digital forensic professionals identify multi-jurisdictional and multi-tenancy challenges as the top legal concerns. [10], the legal dimension of cloud forensics requires the development of regulations and agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides. Also, the confidentiality of other tenants that share the same infrastructure should be preserved.

SLAs define the terms of use between a CSP and its customers. The following terms regarding forensic investigations should be included in SLAs:

1. The services provided, techniques supported and access granted by the CSP to customers during forensic investigations.

2. Trust boundaries, roles and responsibilities between the CSP and customers regarding forensic investigations.

3. The process for conducting investigations in multi-jurisdictional environments without violating the applicable laws, regulations, and customer confidentiality and privacy policies.

**Opportunities:**

Despite the many challenges facing cloud forensics, there are several opportunities that can be leveraged to advance forensic investigations:

- **Cost Effectiveness:**

Security and forensic services can be less expensive when implemented on a large scale. Cloud computing is attractive to small and medium enterprises because it reduces IT costs. Enterprises that cannot afford dedicated internal or external forensic capabilities may be able to take advantage of low-cost cloud forensic services.

- **Data Abundance:**

Amazon S3 and Amazon Simple DB ensure object durability by storing objects multiple times in multiple availability zones on the initial write. Subsequently, they further replicate the objects to reduce the risk of failure due to device unavailability and bit rot. This replication also reduces the likelihood that vital evidence is completely deleted.

- **Overall Robustness:**

Some technologies help improve the overall robustness of cloud forensics. For example, Amazon S3 automatically generates an MD5 hash when an object is stored. IaaS offerings support on-demand cloning of virtual machines. As a result, in the event of a suspected security breach, a customer can take an image of a live virtual machine for offline forensic analysis, which results in less downtime. Also, using multiple image clones can speed up analysis by parallelizing investigation tasks. This enhances the analysis of security incidents and increases the probability of tracking attackers and patching weaknesses. Amazon S3, for example, allows customers to use versioning to preserve, retrieve and restore every version of every object stored in an S3 bucket. An Amazon S3 bucket also logs access to the bucket and objects within it. The access log contains details about each access request including request type, requested resource, requester's IP address, and the time and date of the request. This provides a wealth of useful information for investigating anomalies and incidents.

- **Scalability and Flexibility:**

Cloud computing facilitates the scalable and flexible use of resources, which also applies to forensic services. For example, cloud computing provides (essentially) unlimited pay-per-use storage, allowing comprehensive logging without

compromising performance. It also increases the efficiency of indexing, searching and querying logs. Cloud instances can be scaled as needed based on the logging load. Likewise, forensic activities can leverage the scalability and flexibility of cloud computing.

- **Policies and Standards:**

Forensic policies and standards invariably play catch-up to technological advancements, resulting in brittle, ad hoc solutions. However, cloud computing is still in the early stage and a unique opportunity exists to lay a foundation for cloud forensic policies and standards that will evolve hand-in-hand with the technology.

- **Forensics as a Service:**

The concept of security as a service is emerging in cloud computing. Research has demonstrated the advantages of cloud-based anti-virus software and cloud platforms for forensic computing. Security vendors are changing their delivery methods to include cloud services, and some companies are providing security as a cloud service. Likewise, forensics as a cloud service could leverage the massive computing power of the cloud to support cyber crime investigations at all levels.

## 5. CONCLUSION

Cloud computing delivers its low cost services through the use of large data centers for storage in different jurisdictions with multi-tenant hosting by virtual servers. These are the factors that creak challenges for digital forensics since the locations of data and its replicas (for backup reasons) are unknown. Plus these data are stored in different jurisdictions where different laws regarding the data access may apply. Also the ownership of these data is in question due to sharing the resources (multi-tenancy). Traditional digital forensics is not able to coexist with cloud technology, therefore cloud forensics as a new concept should be developed in different directions including technical, legal and structural aspects.

Opportunities and Challenges of cloud forensics were discussed in order to overcome the difficulties in the forensics investigation procedures in cloud computing, the following steps are recommended by this report:

1. Reconstructing the guidelines for cloud forensics as well as revising regulations and laws regarding the digital forensics in cloud computing

2. The development of Forensics as a Service in cloud computing (by cloud developers) in order to employ fast and reliable procedures for investigations.

3. Revising the Service Level Agreement in a committee including a representative of consumers, cloud providers, digital forensics experts, and legal advisers. SLA should be provided in a way that assists digital forensic investigators while there is no breach of privacy or regulation

4. Attempts should be made to regulate internationally the use of cloud computing services therefore; the forensic investigators have no limitation in different jurisdictions (towards harmonization). Furthermore, research must be conducted in order to develop new cloud-based forensic tools to effectively and efficiently facilitate the forensic investigations.

## REFERENCES

[1] Mell P., Grance T., “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, NIST, U.S Department of Commerce,2009.

[2] Popovic K., Hocenski Z., “Cloud Computing Security Issues and Challenges”, IEEE Press, MIPRO 2010, Opatija, Croatia, pp. 345-349, 2010.

[3] Lawton George, “Cloud Computing Crime Poses Unique Forensics Challenges”, 2011, Online available: <http:// searchcloudcomputing.techtarget.com/feature/Cloudcomputing-crime-poses-unique-forensics-challenges>

[4] Reilly D., Wren C., Berry T., “Cloud Computing: Forensic Challenges for Law Enforcement”, Internet Technology and Secured Transactions (ICITST), IEEE Press, London, 2010.

[5] Fu X., Ling Z., Yu W., and Luo J., “Cyber Crime Scene Investigations (C2SI) through Cloud Computing”, Int. Con. On Distributed Computing Systems Workshops, IEEE press, pp. 26-31, 2010.

[6] Gregg Michael, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Online available: <http://www.globalknowledge.ae/PDF/WP_VI_10SecurityConcernsCloudComputing.pdf>

[7] Jamil D., Zaki H., "Cloud Computing Security", Int. Journal of Eng. Sc. and Tech (IJEST), vol. 3, pp. 3478-3483, 2011 Online available < http://www.ijest.info/docs/IJEST11-03-04-129.pdf>

[8] Podhradsky A., Casey C., "Digital Forensic Challenges in a Cloud Computing Environment", 2011, Online available <http://searchcloudsecurity.techtarget.com/tip/Digital-forensicchallenges-in-a-cloud-computing-environment>

[9] Ruan K., Carthy J., Kechadi T., Crosbie M., "Cloud forensics: An Overview", Centre for Cybercrime Investigation, UniversityCollegeDublin,2011:<http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf>

[10] Carmenatty E., "Cloud Computing a Forensics Immature Technology", A Unit of Knowledge (KNOL), July 2010, < http://knol.google.com/k/cloud-computing-a-forensicsinmature-technology#>

[11] Ruan K., Baggili I., Carthy J., Kechadi T., "Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary analysis", University College Dublin, Zayed University, 2011.

[12] <http://www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf>

[13] Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing V21", December 2009, Online < https://cloudsecurityalliance.org/csaguide.pdf>

[14] Wolthusen Stephen, "Overcast: Forensic Discovery in Cloud Environment", Norwegian Information Security Laboratory, IEEE press, pp. 3-9, 2009.

[15] Delport W., Olivier M., and Kohn M, "Isolating a Cloud for a Digital Forensic Investigation", Information and Computer Security Architectures Research Group, Dept. of Computer Science, University of Pretoria, South Africa, August 2011.

[16] [20] Bursztein E., Fontarensky I., Martin M., and Picod J.,"Doing Forensics in the Cloud Age OWADE: Beyond Files Recovery Forensic", 2011. < http://cdn.ly.tl/talks/owadepaper.pdf>

[17] Birk D., "Technical Challenges of Forensic Investigations in Cloud Computing Environments", 2011:< http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf>

[18] Burke W., Baving R., "Cyber Forensics in the Cloud: Challenges and Best Practice", Sequirt CSi BV, 2011.

[19] <http://www.hackerhalted.com/Portals/3/Docs/Presentation%20Slides/Cyber-Forensic-in-The-Cloud-day3-Wayne-Burke.pdf>

[20] Lee J., Hong D., "Pervasive Forensic Analysis based on Mobile Cloud Computing", Electronics and Telecommunications Research Institute (ETRI), IEEE press, pp.572-576, 2011.

[21] Zhu Meng, "Mobile Cloud Computing: Implications to Smartphone Forensic Procedures and Methodologies", Msc Thesis, Auckland University of Technology, 2011.

[22] National Digital Forensics, Inc, 2009.