UNDERSTANDING THE DIGITAL FORENSICS FRAMEWORK OF CLOUD COMPUTING-CLOUD FORENSICS

Written by ***Parvathi S Shaji***

Lecturer, Department of Law, University of Kerala

ABSTRACT

As cloud services become a mainstream Information and Communication Technology (ICT) solution for business, consumers and governments, security and privacy issues assumes increasing significance. But on the other side of the coin, cloud services are used for criminal activities, or targeted by organized crime, then public Law Enforcement Agencies (LEAs) will want and need to obtain access to data held in cloud services for forensic purposes during the course of an investigation. Such forensic data may be held on systems controlled by a suspect, victim, or an innocent third party, often located in foreign jurisdictions or where the location is unknown. However, the potential for LEA can generate its own commercial security and privacy concerns for cloud users. Indeed there raises a number of technological, economic, legal, security and environmental questions. Further creating new challenges for managing cyber criminality, as cloud computing naturally becomes a new playing field for cybercriminals. Eventually, these groups and individuals see in the cloud opportunities for the automation of cybercrimes, optimized spreading of malware, or the hijacking of data and programmes belonging to cloud clients. Thus, standing at the point of multifarious concerns at hand, the cyber investigation in cloud computing is an area of greater concern, as technological need of man is unending. Functionality of Law Enforcement Agencies paves way for myriads of forensic challenges and the matter to be analysed. The discovery and acquisition of evidence in remote, elastic, provider controlled cloud computing platforms differ from that in traditional digital forensics, and examines lack of appropriate tools for these tasks.

INTRODUCTION

Cloud computing technology is a rapidly growing field of study, which relies on the sharing computer resources rather than having local servers or personal devices to handle applications. Most of the growth in this field is due to transfer of the traditional model of IT services to a novel model of cloud and the ease of access to electronic and digital devices. The internet has travelled from the concept of parallel computing to distributed computing, grid and recently to cloud computing. Cloud computing has become one of the most controversial issues in information technology field that cause to shift many organizations towards transferring their data to the cloud as it presents many promising technical and economic benefits.[i]

Recent interest in cloud computing has been driven by new offerings that are attractive due to peruse pricing and elastic scalability, providing a significant advantage over the typical acquisition and deployment of equipment that was previously required. The effect has been a shift to outsourcing of not only equipment setup, but also the ongoing IT administration of the resources as well.[ii]

Nowadays, digital devices are advancing rapidly. Data generated by these devices require an enormous amount of computational power to analyze them. The concept of cloud forensics is proposed and aims to allow an investigator to focus solely on investigation process in a cloud environment. Cloud computing posed a critical risk and challenges to digital investigators, but provides a plenty of opportunities for improving the digital forensics. Moreover, cloud service providers (CSP's) and customers have yet to establish adequate forensic capabilities that could support investigations of criminal activities in the cloud.[iii]Cloud forensics is a subset of network forensics[iv] and a cloud computing is based on broad network access. Therefore, cloud forensics follows the main network forensics with techniques tailored to cloud computing environments.[v]To ensure service availability and cost effectiveness, Cloud Service Providers (CSP's) maintain data centres around the world. Data stored in one data centre is replicated at multiple locations to ensure abundance and reduce the risk of failure. Also, the segregation of duties between CSP's and customers with regard to forensic responsibilities differ according to the service models being used. Adding to it, multiple jurisdiction and multi tenancy are the default settings for cloud forensics, creating additional legal challenges. Further sophisticated interactions between CSP's and customers, resource sharing by multiple tenants and collaboration between international law and enforcement agencies are required in most cloud forensics investigations.

DEFINING CLOUD COMPUTING – THE NEW VIRTUAL REGIME

In the last one to two decades, computing[vi] applications have increasingly used applications that are not on the user's computer but that are located somewhere with application services providers, which offer services via the Internet. Increasingly, these providers do not merely store data on a local server, but in a distributed way across several servers or server parks. At some point, this model was termed cloud computing, in which the term cloud is based on the custom, in pictures of computing models, of using a cloud to graphically represent the network in which data processing takes place. Cloud computing to put it simply means Internet Computing. The internet is commonly visualized as clouds; hence the term cloud computing for computation done through the Internet.[vii] Although the model of remote and distributed services is not new, the combination of characteristics of present-day cloud computing causes new challenges in many fields. The special combination of characteristics is captured in the US standardisation institute NIST's[viii] definition of cloud computing as

"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[ix]

In simpler terms, cloud computing can be described as 'a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements.[x]

Cloud Based Applications

The various typical cloud-based applications include the following services which are available at myriad platforms:

A. Cloud e-mail service:

There are thousands if not millions of companies that provide separately branded cloud-based email services. There is currently a very low barrier to entry for this market because web-based email is now available as an open source platform, which means that the core software to run an enterprise class web mail server can be obtained for no cost. The popular ones include Gmail, Hotmail, Lycos Mail, AOL, Rediff Mail, etc. This is often done as a complement to the storage of the same email in the cloud. With so many offerings available, users can sign up for multiple email accounts from any email service around the world. Therefore regulations (such as those in Europe) that require data be stored within certain geographical boundaries are not practically enforceable.[xi] For example, even if a large cloud based email provider, such as Hotmail, Gmail, or AOL, were to comply by hosting some of its servers in a given country, there is simply no way to impose such a requirement on the thousands of other cloud based email providers. In other words, there is no effective way to require, across the board, that all the world's cloud services store their data in any given country, that is not the way that the architecture of the Internet was developed, and it is not the way that email and other cloud based services work.

B. Cloud based business and personal organizational tools:

Thousands of cloud-based opportunities are available in order to help individuals and businesses aggregate their use of the web, to make business plans, to make vacation plans, parties, weddings etc. For example, Evernote[xii] is a service that allows users to capture anything, remember everything and access anywhere. This service aggregates information from users and businesses, including photos, plane tickets, notes, research and other materials, all on Evernote's servers. Finally, there are several more excellent cloud-based collaboration suites that offer the opportunity for companies to share their most important data with each other and with customers, such as Huddle, with virtual opportunities for file sharing, discussion boards, work spaces and other collaborative tools. If it appears that the lines are blurred between cloud-based services as those described above and the Internet itself that's because there are no lines. The "Web 2.0"[xiii] services that empower people to compute from any device, anywhere, and to interact with any business and with each other bring tremendous value to businesses and individuals.

C. Social networking, photos, and storage:

Social networking is big business. Recent market valuations of the well-known site Facebook have cited the value of the upcoming IPO as high as $100 Billion.[xiv] The rationale for this valuation is not just based on consumer usage it’s the vast amount of information contained within the Facebook cloud and the value that businesses and users place on it. The most valuable family photos are no longer stored away in an album or shoe box, they are in the cloud, stored on sites such as Picasa,[xv] Flickr,[xvi] Apples’ iCloud[xvii] and many other locations. In addition to the value-added services, there are a number of services that offer hard drive replacement in the cloud, for example, Dropbox,[xviii] Jungle Disk,[xix] Amazon S3,[xx] Egnyte,[xxi] and many others.

D. Banking and money management:

Most banking happens in the cloud. Almost all banks offer users the opportunity to complete online payment transfers, pay bills, purchase and sell stocks, and other activities and in many cases, it has completely replaced the need to either visit a physical bank branch or to keep paper based transactions in many countries, there simply isn’t a need to maintain paper banking records at all. Additionally, there are several suites of cloud-based services that help individuals and businesses manage their money, in a trend that has been called Banking 2.0.[xxii] Cloud-based banking products include Quicken,[xxiii] Mint,[xxiv] Wesabe,[xxv] Geezeo,[xxvi] Xero[xxvii] and others. Many of these suites either integrate data with or share data in some way with other cloud-based suites that can help with tax preparation and filing, such as TurboTax. In sum, the banking and financial ecosystem has completely moved to the cloud, such that individuals and businesses can practically maintain all of their record’s daily transactions, financial planning, taxes, stock trades all via the cloud.

E. Office software tools:

Companies such as Google offer a broad base of business productivity tools and office software replacements in the cloud. Google Apps, for example, is an enterprise-ready suite of applications that includes Gmail, Google Calendar,[xxviii] Google Docs[xxix] and Spreadsheets,[xxx] Google Sites[xxxi] and Google Video[xxxii] . These web-based services can be securely accessed from any browser, work on mobile devices such as BlackBerry and iPhone, and integrate with other popular email systems such as Microsoft Outlook, Apple Mail, and more.

F. E-commerce:

The cloud can enable businesses to set up a completely virtual business presence without the need for any infrastructure. Amazon and eBay offer virtual store fronts that enable cloud-based presentation, advertising, search, and payment processing and delivery. Products such as Google Apps have powered companies such as Open Entry, which offers free e-commerce catalogs to artisans and Small and Medium Enterprises (SMEs) worldwide that includes catalogs managed by Google spreadsheets, images stored on Picasa Web Albums and payments by Google Checkout.[xxxiii]

The Cloud Computing Entities:

The three-layer models of cloud computing entities include a client, a cloud service provider, a cloud host company.

A Client is an entity that uses the service from the provider to solve their business computing problems. It can be considered as an end user. The Consumer access the provider's service, either through the API[xxxiv] or Internet Connection. A cloud consumer is charged on the basis of usage according to Pay per use Model.

A Provider is usually a third party that makes services available for a customer. A cloud service provider working as a bridge between the end user and the cloud Host Company. It maintains the required infrastructure and capabilities to deliver service to the customer. The capabilities vary based on the type of cloud service the provider delivers.

A Cloud Host Company is an intermediary that works on the behalf of Cloud consumers to deal with the provider. It helps the consumer to architect the right system on a cloud provider, and assists in all activities of a provider and consumer.[xxxv]

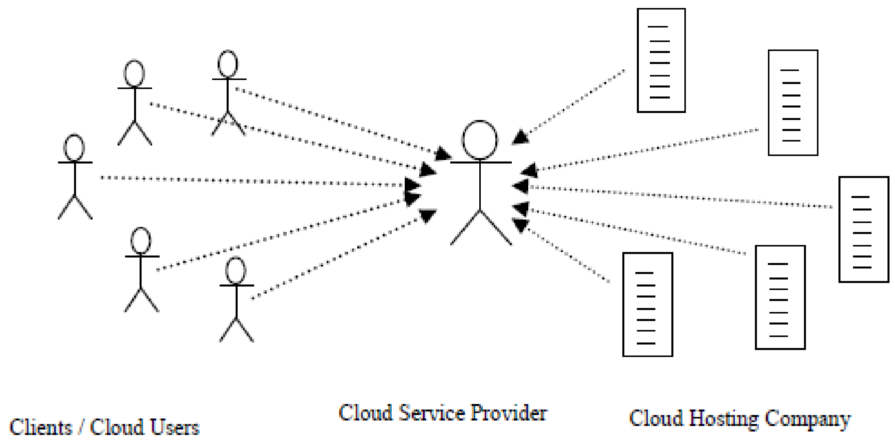


Fig 1(I) Cloud Computing Entities

Evolution of Cloud Computing

"Out of intense complexities intense simplicities emerge", as said by Winston Churchill, indeed the evolution of cyber space in which the development phase witnessed the switch over from in house generated computing power into utility supplied computing resources[xxxvi] delivered over the Internet as Web services, marked in path breaking transformation. In 1961, John Mc Carthy[xxxvii], presented the idea of computing as a utility much like electricity. Another pioneer who later developed the basis for the ARPANET[xxxviii], the Department of Defense's Advanced Research Projects Agency Network, and precursor to the Internet, was J.C.R.Licklider[xxxix]. In the 1960s, Licklider promulgated ideas of both ARPANET and BBN Technologies[xl], the high technology research and development company, that envisioned networked computers at a time when punched card[xli], batch computing[xlii] were dominant.[xliii]

With the rapid evolution of technological advancement, the multi infrastructure companies and other entities are timely responding with creative business models and exciting ways to reach markets. But major technological switch over and with the influx of information the platforms of businesses entities are facing new revolution: "The Cloud".

Phases of Cloud Computing Evolution:

The evolution of Cloud can be analyzed in three phases:

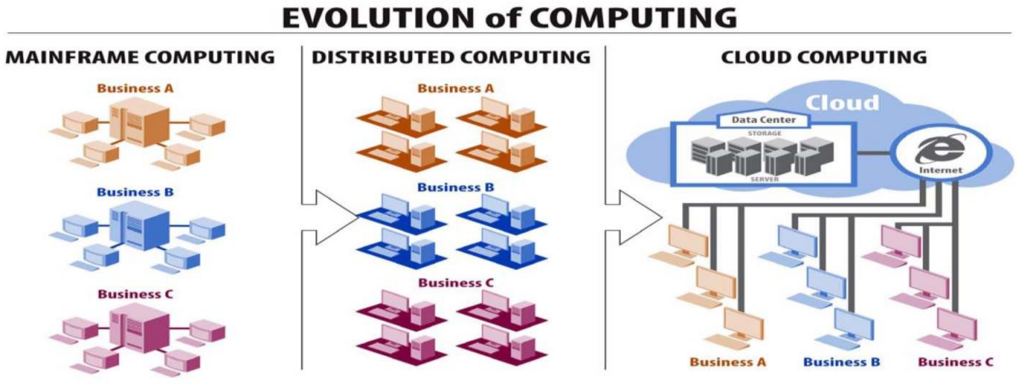


Fig 1(Ii) Evolution of Computing

Phase I of the evolution is the Mainframe computing, in the beginning days, the companies powered their information infrastructure from a mainframe. In one physical location (i.e., a building or an office), this large, powerful computer stored data and ran all the software applications. While it was relatively easy to support multiple applications through one mainframe, maintaining such a large piece of hardware was expensive and inefficient. There existed only few options available to companies that wanted to automate their business. The first being that each company to own their own mainframe environment. But the maintenance of this environment, however, proved as significant of a challenge as maintaining the application itself either it be hardware or software had to be maintained, draining company resources in terms of physical space, staffing, power, cooling, etc. Additionally, as the mainframe grew in functionally and in size, a company might need to hire an entire staff specifically to manage mainframes. Today, as technologies have evolved away from this architecture, there is a lack of expertise in this area. The second option being to rent server/storage space from a third-party vendor and use their larger mainframe to run applications. The unscalable and inflexible nature of the mainframe due to cost limitations associated with hardware, however, negated any potential cost benefits.

Phase II of the evolution is Distributed computing, in this phase as more people wanted access to more powerful applications, mainframe computing became less effective. The next solution for businesses was to replace the mainframe with multiple cheaper computers, each with enough computing power to store data and run applications. In a sense, this computing solution was easier to manage whereas one bug within the mainframe could down every computer relying on it, each cheaper computer ran independently. However, there existed ambiguity in this phase also, as the independence meant that computers didn't coordinate each other. Data sharing was difficult and any resources saved were negated because each computer had to be changed or fixed or updated individually.

Phase III is the Cloud computing, and in this phase out throwing the shortcomings persisted there emerged the third phase i.e., cloud computing era. As a very general definition, the cloud is a shared network of computers through which people and companies store data and run software. As its core, the cloud is data centre, a physical building with hardware and software running on that hardware, connected by pipes and routing to many, many computers. CSP's, who manage and maintain these networks, offer services rather than products in that clients are allowed to access and use the cloud, but they do not own any part of it and there is no software or hardware installation

Thus, the mainframe computing offered for a centralized management, as all the data and applications were centered in the mainframe. However, mainframes and their maintenance were extremely expensive that only large, well established companies could afford mainframe computing. Whereas in the case of distributed computing, companies could buy cheaper, individual computers rather than paying for an expensive mainframe. This made computing scalable and thus more accessible to smaller companies. However, distributed computing still wasn't an ideal computing solution because without a way to centrally manage all the computers, it was too difficult to support. Hence, the advent of cloud computing offered the central management and coordination of mainframe computing with the affordability and scalability of distributed computing. It is therefore ideal computing solution for both large and small companies.

The whole idea of computing refers to fully virtualized model in which different useful functions are being delivered while hiding how their internal works. In reality the convergence of various advances lead to the advent of cloud computing.

ANALYZING THE DIFFERENT CONCEPTS IN RELATION TO CLOUD COMPUTING – A NEW VIRTUAL REGIME

In reality, there is nothing new in any of the technologies that are used in the cloud computing where most of these technologies have been known for ages. It is all about making them all available to the masses under the name cloud computing. Cloud is not simply the latest term for the internet, though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet. The cloud is where you go to use technology when you need it, for as long as you need it neither you install anything on your desktop, and you do not pay for the technology when you are not using it.

The cloud can be both software and infrastructure, it can be an application you access through the web or a server like Gmail and it can be also an IT infrastructure that can be used as per user's request. Whether a service is hardware or software, the following is a simple test to determine whether that service is a cloud service: If you can walk into any place and sit down at any computer without preference for operating system for browser and access a service, that service is cloud- based. Generally, there are three measures used to decide whether a particular service is a cloud service or not:

a. The service is accessible via a web browser or web services API.
b. Zero capital expenditure is necessary to get started.
c. You pay only for what you use.[xliv]

The basic idea behind the cloud computing is that the users of the cloud switch to computing practices on the cloud provider's machines in the cloud and thereby utilizing software that the user rents, instead of using their own hardware and software that they own. And thus, the data inputted by the user is processed by the cloud service provider according to the instructions of the user, and the output is then delivered back to the user[xlv]. Therefore, the service thus satisfies computing and storage needs from a virtually unlimited hardware and communication infrastructure, which is managed by a third-party provider.[xlvi]

Analysing further basic characteristics of cloud computing as enunciated by NIST[xlvii].Cloud computing features the five essential characteristics:

i. On demand self-service: Makes its viable for a consumer to automatically access the services without human interaction with each service provider
ii. Broad network access**:** **S**ince access is available over the network, it can be accessed through client platforms like mobile phone, tablets, laptops, and workstations.
iii. Resource Pooling: Since the cloud provider's resources are pooled to serve multiple consumers, it requires a dynamic assignment and reassignment of the different physical and virtual resources according to consumer demand.

iv. Rapid elasticity**:** Capabilities can be elastically provisioned and released and can be appropriated in any quantity at any time.

v. Measured service: Cloud systems automatically control and optimize resources use by leveraging a metering capability at some level of abstraction appropriate to the type of service[xlviii].Resource usage can be motivated, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

There are different deployment model and the service models which is being made available by the cloud service providers.

The deployments incorporated are as follows:

a. Private cloud: The cloud infrastructure[xlix] is operated solely for a single organization by a third-party organization, the organization itself or a combination of them, on or off premises.

b. Community cloud: The cloud is provisioned for exclusive use by a specific community of consumers from organization that have shared concerns.

c. Public cloud: The cloud is provisioned for open use by the general public. It may be owned, managed, and operated by a business or government organization, or some combination of them. It exists on the premises of the cloud provider.

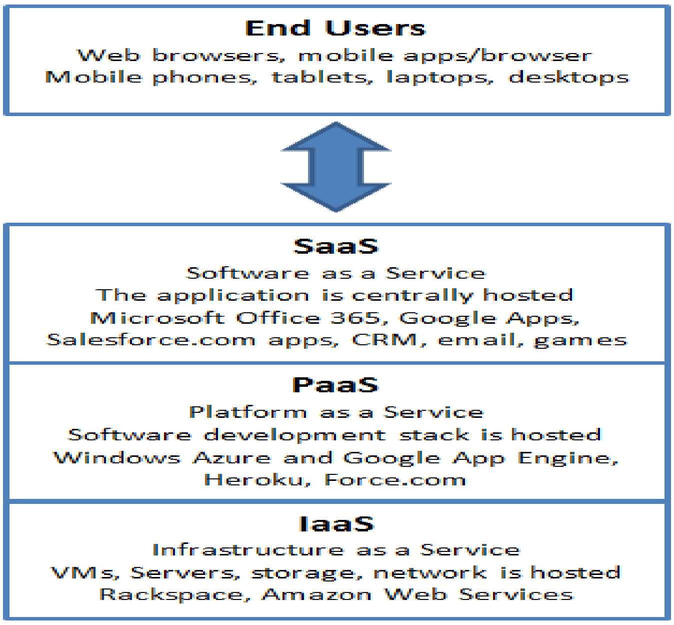
d. Hybrid cloud: The cloud infrastructure is a composition of two or more distinct clouds that remain separate entities, but become bound together by standardized technology that enables portability of data and application.

The service models included are as follows:

a. Software as a Service (SaaS): The consumer is allowed to use the provider's applications while running operations on the cloud infrastructure. The applications are accessible from various client devices. The cloud provider typically is responsible for both physical and logical security. SaaS is the top layer of the cloud, and it provides users with fully functioning applications that rest entirely on a cloud. Google Docs is an example of a SaaS[l]

b. Platform as a Service (PaaS): The cloud provider will supply the user with computing and network resources and the licenses to use the available software tools necessary for the user to develop applications using programming language, libraries, services and tools that are supported by the provider. The user is responsible for the application that is created and deployed in this environment. PaaS thus offers an environment where developers create and host web applications. Google App Engine is an example of a PaaS.

c. Infrastructure as a Service (IaaS): The cloud provider rents computing and network resources to the user and will only assume responsibility for the physical security of the environment and the availability of the infrastructure (electricity, network connectivity and server availability). It is the user's responsibility to implement appropriate application and database security mechanisms as well as security and regulatory compliance associated with them, since he will have complete control over applications, and thus represent the bottom layer of the cloud. Amazon web services mainly offers IaaS



End Users
Web browsers, mobile apps/browser
Mobile phones, tablets, laptops, desktops

SaaS
Software as a Service
The application is centrally hosted
Microsoft Office 365, Google Apps,
Salesforce.com apps, CRM, email, games

PaaS
Platform as a Service
Software development stack is hosted
Windows Azure and Google App Engine,
Heroku, Force.com

IaaS
Infrastructure as a Service
VMs, Servers, storage, network is hosted
Rackspace, Amazon Web Services

Fig 1(Iii) Service Models[li]

Therefore, cloud computing technologies have significant potential to revolutionize the way organizations provision their information technology infrastructure. Migrating to cloud computing involves replacing much of the traditional IT hardware found in an organization's data center including servers, racks, network switches and air conditioning units with virtualized, remote, on- demand software services, configured for the particular needs of the organization.[lii]

DEFINING CLOUD FORENSICS

NIST defines digital forensics as an applied science for “the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”.[liii]

Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, organization and reporting of digital evidence. In each step there are tools and techniques available. Traditional methods and tools of forensics cannot cope up with the cloud forensics because of the fact that the retrieval of the information, the major lead of any case, is diversely located and hence difficult to reach. Cloud computing is based on extensive network access, and network forensics handles forensic investigation in private and public networks. However, cloud forensics also includes investigating file systems, process, cash, and registry history. Every data is important for the investigation. So, in the collection phase, goal is to collect as much as data which is relevant to the investigation.[liv]

EVOLUTION OF CYBER FORENSICS

There exists a need to study the evolution of cyber forensics before examining the concept of cloud forensics. In the mid 1960’s Donn Parker noticed the phenomenon that when people entered the computer center, they left their ethics at the door[lv].On a simple note computer forensics emerged out of the need to solve, document and enable prosecution of computer crime. Further in the 1970s and 1980 relatively personal computers became common and individuals and businesses began to use them on a regular basis. Thus, subsequently law enforcement agencies noticed the emergence of a new class of crime i.e., computer related crime. The emergence of computer forensics was largely in response to a demand for service from the law. By the 1990s Law Enforcement Agencies[lvi] in every technologically advanced country were aware of computer crime, and had a system in place to investigate and to prosecute such activities. Many research centers and scientific groups were also formed, and the software industry started to offer various specialized tools to help in investigating computer crimes[lvii].

For early investigators involved in computer related crimes it became immediately obvious that if their response and findings were to be of any use as court evidence they had to comply with the same rules as any other conventional investigations. The first thing every investigator has to be aware of is Locard's exchange Principle:

"Anyone or anything entering a crime scene takes something of the scene with them, or leaves something of themselves behind with they depart *"*[lviii]

Thus, it became clear that when investigating computer related crime, the same basic rules applied as in a non-computer related crime scene investigation. The investigation process includes phases of physical scene preservation, survey and reconstruction using collected evidence, all of which is formally documented.[lix]

The first computer forensics training course appeared around 1989 at University of North Texas and the first International law Enforcement Conference on Computer Evidence was hosted in 1993 in Australia. With all these developments at hand, computer forensics became a unique discipline of science, and in many areas, it requires a different approach, different tools, as well as specialized education and training. The first period in computer forensics history is characterized by dealing with relatively small capacity devices and a relatively small amount of information. Thus, paving way for the emergence of a new discipline.

PHASES IN A CLOUD FORENSICS

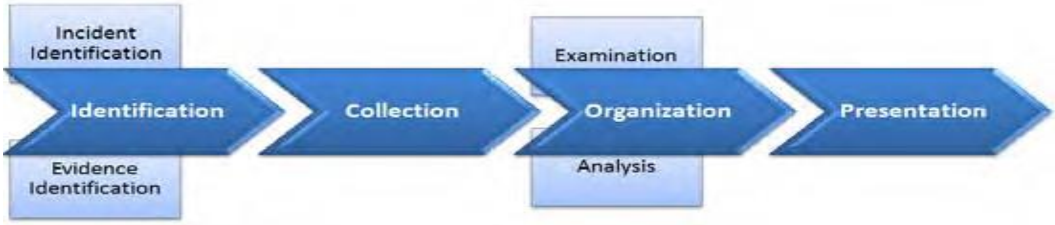


Fig 2 Different steps involved in Cloud Forensics[lx]

Phase 1 is identification of crime which is to ensure that actual crime has happened. Evidences involved in crime are identified in this step.

Phase 2 is known as Collection in which tasks performed under this phase is related to the acquiring, collecting, transporting, storing and preserving of data from all possible electronic devices. In general, this phase is where all relevant data are captured, stored and be made available for the next phase.

Phase 3 is organization, which is the main and the center of the computer forensic investigation processes. It has the greatest number of phases in its group. Thus, reflecting the focus of most models reviewed are indeed on the analysis phase. Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime.

Phase 4 is known as Presentation**,** which includes **t**he finding from analysis phase are documented and presented to the authority. Obviously, this phase is crucial as the case must not only be presented in a manner well understood by the party presented to, it must also be supported with adequate and acceptable evidence. The main output of this phase is either to prove or disprove the alleged criminal acts.

Chain of custody should clearly depict how the evidence was collected, analyzed, and preserved in order to be presented as admissible evidence in court. Chain of custody is one of the most vital issues throughout the entire process. An alleged suspect may claim that the evidence contains information of other users, not her. In this case, the investigator needs to prove to the court that the provided evidence actually belongs to the suspect. Moreover, in the cloud, we need to preserve the privacy of other tenants.

CLOUD FORENSICS, NEED FOR A SEPARATE ENTITY

Technology is a double edged sword that can be used in economic sustainability, to assist in the arrest of cyber criminals etc., and there are various tools that can assist LEAs in investigating cybercrime cases and in cybercrime evidence collection, drafting and creating hard evidence, however the same technology may be used by cyber criminals to commit offences worse still the forensic tools may be used by these cyber criminals to conceal their tracks for instance a criminal may use the disk wipers to clean the hard disks rendering forensic tools immobilized to recover evidence.[lxi]

There are major investigate contingents that arise the requirements for forensic techniques and tools. The following institutional frameworks play a significant role as far this discipline is concerned:

i. Law Enforcement – focuses on gathering evidence
ii. Organizations, Business or e- commerce - for use in keeping the business on track using reasonably effective techniques and ensuring safe online purchasing.
iii. Academia-ensures accuracy of result driven from precise, repeatable methods.
iv. Prosecution - elaboration of the analysis in a court of law.
v. Judiciary- scrutinizing the findings against judicial standards.[lxii]

Further understanding the other aspects, computer forensics is primarily concerned with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place. In broad terms, a forensics life cycle involves the following phases:[lxiii]

i. Preparation and identification;
ii. Collection and recording;
iii. Storing and transporting;
iv. Examination/investigation;
v. Analysis, interpretation and attribution;
vi. Reporting;
vii. Testifying.

Preparing for the evidence & identifying the evidence:

When there exists an enormous amount of potential evidence available for a legal matter and it is also possible that the vast majority of the evidence may never get identified. If there exist a single computer or in case of networked environment, as in the former every sequence of events within a single computer might cause interactions with files they produce and manage, and log files and audit trails of various sorts and in case of latter it extends to all networked devices, potentially all over the world. Thus, definitely it's a matter of tedious task to prepare and identify the evidence.

Collecting and recording digital evidence:

Digital evidence can be collected from many sources[lxiv]. One of the most vital aspect is that special care must be taken when handling computer evidence as most digital evidence is easily changed, and once changed it is usually impossible to detect that a change has taken place unless other measures have been taken. For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.[lxv]

Storing and transporting digital evidence:

In storage, digital media must be properly maintained for the period of time required for the purposes of trial. Depending on the particular media, this may involve any number of requirements ranging from temperature and humidity controls to the need to supply additional power or to read media. Storage must be adequately secure to assure proper chain of custody, and typically, for evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence must be kept to assure that evidence does not go anywhere without being properly traced.

Evidence is often copied and sent electronically, on compact disks or on other media, from place to place. Original copies are normally kept in secure location to act as the original evidence that is introduced into the legal proceedings. Therefore, adequate care must be taken in transportation to prevent spoliation as well.[lxvi]

Examining or investigating digital evidence:

As a general rule one should not examine digital evidence unless one has the legal authority to do so. For the purpose of digital evidence examination, "imaging of electronic media"[lxvii] becomes necessary. During imaging, a write protection device or application is normally used to ensure that no information is introduced onto the evidentiary media during the forensic process. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.[lxviii]

Analysis, interpretation & attribution:

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered in most forensics analysis. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence. However, the actual number of possible sequences may be almost unfathomably large. In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence. Basically, all digital evidence must be analyzed to determine the type of information that is stored upon it.

Reporting:

Once the analysis is complete, a report is generated. The report may be in a written form or an oral testimony or it may be a combination of the two. Finally, evidence, analysis, interpretation and attributions must ultimately be presented in the form of expert reports, depositions and testimony. The following are the broad elements of the report:

a. Identifying of the reporting agency;
b. Case identifier or submission number;
c. Case investigator;
d. Identity of the submitter;
e. Date of receipt;
f. Date of report;
g. Descriptive list of items submitted for examination, including serial number, make and model;
h. Identity and signature of the examiner
i. Brief description of steps taken during examination, such as string searches, graphics image searches and recovery erased files
j. Results or conclusions.[lxix]

Testifying:

This phase involves presentation and cross examination of expert witnesses. Depending on the country and legal frameworks in which a cybercrime is registered, certain standards may apply with regard to the issues of expert witnesses. Digital forensics evidence is normally introduced by expert witnesses except in cases where non- experts can bring clarity to non-scientific issues.

Thus, the chain of evidence and accuracy of digital evidence is very important in cyber forensics investigation. Therefore, experienced human investigators can often analyze crime trends precisely, but as the incidence and complexity of crime increase, human errors occur, analysis time increases and criminals have more time to destroy evidence and escape arrest. By increasing efficiency and reducing errors, crime data mining techniques can facilitate police and enable investigators to allocate their time to other valuable tasks.

Further as cloud services become a mainstream Information and Communication Technology (ICT) solution for business, consumers, and governments, security and privacy issues assume increasing significance. To the extent that cloud services are used for criminal activities, or targeted by organized crime, then public LEAs will want and need to obtain access to data held in cloud services for forensic purposes during the course of investigation. Such forensic data may be held on systems controlled by a suspect, victim, or an innocent third party[lxx], often located in foreign jurisdictions or where the location is unknown.[lxxi]

As in the technical issue it encompasses the procedure and tools that are needed to perform the forensic process in the cloud computing environment which includes data collection, evidence segregation, virtualized environment and proactive measures. As with respect to organizational level, in a cloud computing environment involves at least two entities: the CSP and the cloud customer. Further, the scope of the investigation widens when a CSP outsources services to other parties, thus adding to the existing challenges. The major element involved is the legal dimension of cloud forensics as it requires development of regulations and agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides. In addition, with respect to the confidentiality of other tenants that share the same infrastructure should be preserved. Thus, in cloud environment, the law enforcement agencies face challenges with respect to forensic data collection, live forensics, evidence segregation, virtualized environments, internal staffing, external dependency chains, service legal agreements, multiple jurisdictions and tenancy[lxxii]

VARIOUS REALWORLD CASES:[lxxiii]

Malware Injection:

On June 2011, the cyber criminals from Brazil who first launched their attacks as spam or phishing campaigns, where users were sent spoofed emails with links that look them to one of the malicious domains, created some major problems in Amazon Web Services[lxxiv]. The attackers installed a variety of malicious files on the victim's machines. Additional components that were downloaded during the attack attempted to retrieve login information from a list of nine Brazilian banks and two other international banks, steal digital certificates from eTokens stored on the machine, and collected unique data about the PC itself on the machine, and collect unique data about the PC itself that is used by some banks as part of an authentication routine.[lxxv]

Social Engineering Attack:

A social engineering attack is an intrusion that relies heavily on human interaction and often tricking other people to break normal security procedures[lxxvi]. It can happen in cloud computing. In August 2012, hackers used a social engineering attack to completely destroy technical writer Mat Honan's digital life by remotely deleting the information from his iPad, MacBook and iPod[lxxvii].

Account Hijacking:

In July 2012, Dropbox, the cloud storage service, confirmed that hackers used usernames and passwords stolen from third- party sites to access Drop boxer's account. It was altered after users complained about spam, they were receiving to email address used only for the Dropbox accounts. One stolen password was used to access an employee account that contains a file that included user email addressed. The company believed users who use the same password on multiple websites make it easier for hackers to access their accounts on other websites.[lxxviii]

Traffic Flooding:

In May 2011, LastPass, a cloud-based password storage and management company, announced a possible successful hack against its servers. There were no reports of any data leakage, but the company insisted that customer's take a few measures to ensure that their information is safe. Security experts discovered unusual behavior in the database servers that had more traffic going out compared to incoming data. The company presumed this was hacking activity related to siphoning stored login credentials and other sensitive user data. Master passwords, the passwords that protect lists of passwords to access other websites and online services in the cloud, were immediately changes protect customers from possible data leakage.[lxxix]

CONCLUSION

In the present scenario, indeed the whole advent of cloud computing is pushing the frontiers of digital forensics and certainly the realization for the law enforcement authorities for switching to more sophisticated technologies for facing the new- fangled challenges. The distinctive challenges which are just unique for cloud forensics includes data replication, location transparency, multi tenants, collection of trustworthy evidences etc. Are undeniably alerting the institutional frameworks to advance the efficacy and speed of forensic investigations.

With the increase in the momentum of switch over to new and advanced technologies, so do crimes. But on other side of the story, development of law lags and is not able to be in pace with technological advancements. Its high time law should intentionally address the contemporary problem at hand while retaining flexibility to adapt as technology evolves. Cloud services are so frequently hosted in other jurisdictions or other nations, that discovery, investigations and forensics may actually be obstructed more effectively. Without robust and enforceable memoranda of understanding (MOU) for law enforcement cooperation, it will become difficult to discover or forensically investigate any files stored outside the nation of litigation. Thus, it has reached its pinnacle to be in pace with the changing needs of the hour.

BIBLIOGRAPHY

Authored Books

i. Ian Walden, *Law Enforcement Access to Data in Clouds* in CLOUD COMPUTING LAW 285 (Christopher Millard ed., 2013).

ii. Ian Walden, *Law Enforcement Access to Data in Clouds* in CLOUD COMPUTING LAW 285 (Christopher Millard ed., 2013).

iii. NINA GODBOLE & SUNITA BELAPURE, CYBER SECURITY: UNDERSTANDING CYBER CRIMES, COMPUTER FORENSICS AND LEGAL PERSPECTIVES 342 (2011).

iv. RAJKUMAR BUYYA, JAMES BROBERG & ANDRZEJ GOSCINSKI, CLOUD COMPUTING PRINCIPLES & PARADIGMS 5 (2011).

v. Raun, Keyn,Joe Karby,Tahar Kechadi & Mark Crosbie, *Cloud forensics* in ADVANCES IN DIGITAL FORENSICS 361 (Peterson, Gilbert & Sujeet Shenoi eds , 2011).

vi. RICHARD SAFERSTEIN, FORENSIC SCIENCE HANDBOOK 37 (2001).

vii. RONALD L.KRUTZ & RUSSELL DEAN VINES, COMPREHENSIVE GUIDE TO SECURE CLOUD COMPUTING 1 (2010).

viii. Wuhan Hon & Christopher Millard, *Cloud technologies and Services,* in CLOUD COMPUTING LAW 3 (Christopher Millard ed., 2013).

Journal Articles

i. Asou Aminnezhad, Ali Dehghantanha, Mohd Taufik Abdullah, Mohsen Damshenas, *Cloud Forensics and Opportunities,* 4 IJIPM 76 (2013).

ii. Brian carrier, *Defining Digital Forensic examination and Analysis Tools using Abstraction layers*, 1 INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE 2 (2003).

iii. Chimere Barron, Huiming Yu & Justin Zhan, *Cloud computing Security Case Studies and Research,*2 PROCEEDINGS OF THE WORLD CONGRESS ON ENGINEERING 3- 5 (2013).

iv. D. Svantesson, R. Clarke, *Privacy and Consumer Risks in Cloud Computing*, 4 COMPUTER LAW & SECURITY REVIEW 391-397 (2010).

v. Daniel Buller and Mark Whinow, *Cloud Computing: Emerging Legal Issues, Data Flows and the Mobile Use,* 2 LANDSLIDE 54(2010).

vi. George Grispos, Tim Storer & William Bradley Glisson, *Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics,* 4 INTERNATIONAL JOURNAL OF DIGITAL CRIME AND FORENSICS 28-48 (2012).

vii. Gurmeet Singh & Vineet Kumar Sachdeva, *Impact & challenges of Cloud Computing in Current Scenario,* 1 INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH 131 (2012).

viii. Gurmeet Singh 7 Vineet Kumar Sachdeva, *Impact and Challenges of Cloud Computing in Current Scenario,* 1 INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLIANRY RESEARCH 132 (2012).

ix. Hassan, Qusay, *Demystifying The Cloud: The Cloud and DataHouse's Cloud Services*, 1 THE JOURNAL OF DEFENCE SOFTWARE ENGINEERING 16 (2011).

x. Jared A. Harshberger, *Cloud Computing Providers and Data Security Law*, 16 J.TECH.L & POLY 229 (2011).

xi. Josaih Dykstra & Alan T.Sherman, *Acquiring forensic from Infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques*, 9 DIGITAL INVESTIGATION 590- 598 (2012).

xii. Prasad Purnayae, *Cloud Forensics: Volatile Data Preservation*, 4 IJCSE 42 (2015).

Virginiah Sekgwathe & Mohammad Talib, Cyber Forensics: Computer Security and Incident Response, 2 IJNCAA 127-137 (2012).

xiii. Sun Joo Yoo & Wen-hao David Huang, *Comparison of Web 2.0 Technology Acceptance based on Cultural Differences*, 4 EDUCATIONAL TECHNOLOGY & SOCIETY 241- 252 (2007).

xiv. Vineeth Narayanan, *Harnessing the Cloud: International Law Implications of Cloud Computing* 12 CHI. J INT'L 783 (2012).

Online sources

i. Ahmed Mohamed Gamaleldin, *An Introduction to Cloud Computing Concepts*, available at http://www.secc.org.eg/recocape/SECC_Tutorials_

An%20Introduction%20to%20Cloud%20Computing%20Concepts.pdf (last updated 17 May ,2013).

ii. Arjit Paul, Mayuri Kiran Anvekar & K. Chandra Sekaran, *Cyber Forensics in Cloud Computing*, Computer Engineering and Intelligent Systems www.iiste.org , (last updated March 9, 2012)

iii. D. Fisher, *Attackers using Amazon cloud to host malware,* http://threatpost.com/en_us/blogs/attackers-using-amazon-cloud-hostmalware-060611. (last updated June 6, 2011).

iv. D. Kerr, *Dropbox confirms it was hackers, offers users help,* http://nws.csnet.com/8301-1009_3-57483998-83/dropbox-confirms-it-was hacked-offers-users-help/, (last updated July 17, 2012).

v. Ewa Huebner, Derek Bem & Oscar Bem, *Computer Forensics- Past, Present and Future*, 8 INFORMATION SECURITY TECHNICAL REPORT 32 (2007).

vi. George Simpson, *A Billion Here and a Billion There*, ONLINE MEDIA DAILY, http://goo.gl/ILKOQ, (last updated 4 July, 2011).

vii. J. Pepitone, *Hack attack expose major gap in Amazon and Apple security,* http://money.cnn .com/2012 /08/07 /technology/mathonan-hacked/index.htm., (last updated August 7, 2012).

viii. Kotenko, M. Stepashkin & E. Doynikova, *Security analysis of information systems taking into account social engineering attacks.* IEEE 19TH INTERNATIONAL EURIMICRO CONFERENCE ON PARALLEL, DISTRIBUTES AND NETWORK- BASED PROCESSING (2011)

ix. Michael G.Noblett, Mark M. Politt and Lawrence A. Presley, *Recovering and Examining Computer Forensic Evidence,* 2 FORENSIC SCIENCE COMMUNICATIONS 5 (2000).

x. Neil Robinson, Hans Graux, *Review of the European Data Protection Directive,* RAND EUROPEAN TECHNICAL REPORT , http://www.rand.org/pubs/technicaL _reports /TR710.html (last updated 8 January, 2009).

xi. Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing,* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf(last updated 6 September, 2011).

xii. Simpel Lean, *Cloud Entities: Cloud Computing Certification Training,* http://blog.simplilearn. com/it-service-management/cloud-entities , (last updated February 5, 2015).

xiii. Simpson, *Free e- commerce Catalogs Managed with Googledocs,* GOOGLE DOCS BLOG, February 3, 2010, http://gppgle/gyO6, (last updated Feb 3, 2010).

REFERENCES

[i] Asou Aminnezhad, Ali Dehghantanha, Mohd Taufik Abdullah, Mohsen Damshenas, *Cloud Forensics and Opportunities,* 4 IJIPM 76 (2013).

[ii] Gurmeet Singh 7 Vineet kumar Sachdeva, *Impact and Challenges of Cloud Computing in Current Scenario*, 1 INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLIANRY RESEARCH 132 (2012).

[iii] D. Svantesson, R. Clarke, *Privacy and Consumer Risks in Cloud Computing,* 4 COMPUTER LAW & SECURITY REVIEW 391-397 (2010).

[iv] Network Forensics deals with forensic investigation of networks.

[v] Ruan, Keyun, Joe Carthy, Tahar Kechadi & Mark Crosbie, *Cloud Forensics* in ADVANCES IN DIGITAL FORENSICS 361 (Peterson, Gilbert & Sujeet Shenoi eds., 2011).

[vi] Computing refers to any goal-oriented activity requiring, benefiting from, or creating algorithmic processes through computers. Computing includes designing, developing and building hardware and software systems; processing structuring, and managing various kinds of information; doing scientific research on and with computers; making computer systems behave intelligently; and creating and using communications and entertainment media, also see DAVID EVANS, INTRODUCTION TO COMPUTING- EXPLORATIONS IN LANGUAGE, LOGIC & MACHINES 1- 16(2011).

[vii] Gurmeet Singh & Vineet Kumar Sachdeva, *Impact & challenges of Cloud Computing in Current Scenario,* 1 INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH 131 (2012).

[viii]The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory, also known as a National Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

[ix]Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing,* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last updated 6 September, 2011).

[x]Wuhan Hon & Christopher Millard, *Cloud technologies and Services,* in CLOUD COMPUTING LAW 3 (Christopher Millard ed., 2013).

[xi]In 1995, the European Parliament and Council adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive applies to all 27 member states of the European Economic Area (EEA). Several sources have noted that the Directive has significant weaknesses and that have many aspects of it are ineffective. Also see Neil Robinson, Hans Graux, *Review of the European Data Protection Directive*, RAND EUROPEAN TECHNICAL REPORT , http://www.rand.org/pubs/technicaL _reports /TR710.html (last updated 8 January, 2009).

[xii] Evernote is an American independent, private company offering a closed source premium suite of software and services, designed for note taking and archiving. The company's flagship product allows users to create a note which can be a piece of formatted text, a full webpage or webpage excerpt, a photograph, a voice memo, or a handwritten ink note. Notes can also have file attachments. Notes can be sorted into folders, tagged, annotated, edited, given comments, searched, and exported as part of a notebook. Evernote supports a number of operating system platforms (including OS X, iOS, Chrome OS, Android, Microsoft Windows, Windows Phone, BlackBerry, and web OS) and also offers online synchronization and backup services.

[xiii] Web 2.0 is the term used to describe a variety of web sites and applications that allow anyone to create and share online information or material they have created. A key element of the technology is that it allows people to create, share, collaborate & communicate. Web 2.0 differs from other types of websites as it does not require any web design or publishing skills to participate, making it easy for people to create and publish or communicate

their work to the world. Also see, Sun Joo Yoo & Wen-hao David Huang, *Comparison of Web 2.0 Technology Acceptance based on Cultural Differences*, 4 EDUCATIONAL TECHNOLOGY & SOCIETY 241- 252 (2007).

[xiv]George Simpson, *A Billion Here and a Billion There*, ONLINE MEDIA DAILY, http://goo.gl/ILKOQ, (last updated 4 July, 2011).

[xv] Picasa is an alternative service from Google, a desktop app that organizes the photos on your computer and can backup those files to Google Photos. If you're looking for old-school tools, like burning photos to a disc or batch editing, Picasa can help.

[xvi] Flickr is one of the top names in photo storage. The service offers a lot of flexibility to how you can use it. Storage seekers can organize their photos into albums (dubbed sets) and further organize those albums into collections.

[xvii] Apple's cloud-based photo offering is a solid choice. The iCloud Photo Library, which is part of the larger iCloud storage service, can back up every photo you take.

[xviii] Dropbox is a file hosting service operated by Dropbox, Inc., that offers cloud storage, file synchronization, personal cloud, and client software.

[xix] Jungle Disk is an online backup tool that stores its data in Amazon S3 or Rackspace Cloud Files. The basic Jungle Disk software is sold as a monthly subscription model, and the customer has the option to be billed directly by Jungle Disk or they can choose Amazon Payments.

[xx] Amazon S3 (Simple Storage Service) is an online file storage web service offered by Amazon Web Services

[xxi] Egnyte provides Adaptive Enterprise File Services for businesses. The company stands apart from other cloud-based file-sharing services by being able to store files on a company's existing data center infrastructure, as well as cloud storage. Egnyte integrates with any cloud, storage, device and business application, giving customers ultimate control of where their data exists. That means companies can keep working with the gear they've invested in. With its approach, Egnyte is trying to make itself as friendly as possible to both IT and end users, finding the perfect balance between the two.

[xxii] BANK 2.0 which is a new platform will show bankers that such changes, although inevitable, will bring reduction in costs, longer-term and more profitable customer relationships, and will improve the effectiveness of the organization structure. It just may be extremely painful for those who don't get the future, despite all the benefits Banking 2.0 services includes: Social Media Planning and Management, Business Development Plans, Build Sales Models, Sales Plan Execution, M&A Advisory (Buy and Sell), Data Analytics (Big Data), The Collective Advantage (TCA) Consortium, also see BRET KING & MARSHALL CAVENDISH, BANKING 2.0 – HOW CUSTOMER BEHAVIOUR AND TECHNOLOGY WILL CHANGE THE FUTURE OF FINANCIAL SERVICES 14 (2010).

[xxiii] Quicken is a personal finance management tool developed by Intuit, Inc. Different (and incompatible) versions of Quicken run on Windows and Macintosh systems.

[xxiv] Mint's primary service allows users to track bank, credit card, investment, and loan transactions and balances through a single user interface as well as make budgets and goals

[xxv] Wesabe was a personal finance management website established in December 2005 that analyzes a user's financial data to provide appropriate advice on how to save money.

[xxvi] Geezeo is an application that helps members develops and maintains their budget, while also working with other members to stick to and improve their financial situation.

[xxvii] Xero is a New Zealand-based software company that develops cloud-based accounting software for small and medium-sized businesses Its products are based on the software as a service (SaaS) model and sold by subscription, based on the type and number of company entities managed by the subscriber.

[xxviii] Google Calendar, form of shared calendar system is a time-management web application and mobile app for created by google. The interface of Google Calendar is similar to desktop calendar applications such as Microsoft Outlook or iCal on Mac OS X

[xxix] Google Videos (originally Google Video) is a video search engine from Google. It was formerly a free video-sharing website and allowed selected videos to be remotely embedded on other websites and provided the necessary HTML code alongside the media, similar to YouTube. This allowed websites to host lots of video remotely without running into bandwidth or storage-capacity issues.

[xxx] Google Docs, Sheets and Slides are a word processor, a spreadsheet and a presentation program respectively, all part of a free, web-based software office suite offered by Google within its Google Drive service. The suite allows users to create and edit documents online while collaborating with other users in real-time.

[xxxi] Google Sites is a structured wiki and Web page creation tool offered by Google as part of the Google Apps for Work productivity suite. The goal of Google Sites is for anyone to be able to create a team oriented site where multiple people can collaborate and share files.

[xxxiii]Dan Simpson, *Free e- commerce Catalogs Managed with Googledocs,* GOOGLE DOCS BLOG, February 3, 2010, http://gppgle/gyO6, (last updated Feb 3, 2010).

[xxxiv] API is an abbreviation of application program interface, is a set of routines, protocols, and tools for building software applications. The API specifies how software components should interact.

[xxxv]Simpel Lean, *Cloud Entities: Cloud Computing Certification Training,* http://blog.simplilearn. com/it-service-management/cloud-entities , (last updated February 5, 2015).

[xxxvi] RAJKUMAR BUYYA, JAMES BROBERG & ANDRZEJ GOSCINSKI, CLOUD COMPUTING PRINCIPLES & PARADIGMS 5 (2011).

[xxxvii]John McCarthy (September 4, 1927 – October 24, 2011) was an American computer scientist and cognitive scientist. McCarthy was one of the founders of the discipline of artificial intelligence. He coined the term artificial intelligence (AI), developed the Lisp programming language family, significantly influenced the design of the ALGOL programming language, popularized timesharing, and was very influential in the early development of AI.

[xxxviii]The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet. ARPANET was initially funded by the Advanced Research Projects Agency (ARPA, later Defense Advanced Research Projects Agency, and DARPA) of the United States Department of Defense.

[xxxix] Joseph Carl Robnett Licklider (March 11, 1915 – June 26, 1990), known simply as J. C. R. was an American psychologist and computer scientist who are considered one of the most important figures in computer science and general computing history. He is particularly remembered for being one of the first to foresee modern-style interactive computing and its application to all manner of activities; and also as an Internet pioneer with an early vision of a worldwide computer network long before it was built. He did much too actually initiate this by funding research which led to much of it, including today's canonical graphical user interface, and the ARPANET, the direct predecessor to the Internet.

[xl] BBN Technologies (originally Bolt, Beranek and Newman) is an American high technology company which provides research and development services. BBN is based next to Fresh Pond in Cambridge, Massachusetts, USA. It is a military contractor, primarily for DARPA, and also known for its 1978 acoustical analysis for the House Select Committee on the assassination of John F. Kennedy.BBN of the 1950s and 60s has been referred to by two of its alumni as the third university of Cambridge, after MIT and Harvard. In 1966, the Franklin Institute awarded the firm the Frank P. Brown Medal. BBN became a wholly owned subsidiary of Raytheon in 2009. On February 1, 2013, BBN Technologies was awarded the National Medal of Technology and Innovation.

[xli] A punched card is a flexible write once medium that encodes data, most commonly 80 characters. Groups or decks of cards form programs and collections of data .Users could create cards using a desk- sized keypunch with a typewriter like keyboard. A typing error generally necessitated repunching an entire card.

[xlii] Batch computing refers to the execution of a series of programs on a computer without manual intervention.

[xliii] RONALD L.KRUTZ & RUSSELL DEAN VINES, COMPREHENSIVE GUIDE TO SECURE CLOUD COMPUTING 1 (2010).

[xliv]Ahmed Mohamed Gamaleldin, *An Introduction to Cloud Computing Concepts*, available at http://www.secc.org.eg/recocape/SECC_Tutorials_An%20Introduction%20to%20Cloud%20Computing%20Concepts.pdf (last updated 17 May ,2013).

[xlv] Jared A. Harshberger, *Cloud Computing Providers and Data Security Law,* 16 J.TECH.L & POLY 229 (2011).

[xlvi] Daniel Buller and Mark Whinow, *Cloud Computing: Emerging Legal Issues, Data Flows and the Mobile Use,* 2 LANDSLIDE 54(2010).

[xlvii]*Ibid.*

[xlviii] Services include storage, processing, bandwidth, and active user accounts.

[xlix] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being software deployed across the physical layer, which manifests the essential cloud characteristics.

[l] Vineeth Narayanan, *Harnessing the Cloud: International Law Implications of Cloud Computing* 12 CHI. J INT'L 783 (2012).

[li] *Ibid.*

[lii]George Grispos, Tim Storer & William Bradley Glisson, *Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics,* 4 INTERNATIONAL JOURNAL OF DIGITAL CRIME AND FORENSICS 28-48 (2012).

[liii]Brian carrier, *Defining Digital Forensic examination and Analysis Tools using Abstraction layers*, 1 INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE 2 (2003).

[liv] Prasad Purnayae, *Cloud Forensics: Volatile Data Preservation*, 4 IJCSE 42 (2015).

[lv] Terrell Bynum, *Computer Ethics: Basic Concepts and Historical Overview,* STANFORD ENCYCLOPEDIA OF PHILOSOPHY 2 (2001).

[lvi] Hereinafter refereed as LEA's.

[lvii] Michael G.Noblett, Mark M. Politt and Lawrence A. Presley, *Recovering and Examining Computer Forensic Evidence,* 2 FORENSIC SCIENCE COMMUNICATIONS 5 (2000).

[lviii] RICHARD SAFERSTEIN, FORENSIC SCIENCE HANDBOOK 37 (2001).

[lix]Ewa Huebner, Derek Bem & Oscar Bem, *Computer Forensics- Past, Present and Future,* 8 INFORMATION SECURITY TECHNICAL REPORT 32 (2007).

[lx] *Ibid.*

[lxi] Virginiah Sekgwathe & Mohammad Talib, *Cyber Forensics: Computer Security and Incident Response,* 2 IJNCAA 127-137 (2012).

[lxii]*Ibid.*

[lxiii] NINA GODBOLE & SUNITA BELAPURE, CYBER SECURITY: UNDERSTANDING CYBER CRIMES, COMPUTER FORENSICS AND LEGAL PERSPECTIVES 342 (2011).

[lxiv] There includes two kinds of sources: Obvious sources which includes computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. On the hand Non- obvious sources include setting of digital thermometers, black boxes inside automobiles, RFID tags and webpages.

[lxv] NINA GODBOLE & SUNITA BELAPURE, *supra* note 68, at 341.

[lxvi] For instance, in a hot car, digital media tends to lose bits.

[lxvii] The process of creating an exact duplicate of the original evidentiary media is often called Imaging. Computer Forensics software packages make this possible by converting an entire hard drive into a single searchable file- this file is called an image. Using a stand- alone hard drive duplicator or software imaging tools such as DCFLdd, IXimager or Guymager, the entire hard drive is completely duplicated. This is usually done at the sector level, making a bit stream copy of every part of the user- accessible areas of the hard drive which can be physically store data, rather than duplicating the file system. Thereby the original drive is then removes to secure storage to prevent tampering.

[lxviii] NINA GODBOLE & SUNITA BELAPURE, *supra* note 68, at 346.

[lxix] *Id* at.353.

[lxx] Collectively referred to as cloud users.

[lxxi] Ian Walden, *Law Enforcement Access to Data in Clouds* in CLOUD COMPUTING LAW 285 (Christopher Millard ed., 2013).

[lxxii] RAUN, KEYN, JOE KARBY, TAHAR KECHADI & MARK CROSBIE, *supra* note 77, at 17.

[lxxiii] Chimere Barron, Huiming Yu & Justin Zhan, *Cloud computing Security Case Studies and Research,*2 PROCEEDINGS OF THE WORLD CONGRESS ON ENGINEERING 3- 5 (2013).

[lxxiv] D. Fisher, *Attackers using Amazon cloud to host malware,* http://threatpost.com/en_us/blogs /attackers-using-amazon-cloud-hostmalware-060611. (last updated June 6, 2011).

[lxxv] Chimere Barron, Huiming Yu & Justin Zhan, *supra* note 82, at 2.

[lxxvi] Kotenko, M. Stepashkin & E. Doynikova, *Security analysis of information systems taking into account social engineering attacks.* IEEE 19TH INTERNATIONAL EURIMICRO CONFERENCE ON PARALLEL, DISTRIBUTES AND NETWORK- BASED PROCESSING (2011).

[lxxvii]J. Pepitone, *Hack attack expose major gap in Amazon and Apple security,* http://money.cnn .com/2012 /08/07 /technology/mathonan-hacked/index.htm., (last updated August 7, 2012).

[lxxviii] D. Kerr, *Dropbox confirms it was hackers, offers users help,* http://nws.csnet.com/8301-1009_3-57483998-83/dropbox-confirms-it-was hacked-offers-users-help/, (last updated July 17, 2012).

[lxxix] Chimere Barron, Huiming Yu & Justin Zhan, *supra* note 82, at 4.