Challenges of Cloud Forensics

Hamid Jahankhani[1] and Amin Hosseinian-Far[2](✉)

[1] Department of Digital Technology and Computing,
GSM London, London, UK
Hamid.Jahankhani@gsmlondon.ac.uk

[2] School of Computing, Creative Technologies and Engineering,
Leeds Beckett University, Leeds, UK
A.Hosseinian-Far@leedsbeckett.ac.uk

Abstract. Legal requirement for cloud forensics is currently uncertain and presents a challenge for the legal system. These challenges arises from the fact that cloud environment consists of distributed shared storages so there is a level of necessary interactions forensic examiners and law enforcement officers require from the cloud provider in order to conduct their investigations. Cloud computing has generated significant interest in both academia and industry, but it is still an evolving paradigm. Cloud computing services are also, a popular target for malicious activities; resulting to the exponential increase of cyber-attacks. Digital evidence is the evidence that is collected from the suspect's workstations or electronic medium that could be used in order to assist computer forensics investigations. Cloud forensics involves digital evidence collection in the cloud environment. The current established forensic procedures and process models require major changes in order to be acceptable in cloud environment. This chapter aims to assess challenges that forensic examiners face in tracking down and using digital information stored in the cloud and discuss the importance of education and training to handle, manage and investigate computer evidence.

Keywords: Cloud computing · Cloud forensics · Digital evidence · Cyber security strategy · Computer misuse act · Anti-forensics · Challenges of cloud forensics

1 Introduction

In a fully connected truly globalised world of networks, most notably the internet, mobile technologies, distributed databases, electronic commerce and E-governance E-crime manifests itself as Money Laundering; Intellectual Property Theft; Identity Fraud/Theft; Unauthorised access to confidential information; Destruction of information; Exposure to Obscene Material; Spoofing and Phishing; Viruses and Worms and Cyber-Stalking, Economic Espionage to name a few.

According to the House of Commons, Home Affairs Committee, Fifth Report of Session 2013–14, on E-crime, "Norton has calculated its global cost to be $388bn dollars a year in terms of financial losses and time lost. This is significantly more than the combined annual value of $288bn of the global black market trade in heroin, cocaine and marijuana." (Home Affairs Committee 2013).

V. Chang et al. (Eds.): Enterprise Security, LNCS 10131, pp. 1–18, 2017.
DOI: 10.1007/978-3-319-54380-2_1

Since the launch of the UK's first Cyber Security Strategy in June 2009 and the National Cyber Security Programme (NCSP) in November 2011, UK governments have had a centralised approach to cybercrime and wider cyber threats.

Until recently E-crimes had to be dealt with under legal provisions meant for old crimes such as conspiracy to commit fraud, theft, harassment and identity theft. Matters changed slightly in 1990 when the Computer Misuse Act was passed but even then it was far from sufficient and mainly covered crimes involving hacking.

Over the years, the exponential growth of computing era has brought to light many technological breakthroughs. The next radical wave of this growth appeared to be outside the traditional desktop's realm. An evolving terminology that can describe this paradigm is cloud computing. Smith (2011) and Martini and Choo (2012) argued that cloud computing has recently become a prevalent technology and currently is one of the main trends in the ICT sector. In cloud computing several tangible and intangible objects (such as home appliances) surrounding people can be integrated in a network or in a set of networks (Cook 2007).

Migration to cloud computing usually involves replacing much of the traditional IT hardware found in an organisation's data centre (such as servers and network switches) with remote and virtualised services configured for the particular requirements of the organisation. Hence, data comprising the organisation's application can be physically hosted across multiple locations, possibly with a broad geographic distribution (Grispos et al. 2012).

As a result, the use of cloud computing can bring possible advantages to organisations including increased efficiency and flexibility. For instance, virtualised and remote services can provide greater flexibility over a physical IT infrastructure as they can be rapidly Re-configured to meet new requirements without acquiring a new or potentially redundant hardware (Sammons 2015). Further, Khajeh-Hosseini et al. (2010) found that cloud computing can be a significantly cheaper alternative to purchasing and maintaining system infrastructure In-house.

Though, the other side of the coin supports that cloud computing services are a popular target for malicious activities; resulting to the exponential increase of cybercrimes, Cyber-Attacks (Bluementhal 2010). Consequently, this phenomenon demonstrates the need to explore the various challenges and problems of cloud computing in the forensics community to potentially prevent future digital fraud, espionage, Intellectual Property (IP) theft as well as other types of concern.

2 Cloud Computing; Concept, Technology & Architecture

In 1980's the main centralized processing power for various computation tasks was through mainframes (Jadeja and Modi 2012), however this centralized public utility architecture is gaining momentum in today's industries and numerous applications therein. According to (Givehchi and Jasperneite 2013) "*the main goal of cloud computing is to provide on-demand computing services with high scalability and availability in a distributed environment with minimum complexity for the service consumers*". According to Chang et al. (2016a) many businesses are now considering cloud computing as an option to reduce their costs and to enhance the efficiency in their business processes. Cloud computing offers a variety of advantages as opposed to non-distributed architectures. Users can access the application only using a browser, regardless of the geographical area they reside in, and the type of system they are using. Knowing the centralised nature of the cloud, it is an ultimate solution in disastor recovery and and for crucial nature of business continuity (Jadeja and Modi 2012).

There are three known cloud categories; Romgovind et al. (2010) depicted these categories in a so called 'Cloud Computing Map':

They also outlined three main cloud delivery models i.e. 'Software as a Service', 'Platform as a Service', and 'Infrastructure as a Service', in the same figure (Fig. 1). In the SaaS delivery model, the focus is on how the user is accessing the software on a cloud. The software is accessible by the user through his/her browser and the user would not need to be concerns about the software deployment, installation and the system's resources, etc. (Kumar 2014). Instances include but not limited to Mobile Application, Thin Clients, etc. PaaS delivery model is where the cloud provider offers the required platform for the user in which software can be created and deployed. This is not a single technology/platform and entails a range of different resources and services (Devi and Ganesan 2015). Instances include but not limited to Database, Web Server and Tools required for Development, etc. Considering the cloud architecture as stack, Infrastructure as Service (IaaS) would be the base layer offering the full required computing infrastructure for the above mentioned delivery models. The infrastructure will be available and distributed through the Internet and Web; an instance include Amazon Web Services (Alhadidi et al. 2016).

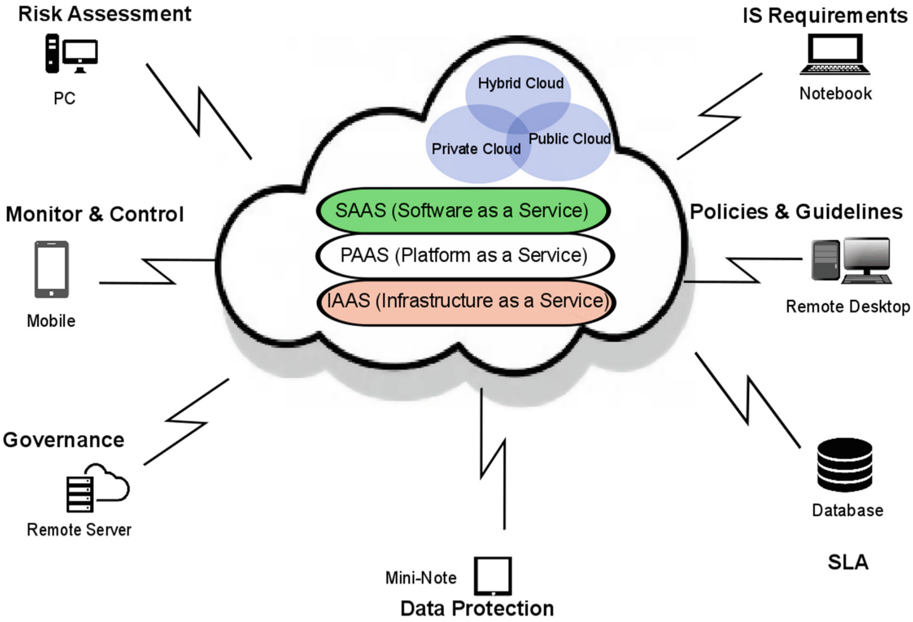

Fig. 1. Cloud computing map; adapted from (Romgovind et al. 2010)

With regards to generic cloud categorisation, there are numerous definitions and characteristics for the above-mentioned three categories. Batra and Gupta (2016) define the categories as:

Private Cloud: In private cloud computing, cloud services are offered to pre-defined and selected users. Overall security and users' authentication and access levels are imperative in this category.

Public Cloud: In this type of cloud computing, the cloud services are provided; Usually through a third party, and via the Internet.

Hybrid Cloud: This category is a mixed representation of the above two types of cloud computing. Many businesses are benefitting from both private and public cloud services.

Table 1. Advantages and disadvantages of different cloud types; by Hu et al. (2011)

	Public cloud	Private cloud	Hybrid cloud
Advantages	Simplest to implement and use	Allows for complete control of server software updates patches, etc.	Most cost-efficient through utilization flexibility of public and private clouds
	Minimal upfront costs	Minimal long-term costs	Less susceptible to prolonged service outages
	Utilization efficiency gains through server virtualization	Utilization efficiency gains through server virtualization	Utilization efficiency gains through server virtualization
	Widespread accessibility	–	Suited for handling large spikes in workload
	Requires no space dedicated for data center	–	–
	Suited for handling large spikes in workload	–	–
Disadvantages	Most expensive long-term	Large upfront costs	Difficult to implement due to complex management schemes and assorted cloud center
	Susceptible to prolonged services outages	Susceptible to prolonged services outages	Requires moderate amount of space dedicated for data center
	–	Limited accessibility	–
	–	Requires largest amount of space dedicated for data center	–
	–	Not suited for handling large spikes in workload	–

According to Batra and Gupta (2016), organisations offer the private cloud services in cases where the service has a high importance and the security of the operation is vital, whilst the public cloud services are offered for the lengthy tasks and will be offered when required.

Hu et al. (2011) summarizes the advantages and disadvantages of Private, Public and Hybrid cloud (Table 1):

3 Cloud Storage Models

The goal of cloud storage system is an effective organizational system node to store data. Following are the common four types of services:

3.1 Elastic Compute Clusters

A compute cluster includes a set of virtual instances that run a customer's application code. Each virtual instance can be a bare-metal VM (in an infrastructure-as-a-service provider, such as AWS and Cloud Servers) or a sandbox environment (in a platform-as-a-service provider, such as AppEngine). Clusters are elastic in that the number of instances can scale dynamically with the application's workload. For instance, in a cloud-based Web application, the number of front-end server instances can scale according to the incoming request rate, so that each server instance won't be overwhelmed by too many simultaneous requests.

3.2 Persistent Storage Services

These services store application data in a non-ephemeral state; all instances in the cluster can access them. They're different from the local storage (for example, the local hard drive) in each virtual instance, which is temporary and can't be directly accessed by other instances. They're also different from block storage services that some providers offer (for example, Amazon's Elastic Block Storage). The latter can't be accessed by multiple instances simultaneously and serves primarily as backup. There are several common types of storage services. Table storage (SimpleDB, Google's DataStore, and Azure's Table Storage) is similar to a traditional database. Blob storage (S3, Rackspace's Cloud Files, and Azure's Blob Storage) keeps binary objects such as user photos and videos. Queue storage (SQS and Azure's Queue Storage) is a special type of storage service.

Persistent storage services are usually implemented as RESTful Web services (REST stands for Representational State Transfer) and are highly available and scalable compared to their non-cloud siblings.

3.3 Intracloud Networks

These networks connect virtual instances with each other and with storage services. All clouds promise high-bandwidth and low-latency networks in a data centre. This is because network performance is critical to the performance of distributed applications such as multitier Web services and MapReduce jobs.

3.4 Wide-Area Networks

Unlike intra cloud networks, which connect an application's components, wide-area networks (WANs) connect the cloud data centres, where the application is hosted, with end hosts on the Internet. For consumer applications such as websites, WAN performance can affect a client's response time significantly. All cloud providers operate multiple data centres at different geographical regions so that a nearby data centre to reduce WAN latency can serve a user's request.

3.5 Putting It All Together

These four types of services are fundamental in building a generic online computation platform. Imagine a typical online cloud application, such as a social network website. Its servers can run in the compute cluster, leveraging the scaling feature to absorb flash-crowd events. Its user data can be stored in the various storage services and accessed through the intracloud network. Its Web content can be delivered to users with just a short delay, with a WAN's help. Other important cloud services, such as MapReduce (Hadoop) services and backup services, aren't as common, probably because they aren't essential to most cloud applications.

Considering the complexities of digital oil fields in the cloud, oil and gas industry still is geared to migrate to the cloud because of the various advantages in exploration and production information deliver, collaboration and decision-support. However, for an effective migration to cloud environment, it is paramount that a set of clear metrics based on business analytics objectives are defined. Of course, the choice of appropriate deployment model is based on the security, compliance, cost, integration and quality of service.

4 Cloud Storage Challenges

Cloud services are applications running in the Cloud Computing infrastructures through internal network or Internet. Cloud computing environments are multi domain environments in which each domain can use any security, privacy, and trust needs and potentially employ various mechanisms, interfaces, and semantics (Zhou et al. 2010). Such domains could signify individual enabled services or other infrastructural or application components. Service-oriented architectures are naturally relevant technology to facilitate such multi domain formation through service composition and orchestration.

4.1 Authentication and Identity Management

By using cloud services, users can easily access their personal information and make it available to various services across the Internet. An identity management (IDM) mechanism can help authenticate users and services based on credentials and characteristics. The key to the issue concerning IDM in clouds is interoperability drawbacks that could result from using different identity tokens and identity negotiation protocols. Existing password-based authentication has an inherited limitation and poses significant risks. An IDM system should be able to protect private and sensitive information related to users and processes. How multi-tenant cloud environments can affect the privacy of identity information isn't yet well understood. In addition, the multi-jurisdiction issue can complicate protection measures. While users interact with a front-end service, this service might need to ensure that their identity is protected from other services with which it interacts. In multi-tenant cloud environments, providers must segregate customer identity and authentication information. Authentication and IDM components should also be easily integrated with other security components.

4.2 Access Control and Accounting

Heterogeneity and diversity of services, as well as the domains' diverse access requirements in cloud computing environments, demand fine-grained access control policies particularly, access control services should be flexible enough to capture dynamic, context, or attribute- or credential-based access requirements and to enforce the principle of least privilege. Such access control services might need to integrate privacy-protection requirements expressed through complex rules.

It's important that the access control system employed in clouds is easily managed and its privilege distribution is administered efficiently. We must also ensure that cloud delivery models provide generic access control interfaces for proper interoperability, which demands a policy-neutral access control specification and enforcement framework that can be used to address cross-domain access issues. The access control models should also be able to capture relevant aspects of SLAs. The utility model of clouds demands proper accounting of user and service activities that generates privacy issues because customers might not want to let a provider maintain such detailed accounting records other than for billing purposes. The out-sourcing and multi-tenancy aspects of clouds could accelerate customers' fears about accounting logs.

4.3 Trust Management and Policy Integration

Even though the multiple service providers coexist in the cloud and collaborate to provide various services, they might have different security approaches and privacy mechanisms, so it is important that we must address them heterogeneity among their policies. Cloud service providers might need to compose multiple services to enable bigger application services. So mechanisms are placed to ensure that such a dynamic collaboration is handled securely and that security breaches are effectively monitored during the interoperation process. Now, even though individual domain policies are verified, security violations can easily occur during integration and providers should carefully manage access control policies to ensure that policy integration doesn't lead to any security breaches.

In cloud computing environments, the interactions between different service domains, which are driven by service requirements, can also be dynamic, transient, and intensive and a trust framework should be developed to allow for capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements. The cloud's policy integration tasks should be able to address challenges such as semantic heterogeneity, secure interoperability, and policy-evolution management. Furthermore, customers' behaviors can evolve rapidly, thereby affecting established trust values. This suggests a need for an integrated, trust-based, secure interoperation framework that helps establish, negotiate, and maintain trust to adaptively support policy integration.

4.4 Privacy and Data Protection

Privacy is a core issue here, including the need to protect identity information, policy components during integration, and transaction histories. This helps to store their data and applications on systems that reside outside of their on-premise data centers. This might be the single greatest fear of cloud clients. By migrating workloads to a shared infrastructure, customers' private information faces increased risk of potential unauthorized access and exposure (Tianfield 2012). Cloud service providers must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy-protection mechanisms must be embedded in all security solutions. In a related issue, it's becoming important to know who created a piece of data, who modified it and how, and so on. Provenance information could be used for various purposes such as trace back, auditing, and history-based access control. Balancing between data provenance and privacy is a significant challenge in clouds where physical perimeters are abandoned (Carroll et al. 2014).

Chang et al. (2016a) strongly believe that privacy is one of the most important factors in cloud security. They also argue that many organisations are willing to invest in making the cloud private and ultimately secure. In a recent research work conducted by Chang et al. (2016b), privacy was considered as the most imperative factor with regards to the overall security of the system. That was followed by identity management, trust, etc.

4.5 Risk Management

Cloud computing provides several benefits to an organization including, cost, investment on physical or software infrastructure, users can access their data anywhere and finally, easier and faster data sharing.

The cloud computing concept arises from the notion of "software as a service" (SaaS). A set of services is provided on a set of platforms at various locations. The five key characteristics and benefits of cloud computing can pose downside risks that require identification, evaluation, assessment and mitigation. For example, unavailability of on-demand self-service, sensitivities to location-independent resource pooling such as security concerns, unresponsive elasticity/scalability are illustrative downside risks that a fully cloud dependent/migrated enterprise may need to be aware of and provide requisite solutions for.

The code of practice for the implementation of the ISO31000 standard on risk management highlights a number of principles that any risk management system shall ideally follow and embed (Jahankhani et al. 2015). The key principles relevant to cyber risk management are:

- Risk management should be systematic and structured, the approach to risk management should, where practicable, be consistently applied within the organisation
- Risk management should take into account organizational culture, human factors and behaviour
- Risk management should create and protect value, the organization should optimize risk management to contribute to the demonstrable achievement of objectives and maximize overall business and commercial benefits
- Risk management should be transparent and inclusive, Management and stakeholders should be actively involved in risk identification, assessment and response
- Risk management should be dynamic, iterative and responsive to change; the organization should ensure its risk management continually identifies and responds to changes affecting its operating environment.

A comprehensive risk register, identifying, characterizing, assessing and mitigating all risks need to be devised to ensure business continuity should any of the promised key benefits be interrupted due to local or global disruptions or threats. The Institute of Risk Management (IRM) has also issues guidelines on the risk management process framework of related to ISO31000 (Theirm.org 2010).

Chang (2014) discusses the concept of Business Intelligence as a Service (BIaaS) in which financial risk assessment is considered as one of the intelligent services that can be offered on cloud. Fan and Chen (2012) argue that many risks and cost exposures that arise as a result of cloud implementation are due to social factors, and have proposed a risk management strategy. It can be argued that education and training would minimise such social risks (Jahankhani and Hosseinian-Far 2014). This risk management strategy can be useful for executive decision making. Theoretically, Bedford et al. (2014) propose a probabilistic risk analysis using minimum information methods which can also be applied to the cloud risk assessment.

4.6 Disaster Recovery in Cloud Systems

Considering all the above mentioned challenges, there is always a risk of using key and vital business data at the time of disastrous incidents. Although many scholars focus on different security challenges in cloud computing, few outline the contingency planning and recovery procedures in the event of system failure as a result of an incident (Chang 2015). The disaster recovery plans and systems are usually context dependent and vary application by application. There are also automatics systems that can be accessible when it comes to disaster recovery. Clarkson (2016) has a patent on an automatics disaster recovery system in which restoration devices are used to get the copied data for post-disaster recovery. The significance and vitality of disaster recovery techniques become apparent when, the incident is viewed from the business perspective. Considering ‘business continuity’ or survival as one of the key business objectives, we would agree that despite the higher costs of contingency planning, disaster recovery techniques worth the investment. Disaster recovery and contingency planning depends on the context and the utilised system, however some scholars have generalised the procedure using a macro perspective. There are numerous examples of disaster recovery in cloud systems. Haji (2016) has defined the set of requirements, challenges and some procedures for contingency planning in the Airline business context. The concept of business continuity and sustainability is also perceived from a different perspective. The virtualisation in cloud has already helps the business to maintain a solid disaster recovery plan through using cloud services (Pulsant Business Limited 2015). There are numerous platforms for disaster recovery of cloud services. Khoshkholghi et al. (2014) have conducted a thorough survey on disaster recovery techniques and properties for cloud services; in which strengths and weaknesses of each system are methodically assessed.

5 Challenges Raised by Cloud Computing with Respect to Existing Digital Forensics Models

It has been observed that use of cloud computing currently presents several challenges to its users (i.e. individuals, organisations, regulatory and law enforcement authorities).

In 2006 two new laws were passed to tackle E-crime namely the Fraud Act 2006 which came into force in 2007 which “the new law aims to close a number of loopholes in proceeding Anti-fraud legislation, because, the Government said was unsuited to modern fraud”, and the Police and Justice Act 2006 (part 5) which prohibits “unauthorised access to computer material; unauthorised acts with intent to impair operation of computer and the supply of tools that can be used for hacking” (The National Archives 2006).

Documented guidance, practices and procedures were outdated and wholly inadequate to help tackle electronic evidence in a forensic manner, until first E-crime publication by ACPO in July 2007 and subsequently revised in November 2009 and 2012. This is recognised as the best guidelines ever produced to assist law enforcement in handling digital evidence (ACPO 2012). On one hand these guidelines seem sustainable and functional; however on the other hand it is still yet practically unclear how digital evidence used in courts produced by a digital forensic investigation could be gathered by such guidelines in a cloud environment.

Digital evidence is the evidence that is collected from the suspect’s workstations or electronic medium that could be used in order to assist computer forensics investigations.

There are basically two types of evidences that could support a digital forensic investigation, which are, physical evidence and digital evidence. Physical evidences are categorised as touchable and substantial items that could be brought to court and shown physically. Examples of physical evidence that could assist in the investigations are computers, external hard disk drives and data storage (memory sticks and memory cards) handheld devices including mobile phones/smart phones, networking devices, optical media, dongles and music players. Digital evidence would be the data that is extracted from the physical evidence, or the computer system.

In order to perceive a bit of information or data as evidence, it needs to satisfy the 5 rules that are:

(1) The evidence should be admissible and excepted in the court of law
(2) The evidence needs to be authentic and not contaminated
(3) The evidence needs to the whole piece, not just indicative parts
(4) The evidence has to be reliable, dependable
(5) The evidence needs to be believable

Digital evidence, as compared to hard evidence, are difficult to find, in terms of defining the nature of the data, and classifying it as a digital evidence that is worthy to be presented in court.

Proving evidence which is reliable has been proven to be a difficult task, not just because the nature of evidence, but also the wide scope and environment in which the evidence are extracted from.

In a corporate environment, the forensic investigator team will need to identify, contain and maintain the integrity of the evidence, and differentiate whether the piece of evidence is relevant or not to the current crime being investigated, and whether it would stand a chance in finding the culprit and charging them through legal proceedings.

Among the considerations that need to be evaluated by the investigators when dealing with collecting digital evidence are the expenses, cost and loss incurred and the availability of the service during and after the incident.

However, the question here is, can we investigate a crime in the cloud using the existing computer forensics models, frameworks and tools?

According to Grispos et al. (2012), the available digital forensic practices, frameworks and tools are mainly intended for Off-line investigation, therefore if an investigation is conducted in a cloud computing environment new challenges come to light since the potential evidence that arises is likely to be ephemeral and stored on media beyond the investigator's immediate control.

In addition, digital forensics investigation processes heavily rely on theoretical frameworks and enhanced Digital Investigation Process Models which are practically not very useful for the current available cloud technologies as they were developed prior to their advent; and mainly assume that the investigator has physical access and control over the storage media of the targeted network, system or device (Grispos et al. 2012).

As a result, it is apparent that the current cloud technologies face numerous significant challenges as the majority of available forensic process models do not respond adequately to the requirements of a digital forensic investigation and therefore they do not meet the needs of a complex cloud environment. All of the assumptions of the suggested forensic process models are likely to be invalidated when investigating forensic activities in a cloud environment as the majority of them strictly follow tactics of a physical investigation.

Roussev et al. (2009) argues that, although the digital forensics models comprehensively reviews the stages of a digital forensic process and analyses the cloud forensics' impact on this process; most of its assumptions are not yet valid in the context of cloud computing and the problem will only get worse with the explosive growth of data volumes. As a result they proposed the Distributed Digital Forensic (DDF). This of course is not new and several researchers have already proposed models for DDF services for cloud computing paradigm. However, Roussev et al. (2009) proposal is based on the MPI MapReduce (MMR) framework.

Grispos et al. (2012) have summarises the challenges of cloud forensics in Table 2.

Dykstra and Sherman (2013) introduced FROST which is three new tools for the OpenStack cloud platform. These tools are integrated into the management plane of cloud architecture; hence, forensic investigators can obtain trustworthy forensics data independent of the cloud providers. OpenStack (2016) is an Open-Source cloud computing platform and users includes many large organizations such as Intel, Argonne National Laboratory, AT&T, Rackspace and Deutsche Telekom.

Table 2. Summary of challenges to digital forensics in cloud environments (Grispos et al. 2012).

Phase	Action	Challenges
Identification	Identifying an illicit event	Lack of frameworks
Preservation	Software tools	Lack of specialist tools
	Sufficient storage capacity	Distributed, virtualized and volatile storage; use of cloud services to store evidence
	Chain of custody	Cross-jurisdictional standards, procedures; proprietary technology
	Media imaging	Imaging all physical media in a cloud is impractical; partial imaging may face legal challenges
	Time synchronization	Evidence from multiple time zones
	Legal authority	Data stored in multiple jurisdictions; limited access to physical media
	Approved methods, software and hardware	Lack of evaluation, certification generally, but particularly in cloud context
	Live vs. Dead acquisitions	Acquisition of physical media from providers is cumbersome, onerous and time consuming data is inherently volatile
	Data integrity	Lack of write-blocking or enforced persistence mechanisms for cloud services and data
Examination	Software tools	Lack of tested and certified tools
	Recovery of deleted data	Privacy regulations and mechanisms implemented by providers
	Traceability and event reconstruction	Events may occur on many different platforms
Presentation	Documentation of evidence	Integration of multiple evidence sources in record
	Testimony	Complexity of explaining cloud technology to jury

Legal requirement for cloud forensics is currently uncertain and presents a challenge for the legal system. These challenges arises from the fact that cloud environment consists of distributed shared storages so there is a level of necessary interactions forensic examiners and law enforcement officers require from the cloud provider in order to conduct their investigations. This means they are at the mercy of their public cloud providers to assist in an investigation. In cloud investigation this lack of physical access due to the decentralized nature of the data processing causes enormous technical and legal disruptive challenges Orton et al. (2013). There are two legal issues:

(1) Validity-Of-the-Warrant – Establishing a specific location for search warrant that evidence is believed will be found together with the specifics required in the warrant.

(2) Authenticity – Making sure that the data is of the suspect (defendant) alone when searching shared storages.

The National Institute of Standards and Technology released a draft report in 2014 (NIST 2014), highlighting the requirement for cloud forensics standards to aid law enforcement. In that report NIST identified 65 challenges in 9 major groups that forensics investigators face in gathering and analysing digital information stored in the cloud. The nine major groups are architecture, data collection, analysis, Anti-forensics, incident first responders, role management, legal, standards, and training. Figure 2 is the NIST mind map of forensic challenges.

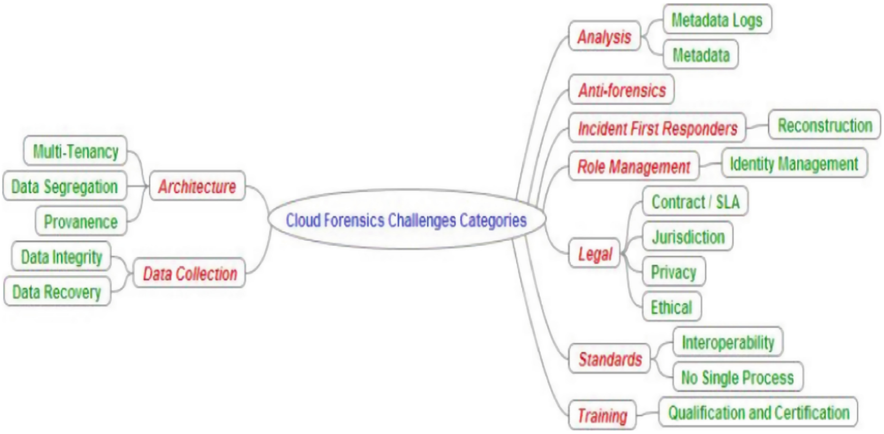

Fig. 2. NIST mind map of forensic challenges (NIST 2014).

Considering all the above-mentioned challenges with regards to cloud forensics, the complexity of the cloud architecture on its own would also make the overarching security processes very challenging. This complexity is outlined in a conceptual model in Fig. 3.

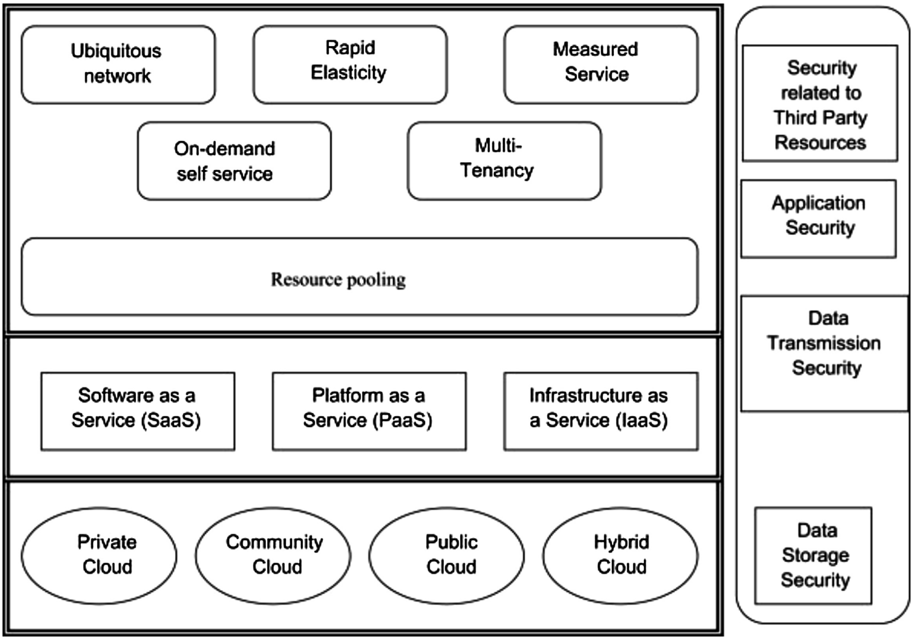

Fig. 3. Cloud computing complexity and challenges for cloud security (Subashini and Kavitha 2011)

6 Anti-forensics

Anti-forensics as a concept is as old as the traditional computer forensics. Someone that commit a punishable action use any possible way to get rid of any evidence connected with the prohibited action. The traditional forensics can have a range of Anti-forensics that start from a trivial level (e.g. wiping fingerprints from a gun) and to a level where our fantasy can meet the implementation of an Anti-forensic idea (e.g. alteration of DNA left behind in a crime). In digital Anti-forensics the same rules exists, with the difference that they are fairly new with little research and development (Jahankhani et al. 2007).

There are number of techniques that are used to apply Anti-forensics. These techniques such as obfuscation, data hiding, and malware are not necessarily designed with Anti-forensics dimension in mind.

While in theory the forensics investigator should monitor everything available around the suspect, in reality the post incident response could end up quite dramatically. This could be due to; ignorance regarding the network activity logs, legal barriers between the access point and the forensics acquisition, non–cooperative ISP's, etc.

Anti-forensics is a reality that comes with every serious crime and involves tactics for "safe hacking" and keeps the crime sophistication in a high level. Computer forensic investigators along with the forensic software developers should start paying more attention to Anti-forensics tools and approaches.

If we consider the Computer Forensics as the actions of collection, preservation, identification and presentation of evidence, Anti-forensics can affect the first three stages. Because these stages can be characterized as “finish to start” between them from a project management point of view, the failure of one of them could end up as a failure of the lot. Thus, there is a high impact of Anti-forensics to the forensics investigations.

Officially there is no such thing as Anti-forensic investigations because the Anti-forensic countermeasures are still part of the investigator’s skills.

7 The Main Difficulties Faced by Law Enforcement Officers Fighting Cyber-Crime

It is evident that cybercrime is no longer in its infancy. It is ‘big business’ for the criminal entrepreneur with potentially lots of money to be made with minimal risks. Cloud computing has generated significant interest in both academia and industry, but it is still an evolving paradigm. Confusion exists in IT communities about how a cloud differs from existing models and how its characteristics affect its adoption. Some see cloud as a novel technical revolution; some consider it a natural evolution of technology, economy, and culture (Takabi et al. 2010). Nevertheless, cloud computing is an important concept, with the strong ability to considerably reduce costs through optimization and increased operating and economic efficiencies. Furthermore, cloud computing could significantly enhance collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several surveys of potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption. At the same time cloud creates unique challenges for digital forensic investigators, and one of the areas which have been recognised as the contributory elements in the failing by law enforcement officers is lack of proper training.

From law enforcement point of view the task of fighting Cyber-Crime is a difficult one. Although crime is irrespective of how big or small, a decision has to be made on the merits of each case as to whether investigating and prosecuting is in the public’s interest and therefore, it is becoming necessary to understand and manage the Computer Forensics process in the cloud.

Computer Forensics is no longer a profession where training on the job to get experience is sufficient, especially when dealing in cloud environment. Most other professions require one to have a degree before one can progress to train in their vocation i.e. teachers, lawyers, forensic scientist and doctors etc., the same should be with Computer Forensic as the work done is as important as those in other fields and be it positive or negative does affect people’s lives.

Numerous universities in in UK and abroad are offering Computer Forensic and Information Security courses to graduate and Post-Graduate level which will help those taking on the courses to have a good grounding in computer science, a better understanding of computer forensic theories and most of all help them develop to be more innovative in coming up with new forensically sound ways of fighting E-crime and to “think outside the box”.

It is time for the government to actively work in partnership with universities to encourage people to take on these courses especially those already working in the field in the public sector.

A degree is now a prerequisite in the private sector as well as experience, as it is becoming a lot more difficult for one to claim to be an expert in the field of computer forensics and an expert witness in a court of law. Gone are the days where Do-It-Yourself forensics will be accepted (Jahankhani and Hosseinian-Far 2014).

This leads us to another area a lot of experts in the field of computer forensics have been reserved about and that is the idea of accreditation. It is an area that is very difficult to make decisions on. Most agree and recognize that a board should be set up, but what cannot be agreed upon is who should lead it. Some have suggested that it should be led by universities, by government, by their peers or jointly by universities, government and businesses.

If it is government lead, without set of standards the situation will be no different from what we have at present. It will also involve those working in the profession to give it some direction and it is still doubtful as to whether those people are in a position to decide what form of accreditation to be embarked upon.

This brings us to the option of, a joint partnership with government, universities and businesses. This is the most feasible option but a lot of joint effort will be required to come up with a credible accreditation that will be accepted by all.

One thing is for sure having a form of accreditations will force government, academics, researches and those working in the field of computer forensics to set more appropriate standards and controls for those who handle, analyse and investigate computer evidence.

8 Conclusions

Cloud computing is still an evolving paradigm and has already created challenges for law enforcement around the globe to effectively carry out cloud forensics investigations. Although the digital forensics models comprehensively reviews the stages of a digital forensic process and analyses the cloud forensics' impact on this process; most of its assumptions are not yet valid in the context of cloud computing and the problem will only get worse with the explosive growth of data volumes.

Legal requirement for cloud forensics is currently uncertain and presents a challenge for the legal system. These challenges arises from the fact that cloud environment consists of distributed shared storages so there is a level of necessary interactions forensic examiners and law enforcement officers require from the cloud provider in order to conduct their investigations. One of the areas, which have been recognised as the contributory element in the failing by law enforcement officers, is lack of proper training. Education and training will help to provide good grounding in computer science, a better understanding of computer forensic theories and most of all help to develop to be more innovative in coming up with new forensically sound ways of fighting E-crime and to "think outside the box".

References

ACPO. ACPO Good Practice Guide for Digital Evidence (2012). http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Alhadidi, B., Arabeyat, Z., Alzyoud, F., Alkhwaldeh, A.: Cloud computing security enhancement by using mobile PIN code. J. Comput. **11**(3), 225–231 (2016)

Batra, M., Gupta, N.: Various security issues and their remedies in cloud computing. Int. J. Adv. Eng. Manag. Sci. (IJAEMS) **2**(2), 18–20 (2016)

Bedford, T., Wilson, K.J., Daneshkhah, A.: Assessing parameter uncertainty on coupled models using minimum information methods. Reliab. Eng. Syst. Saf. **125**, 3–12 (2014)

Bluementhal, M.S.: Hide and seek in the cloud. IEEE Secur. Priv. **8**(2), 57–58 (2010)

Carroll, N., Helfert, M., Lynn, T.: Towards the development of a cloud service capability assessment framework. In: Mahmood, Z. (ed.) Continued Rise of the Cloud: Advances and Trends in Cloud Computing, pp. 289–336. Springer, London (2014)

Chang, V.: The business intelligence as a service in the cloud. Future Gener. Comput. Syst. **37**, 512–534 (2014)

Chang, V.: Towards a big data system disaster recovery in a private cloud. Spec. Issue Big Data Inspired Data Sens. Process. Netw. Technol. **35**, 65–82 (2015)

Chang, V., Kuo, Y., Ramachandran, M.: Cloud computing adoption framework: a security framework for business clouds. Future Gener. Comput. Syst. **57**, 24–41 (2016a)

Chang, V., Ramachandran, M., Yao, Y., Li, C.: A resiliency framework for an enterprise cloud. Int. J. Inf. Manag. **36**(1), 155–166 (2016b)

Clarkson, D.B.: Automatics Cloud-Based Disaster Recovery System. United States Patent Application, Patent No. 20160036623 Kind Code: A1 (2016)

Cook, T.: The Cloud of Unknowing, 1st edn. Harcourt Inc., Orlando (2007)

Devi, T., Ganesan, R.: Platform as a Service (PaaS): model and security issues. Indones. J. Electr. Eng. **15**(1), 151–161 (2015)

Dykstra, J., Sherman, A.T.: Design and implementation of FROST: digital forensic tools for the OpenStack computing platform. Digit. Investig. **10**, 87–95 (2013)

Fan, C.K., Chen, R.-C.: The risk management strategy of applying cloud computing. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **3**(9), 18–27 (2012)

Givehchi, O., Jasperneite, J.: Industrial Automation Services as part of the Cloud: First Experiences. Jahreskolloquium Kommunikation in der Automation, Magdeburg (2013)

Grispos, G., Storer, T., Glisson, W.B.: Calm before the storm: the challenges of cloud computing in digital forensics (2012)

Haji, J.: Airline business continuity and IT disaster recovery sites. J. Bus. Contin. Emerg. Plan. **9** (3), 228–238 (2016)

Home Affairs Committee: E-Crime, Fifth Report of Session 2013–14. House of Commons, London (2013)

Hu, F., et al.: A review on cloud computing: design challenges in architecture and security. J. Comput. Inf. Technol. - CIT **19**, 25–55 (2011)

Jadeja, Y., Modi, K.: Cloud computing - concepts, architecture and challenges. In: IEEE International Conference on Computing, Electronics and Electrical Technologies (2012)

Jahankhani, H., Altawell, N., Hessami, A.G.: Risk and privacy issues of digital oil fields in the cloud. In: Jahankhani, H., Carlile, A., Akhgar, B., Taal, A., Hessami, A., Hosseinian-Far, A. (eds.) Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. ICGS3 2015. Communications in Computer and Information Science, vol. 534, pp. 275–284. Springer, Heidelberg (2015). doi:10.1007/978-3-319-23276-8_25

Jahankhani, H., Anastasios, B., Revett, K.: Digital Anti Forensics: Tools and Approaches. Defence College of Management and Technology, Shrivenham (2007)

Jahankhani, H., Hosseinian-Far, A.: Digital Forensics Education, Training & Awareness. In: Cyber Crime and Cyber Terrorism Investigator's Handbook. Elsevier, pp. 91–100 (2014)

Khajeh-Hosseini, A., Greenwood, D., Sommerville, I.: Cloud migration: A Case Study of Migrating an Enterprise IT System to IaaS. IEEE, Miami (2010)

Khoshkholghi, M.A., et al.: Disaster recovery in cloud computing: a survey. Comput. Inf. Sci. **7**(4), 39–54 (2014)

Kumar, M.K.: Software as a service for efficient cloud computing. IJRET: Int. J. Res. Eng. Technol. **3**(1), 178–184 (2014)

Martini, B., Choo, K.: An integrated conceptual digital forensic framework for cloud computing. Digit. Investig. **9**, 71–80 (2012)

NIST: NIST Cloud Computing Forensic Science Challenges - NISTIR8006. NIST Cloud Computing Forensic Science Working Group - Information Technology Laboratory (2014)

OpenStack. OpenStack Open Source Cloud Computing Software (2016). http://www.openstack.org/

Orton, I., Alva, A., Endicott-Popovsky, B.: Legal process and requirements for cloud forensic investigations. In: CyberCrime and Cloud Forensics: Applications for Investigation Processes. IGI Global (2013)

Pulsant Business Limited: Rethinking Business Continuity with the Cloud. Pulsant, Reading (2015)

Romgovind, S., Eloff, M.M., Smith, E.: The Management of Security in Cloud Computing, pp. 1–7. IEEE, Johannesburg (2010)

Roussev, V., Wang, L., Richard, G., Marziale, L.: A cloud computing platform for large-scale forensic computing. Advances in Digital Forensics, pp. 201–214. Springer, Heidelberg (2009)

Sammons, J.: The Basics of Digital Forensics, 2nd edn. Elsevier, Waltham (2015)

Smith, D.M.: Hype cycle for cloud computing (white paper). Gartner Inc. (2011)

Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)

Takabi, H., Joshi, J.B., Ahn, G.: Security and privacy challenges in cloud computing environments. IEEE Computer and Reliability Societies (2010)

The National Archives. Police and Justice Act 2006 (2006). http://www.legislation.gov.uk/ukpga/2006/48/contents

Theirm.org: A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 (2010). https://www.theirm.org/media/886062/ISO3100_doc.pdf. Accessed 2016

Tianfield, H.: Security Issues in Cloud Computing. IEEE, Seoul (2012)

Zhou, M., et al.: Security and privacy in cloud computing: a survey, pp. 105–112 (2010)