Cloud Forensics Challenges Faced by Forensic Investigators

Wakas Mahmood, Hamid Jahankhani(✉), and Aykut Ozkaya

GSM-London, London, UK
Hamid.jahanhani@gsm.org.uk

Abstract. 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 paper, aims to assess challenges 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." [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

H. Jahankhani et al. (Eds.): ICGS3 2015, CCIS 534, pp. 74–82, 2015.
DOI: 10.1007/978-3-319-23276-8_7

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 [2] and Martini & Choo [3] 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 [4].

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 [5].

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 Reconfigured to meet new requirements without acquiring a new or potentially redundant hardware [6]. Further, Khajeh-Hosseini et al. [7] found that cloud computing can be a significantly cheaper alternative to purchasing and maintaining system infrastructure Inhouse.

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 [8]. 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 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" [9].

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 [10]. 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. [5], 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 [5].

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., [11] 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., [11] proposal is based on the MPI MapReduce (MMR) framework.

Grispos et al. [5], have summarises the challenges of cloud forensics in Table 1 below.

Table 1. Summary of challenges to digital forensics in cloud environments. [5]

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

Dykstra & Shermann [12], 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 [13] 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.

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 cause enormous technical and legal disruptive challenges [14]. 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 [15], 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 1, is the NIST mind map of forensic challenges.

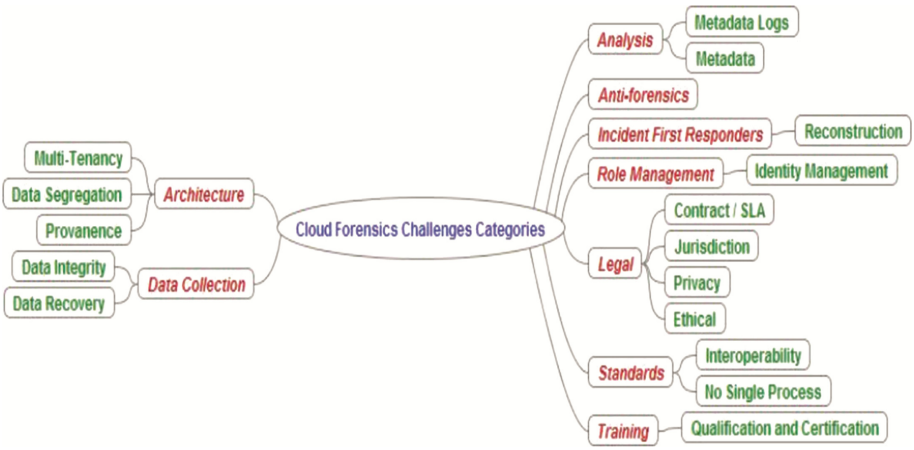

Fig. 1. NIST mind map of forensic challenges. [15]

3 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 [16].

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.

4 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 differ 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 [17]. 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 [18].

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 lead 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.

5 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

1. House of Commons, Home Affairs Committee, E-Crime, Fifth Report of Session 2013–14, http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf
2. Smith, D.M.: Hype cycle for Cloud Computing (White Paper). Gartner Inc., Stamford (2011)
3. Martini, B., Choo, K.: An integrated conceptual digital forensic framework for cloud computing. Digital Invest. **9**, 71–80 (2012)
4. Cook, T.: The Cloud of Unknowing, 1st edn. Harcourt Inc, Orlando (2007)
5. Grispos, G., Storer, T., Glisson, W.B.: Calm before the storm: the challenges of cloud computing in digital forensics, 1–25 (2012)
6. Sammons, J.: The Basics of Digital Forensics, 2nd edn. Elsevier, Waltham (2015)
7. Khajeh-Hosseini, A., Greenwood, D., Sommerville, I.: Cloud migration: a case study of migrating an enterprise IT system to IaaS. Paper presented at the IEEE International Conference on Cloud Computing, CLOUD 2010, Miami, USA (2010)
8. Blumenthal, M.S.: Hide and Seek in the Cloud. IEEE Secur. Priv. **8**(2), 57–58 (2010)
9. Police and Justice Act (2006). http://www.legislation.gov.uk/ukpga/2006/48/contents
10. ACPO Guidelines (2009). http://www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf
12. Roussev, V., Wang, L., Richard, G., Marziale, L.: A cloud computing platform for large-scale forensic computing. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics V. IFIP Advances in Information and Communication Technology, vol. 306, pp. 201–214. Springer, Heidelberg (2009)
12. Dykstra, J., Sherman, A.T.: Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform. Digit. Invest. **10**, S87–S95 (2013). Elsevier
13. OpenStack: OpenStack open source cloud computing software (2012). http://www.openstack.org/

14. Orton, I., Alva, A., Endicott-Popovsky, B.: Legal process and requirements for cloud forensic investigations. In: Ruan, K. (ed.) Cybercrime and Cloud Forensics: Applications for Investigation Processes. IGI Global, Hershey (2012)
15. NIST, Cloud Computing Forensic Science Challenges, Draft NISTIR 8006, NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory (2014). http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf
16. Jahankhani, H., Anastasios, B., Revett, K.: Digital anti forensics: tools and approaches. In: 6th European Conference on Information Warfare and Security Defence College of Management and Technology, Shrivenham, UK, 2–3 July 2007 (2007)
17. Takabi, H., Joshi, J.B.D., Hn, G.J.A.: Security and privacy challenges in cloud computing environments. IEEE Comput. Reliab. Soc. (2010). http://www.cs.ru.nl/~jhh/pub/secsem/takabi2012security-privacy-cloud-challenges.pdf
18. Jahankhani, H., Hosseinian-far, A.: Digital Forensics education, training and awareness. In: Cybercrime and Cyber Terrorism Investigators' Handbook, pp91–100. Elsevier (2014) ISBN 978-1447126829