Technical Challenges of Cloud Forensics and Suggested Solutions

Md. Yasir Arafat[1], Bipasha Mondal[2], Sreeti Rani[3]

[1]*Lecturer, Dept. of Computer Science Engineering, Jessore- 7408, Bangladesh*

[2, 3]*Dept. of Computer Science Engineering, Jessore- 7408, Bangladesh*

(E-mail: [1]arafat.cse.jstu@gmail.com)

Abstract: Today one of the most effective headway in information technology (IT) is cloud computing. It presents many hopeful technological and economic benefits in the recent world. There is no doubt that the new cloud computing concepts allow an amenable worship to numerous users. Many cloud customers remain unwilling to move their own business to the cloud and the main attention of cloud customer is cloud security and the threat of the unknown. Cloud platform add to the challenges of physical location, identification, analysis, preservation of digital evidence. Digital forensic in cloud computing fetches new technical and legal challenges to provide digital computing and solutions. There are a lot of challenges in the field of forensics investigation that is faced by the investigator which may complicate in the extraction of evidences. Forensic scientists analyze digital evidence; provide expert testimony and training in the recognition, collection and preservation of digital evidence. In cloud computing the issues are explained using the phases of digital forensics as the root. In this paper, we mention different phases; each phase includes digital challenges, suggested solutions and comments. In our paper we methodically measure the forensic challenges in cloud environment and discuss new methodologies solutions and developments to perform investigations.

*Keywords:*Cloud computing; Digital Forensic; Digital evidence; Cloud forensics; Investigation challenges.

1. Introduction

Cloud computing is an internet based model of providing available, convenient, on demand access to a shared computer processing resources and data to computers. It is a model for enabling universal on demand access to a shared pool of configurable computing resources such as computer networks, servers, storage, applications and services which can be rapidly provisioned and released with minimal management effort [1].

Distributed computing uses both equipment and programming put away on supplier's server farms to be conveyed as administrations over web fordone through identification, collection, preservation, examination, interpretation and clients. Distributed computing has the ability to get to information over web utilizing diverse sort of space registering gadgets like PCs, tablets, cell phones or workstations. Cloud computing introduce a number of service models to meet all types of customer requirements. The available service models are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service(IaaS) and Storage as a Service (StaaS). In SaaS Cloud forensics have defined as "the application of digital forensic science in cloud environments as a subset of network forensics" [2]. Forensic investigation in cloud computing is done through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

In SaaS model, the cloud enables users to access applications running on a cloud infrastructure via web browsers or client applications. In PaaS model enable users to deploy their application on cloud created by supported programming languages, libraries and tools. In IaaS model, cloud provide users with basic computing resources like processing, storage and network to run and deploy arbitrary software which may consists of operating systems and applications. In StaaS model it is owned and managed by cloud provider and provided as a service that is accessed through web based applications or Application Program Interfaces (APIs) like desktop storage applications [3].

On the other hand, digital forensics has developed as a discipline to support law enforcement in dealing with the use of digital device in illegal acts [4]. Computerized crime scene investigation is viewed as a science since it is an orderly,

mechanical assessment of a PC framework and its substance. Its aim is to find and preserve electronic confirmation for use in criminal investigation. In particular, Note that cloud systems have been hardly designed with digital forensics and evidence integrity in mind, and thus forensics investigators face very challenging technical, legal and logistical issues [5].

1.1. Digital forensics

Digital forensics is a branch of forensic science which is concerned with the use of digital information (produced, stored and transmitted by computers) as source of evidence in investigations and legal proceedings. The first Digital Forensics Research Workshop held in New York in 2001 provided the following working definition of digital forensics [6]: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering their construction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. "Digital Forensics (DF), as defined by McKemmis [7], is the "process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable".

The aim of a forensic investigation is to identify and preserve the evidence, extract the information, document every process, and analyse the extracted information to find answers with respect to the 5Ws (Why, When, Where, What, and Who) [8]. Types of digital forensics: Network forensics, Computer forensics, memory forensics, enterprise forensics, proactive forensics, e-mail forensics, web forensics, system forensics, cyber forensics, data forensics.

1.2. Cloud computing

Cloud computing is fairly marketing term that takes the technology, services, and applications for the delivery of hosted services over the internet and turns them into a self-service utility. NIST defines 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" [9]. Cloud computing uses three main levels of service that differ on the services that are delivered to the end user [10]:

- Software as a Service (SaaS): Providers offer access to their applications that are hosted on their own servers and consumers make use of them [10]. Common examples include file storage, social networking and email.
- Platform as a Service (PaaS): Here cloud providers offer a platform where consumers deploy and run their applications [10]. The underlying hardware, network and tools are provided by the cloud service. Examples include Google App Engine, Microsoft Azure, Engine Yard, Cloud enabled application platform (CEAP) and Windows Azure.
- Infrastructure as a Service (IaaS): Consumers buy raw computing and storage space and they can control and manage the underlying infrastructure like the operating systems, software and network [10]. Examples are Amazon EC2 and Rackspace Cloud Services.

Cloud services can be categorised by their organisational deployment: Private, the infrastructure is provisioned exclusively to a single organisation for private use [10]. Community is used by a specific community of organisations that share common concerns [10]. When the infrastructure is for open use, it is considered public [10]. Hybrid refers to the combination of two or more distinct cloud infrastructure [10].

1.3. Cloud forensics

According to [11], cloud forensics can be defined as the application of computer forensics principles and procedures in a cloud computing environment. Although cloud computing provides many promising economic and technological advantages such as more efficient use of resources, greater availability on a massive scale and reduced costs, there are serious concerns associated with it which must be addressed and overcome. There are lots of digital artefacts in server such as system logs,

application logs, user authentication and access information, database logs etc.

The physical incomprehension and unknown location of data makes it more complex to identify, collect, and analyze of data in cloud forensics environment. Traditional approach to seizing the system is no more practical either, even if the location is known, as it could bring down whole data centre, affecting other customers due to multi-tenancy. A number of researchers have cited this issue and some partially suggested possible solutions [[1], [12],[13]].

2. Related Work

The cloud computing becomes the most powerful environment for the upcoming companies. In cloud computing the forensic investigation support is not completely given by the cloud providers. There are few challenges in attaining the forensic support. The author highlights the cloud characteristics, models, architecture and the challenges in achieving Forensic support. Some of the challenges are data recovery in finding and retaining forensic evidence from law enforcement perspective. New methods are proposed to bring the evidence of the cyber-attack in the cloud environment. Likewise there are challenges in Investigations on virtual machine. Henceforth, the extended Forensic Investigation system is mandatory to meet the Forensic challenges in cloud environment [14].

The potential benefits and challenges of cloud computing for digital forensic investigations have been discussed by several authors. One potential benefit of cloud computing is having data in a centralized location, which can mean incidents can be investigated more quickly [15]. When attempting to locate evidence in a distributed environment such as the cloud, major challenges will need to be overcome because evidence could be located across several locations making evidence collection difficult. The distribution of evidence can be across multiple virtual hosts, physical machines, data centres and geographical and legal jurisdictions.

The distributed nature of control and storage in a cloud will also likely make tracing activity and re-construction of events more challenging [16]. Other challenges identified includes a loss of important forensic information such as registry entries temporary files, and metadata which could be stored in the cloud as well as a lack of tools for dealing with investigations involving cloud data centres [17]. Very few High Tech Crime Units (HTCUs) in the UK were prepared to deal with crimes involving cloud computing. Even when HTCUs are prepared to investigate such crimes, current legislation for accepting digital evidence in court presents further challenges [18].The use of cloud computing as a means of ‘speeding up’ forensics investigations. A framework which takes advantage of distributed computing resources was developed and results showed that such an environment could assist investigators examine large forensic data sets in real time [12].

The challenges can be listed as the evidence identification, legal, data acquisition and the suitability of traditional digital forensic tools to acquire data within Cloud based environments. The challenges not only exacerbate the problems of digital forensics within Cloud based environments but create a brand new front for digital forensic investigations. Also highlights the important issue of data identification with Cloud based environments [19]. Identified some research challenges, including “discovery of computation structure,” “attribution of data,” “stability of evidence,” and “presentation and visualisation of evidence”. Multi-jurisdictional law is escalating the challenge of Cloud forensics. The very nature of Cloud computing is that it is distributed worldwide [16].

3. Challenges of Cloud forensics

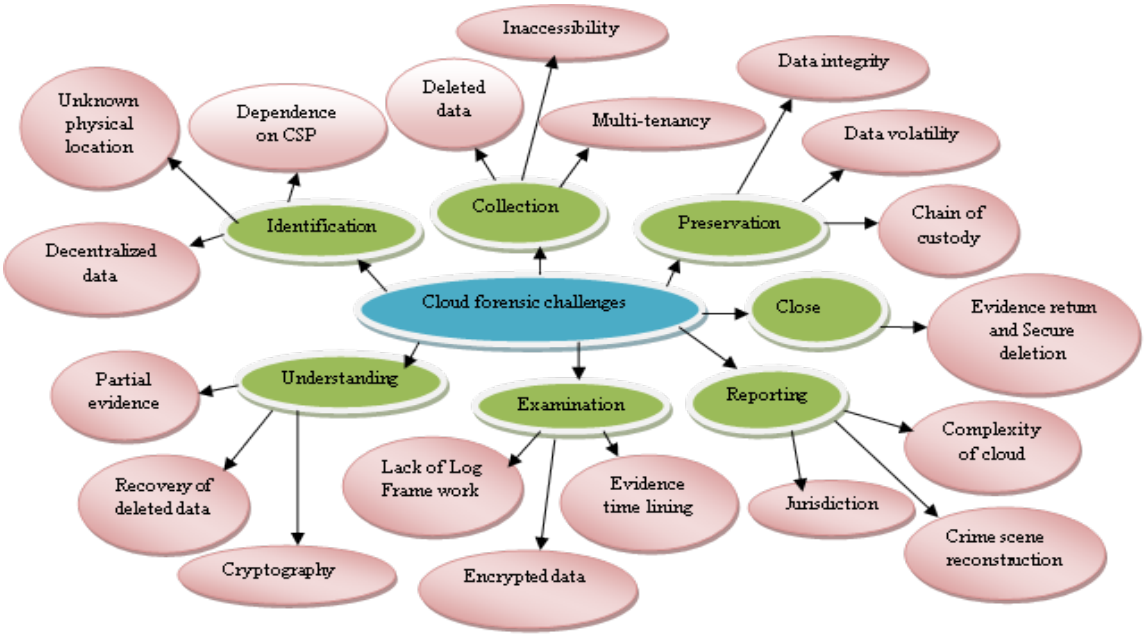

Fig. 1.Cloud forensics challenges with phases

Table 1

List of challenges and suggested solutions

Phase	Challenges	Suggested Solutions	Comments
Identification	1. Unknown or not accessible physical location	Resource tagging [13] Robust SLA with CSPs [1], SLA in support of cloud forensics [2]	Adversely affects CSPs ability to ensure flexibility, service availability and manageability. Most of the SLA guidelines are mainly focused on security requirements and less on forensic requirements.
	2. Decentralized data	Log frame work [20]	Allows data to be created, stored, processed and distributed over several data centres and physical machines. Stored data is replicated, distributed and fragmented.
	3. Dependence on CSP	SLA specifying the specific forensic Services [2]	Good SLA guarantees benefit accessibility and consistence.
Collection	1. Inaccessibility	Snapshot analysis [1]. Remote data acquisition [21]	Snapshot or forensic image is a process of taking a clone of virtual image including running system's memory, and saving the clone to a persistent storage. By data imaging tools such as EnCase, FTK Imager, X-Ways, F-Response, Paladin etc., over a secure network link.
	2. Deleted data	Frequent snapshots	Deleted data can be collected from the media using data carving methods and difficult to achieve and manage of snap shot images.
	3. Multi-tenancy and resource sharing	Isolating cloud instance [22] Sandboxing [22]&[23]	Adds to the complexity of forensics data collection and easy to seize the hardware. Popular method of isolating the instance and supported by the vendors.
Preservation	1. Data integrity	Live forensic training	Live forensic techniques and cloud provider's expertise use their own crucial environment.
	2. Chain of custody	RSA Signature [24]	Can be used to verify the chain of custody and data integrity.
	3. Data volatility	Persistent storage [1]	Having a persistent storage and keeping the storage synchronized frequently between the VM instances and persistent storage have been suggested by researchers to counter the data volatility issues [1].
Understanding	1. Recovery of deleted data	Backups and Repositories and Snapshots and Mobile forensics and computer forensic	More complex task in cloud computing environments and recovering of deleted data from backups, repositories, previous snapshots or other handsets or computer can solve.
	2. Partial evidence	Return to early stages of investigation	An examination with partial evidence is real risk because partial or incomplete evidence may be inadmissible in court.
	3. Cryptography	Brute-force and Mobile forensics	Better way to check the suspect's phones or tablets for unencrypted files or data or passwords.

Phase	Challenges	Suggested Solutions	Comments
Examination	1. Lack of Log Frame work	Comprehensive Log Management system [[20],[25],[21]]	Creates challenges in time lining of events and logs really help an investigator to connect the dots.
	2. Encrypted data	Cloud key management infrastructure [5]	Possible more future implementation
	3. Evidence time lining	Secure Logs with proper time stamps Secure Provenance [26]	End-to-end log helps to create a time line of events Provides the ownership and history of dataObjects
Reporting	1. Jurisdiction	Cross border law, International relations	Legal Agreements and a challenge presenting the case
	2. Crime scene reconstruction	Framework, process and guidelines, supported by tools and technology	Lack of applicable tools and supporting process and guidelines and reconstruction of cloud storage and evidence.
	3. Complexity of cloud	Time lining of events	Difficult to explain the complexity of cloud toJury
Close	1. Evidence return and Secure deletion	Legal training and Legal advice	Returning of the evidence is not always needed.

4. Cloud forensics: phases, challenges and solutions

4.1. Identification

- Challenge: Unknown or not accessible physical location

The cloud asset customers "tag" their assets to stamp the area of their data resources, which can likewise be utilized by CSPs to decide regardless of whether they can be moved and if so give the permitted local limit of relocation [13]. CSPs (Amazon) select geographic location and solve the Amazon's client's jurisdiction and data location. Client use CSP to identify locations of VM instances that stored to SLA.

- Challenge: Decentralized data

Cloud computing allows data to be created, stored, processed and distributed over several data centres and physical machines. The CSPs gives the details of how the logs are created and where they are stored.

- Challenge: Dependence on CSP:

Clients and investigators depend on the CSPs to identify, locate and lock forensic evidence. Logs are collected and stored at CSP and the users to depend on CSPs for accessing network logs and server logs.

4.2. Collection

- Challenge: Inaccessibility

Snapshotting is a process of taking a clone of virtual image in running state, including all the system memory, and saving the clone to a persistent storage. Snapshot technology enables customer to freeze a specific state of VM [1].

- Challenge: Deleted data

From crime scene investigation viewpoint, erased information and crediting the erased information to a particular client are crucial wellsprings of confirmation. Typically, the erased information can be gathered from the media utilizing information cutting strategies bolstered by crime scene investigation apparatuses. Notwithstanding, if there should be an occurrence of cloud, the unpredictability and flexibility of cloud situations make it substantially harder to gather the erased information [5].

- Challenge: Multi-tenancy and resource sharing

Two of the principle attributes of cloud situations are multi-tenancy and resource sharing. The first implies that a solitary framework serves numerous clients. The second one alludes to the sharing of similar equipment and programming assets between clients. This makes information area much harder in light of the fact that law implementations need to grab the particular segment of the media where the aspect's information is put away.

4.3. Preservation

- Challenge: Data integrity

Information Integrity guarantees that the confirmation is an exact portrayal of the information found in the PC framework. A few parts of the cloud condition influence the information respectability, however keeping up the honesty stays to be a pivotal part of cloud crime

scene investigation. The known strategy to protect information trustworthiness is utilizing demonstrated hash strategies for example, MD5, SHA1, SHA256 [5].

- Challenge: Chain of custody

For conventional forensic process, chain of custody can be defined as “a roadmap that shows how evidence was collected, analysed and preserved in order to be presented as evidence in court” [27]. Specialists and legitimate professionals have featured the significance of keeping up legitimate chain of care log.

- Challenge: Data volatility

Unpredictability alludes to the loss of substance in memory or capacity when the power is turned off. This is a major issue from a measurable perspective in view of the fact that if the server goes down, all procedures in memory and CPU will vanish. These issue increments in difficulty when the case includes Virtual Machines (VM). For instance, IaaS VM have no persistent storage in this way, all volatile information might be lost if the VM goes down.

4.4. Understanding

- Challenge: Recovery of deleted data

Forensic practitioners regularly can restore erased documents from storage devices, for example, hard drives, USB sticks and cell phones. But, in distributed computing, restore of the information is a challenging assignment because of the volatility and resource sharing attributes of this condition [28].

- Challenge: Partial evidence

Directing examinations with fractional confirmation is genuine risk. Incomplete information may make false positives and might reach to wrong inferences. Most lawful frameworks work under Blackstone's plan, which is the rule that "It is better that ten blameworthy people escape than that one blameless endure". Accordingly, partial or inadequate information might be forbidden in court.

- Challenge: Cryptography

More and more providers are offering encryption to their customers to protect their data. For example, Google Drive encrypts data at transmission level with HTTPS and Perfect Forward Secrecy (PFS) at service level. The 2048 RSA encryption keys are also used for validation and key exchange [29].

4.5. Examination

- Challenge: Lack of Log Frame work

All in all, cloud specialist co-ops utilize their own logging arrangement and configuration. Absence of appropriate forensically substantial log structure appropriate to distributed computing produces challenges in time covering of occasions. Be that as it may, logs are not required for investigative reason and examinations can be directed by inspecting document substance; get to time stamps and information remainders. All things considered, logs truly help an examiner to come to an obvious conclusion.

- Challenge: Encrypted data

Encryption is done by and large generally utilized by cloud client as a measure of securing the information, or to fulfil legitimate and consistence prerequisites. In any case, culprits can likewise utilize encryption for unlawful reason.[7]pointed

out the wide spread usage of encryption by criminals to hide illegal images.

- Challenge: Evidence time lining

Time lining gives a relationship of timestamps with every occasion or information thing of enthusiasm for request to remake a succession of occasions. Digital evidence must be (i) Authentic, (ii) Reliable, (iii) Complete, (iv) Believable and (v) Admissible [15].

4.6. Reporting

- Challenge: Jurisdiction

Cloud forensics, being a multi-dimensional issue and consisting of technical, organizational and legal domains, requires collaboration between international law enforcement agencies and legal framework to conduct and present crimes conducted using cloud computing [30].

- Challenge: Crime scene reconstruction

Reconstructing crime scene in the cloud remains as a challenge, due to lack of applicable tools and supporting process and guidelines. The algorithms and software tools for reconstruction of cloud

storage and evidence are yet to be validated and developed [5].

- Challenge: Complexity of cloud

Complexity of cloud means there are very limited or no understanding of cloud computing technology. Therefore expert witness will be faced with the daunting task of ensuring juries fully understand the principles and technology of cloud computing [27]. In general time lining events would help to explain the case better to a jury and easier to understand.

4.7. Close

- Challenge: Evidence return and secure deletion

Removing of data should be secured in such a way that it would be infeasible to recover them. Forensic practitioners need legal training and legal advice to know what to do with the data depending on the law.

5. Proposed Model

Fig.2. Shows the proposed model to perform forensic investigation process in cloud computing environment using digital evidence. Malicious activity are distinguished when clients of that play out any movement like over the top access from area, transfer malware to various frameworks in the cloud foundation, exceptional number of downloads and transfers in a brief timeframe, dispatch dynamic assault focuses, breaking passwords, translating/building web tables or rainbow tables, defilement or erasure of touchy information, noxious information hosing, adjusting information, executing botnet charges. Intrusion Detection Systems (IDS) are consolidated in all the virtual machine for checking malicious activities. The concept of the proposed model is that the CSP stores digital evidence whose activities are identified as malicious by an intrusion detection system. The CSP should be requested for log files and the search team collects and processes the log files. The search team identifies the sources of evidence, and collect the digital evidences. Isolation saves corruption and impurity of collected evidence. The investigator team preserve the digital evidence such as computer hard disk, mobile phone, e-mail file etc. and analysis this evidences. The forensic officer reporting and presentation the evidence and finally close the investigation process.

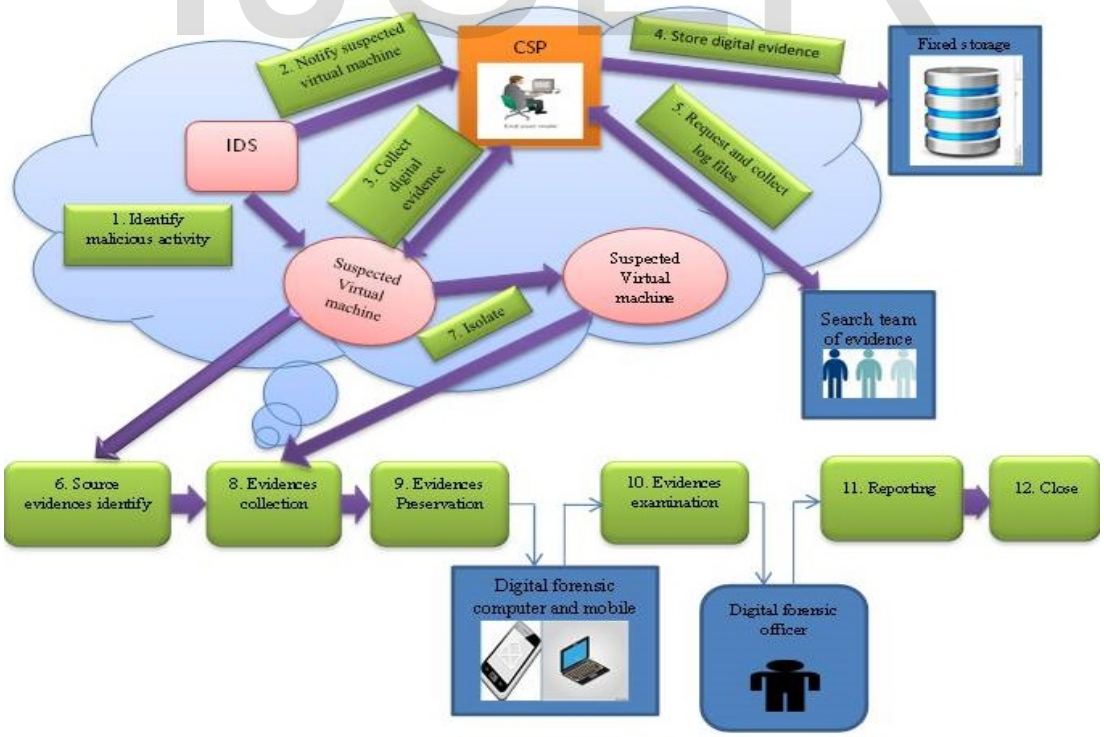

Fig. 2.Model of digital forensics process in cloud environment.

6. Conclusion

The requirement for cloud forensics sciences is on the increase, due to its quick development in cloud computing and because of the likelihood of cloud-related crime happening in the advanced world. An ever increasing number of organizations and people are depending on cloud computing for their information, applications and services. This expansion of cloud computing use has brought many challenges to specialists. In this paper, the challenges are summarised faced in cloud forensics and the suggested solutions are searched to overcome some of technical challenges. Moreover, having such solution can strengthen evidence acceptability in the court and will give a better resources use including time and cost. We proposed here a new model for describing the challenges occurred in different phases in cloud forensics and collects all necessary information related to deceitful activities required for forensics analysis. Thus, stronger worldwide participation for cloud forensics is required.

Acknowledgments

We would like to articulate our deep gratitude to thefirst author who has shared his excellent idea, suggestions and inspiration; we are carrying out our work.

References

[1] Birk, D. and C. Wegener. Technical issues of forensic investigations in cloud computing environments. in Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on. 2011. IEEE.

[2] Ruan, K., et al. Key Terms for Service Level Agreements to Support Cloud Forensics. in IFIP Int. Conf. Digital Forensics. 2012. Springer.

[3] Martini, B. and K.-K.R. Choo, An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 2012. **9**(2): p. 71-80.

[4] Nasreldin, M.M., et al., Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing. International Journal of Computer Science Issues (IJCSI), 2015. **12**(1): p. 153.

[5] Pichan, A., M. Lazarescu, and S.T. Soh, Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, 2015. **13**: p. 38-57.

[6] Palmer, G., A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 2001.

[7] McKemmish, R., What is forensic computing? 1999: Australian Institute of Criminology Canberra.

[8] Kruse II, W.G. and J.G. Heiser, Computer forensics: incident response essentials. 2001: Pearson Education.

[9] Mell, P. and T. Grance, The NIST definition of cloud computing. 2011.

[10]Mell, P. and T. Grance, The NIST definition of cloud computing. 2010, Assoc Computing Machinery 2 PENN PLAZA, STE 701, NEW YORK, NY 10121-0701 USA.

[11] Zawoad, S. and R. Hasan, Cloud forensics: a meta-study of challenges, approaches, and open problems. arXiv preprint arXiv:1302.6312, 2013.

[12] Roussev, V., et al., A cloud computing platform for large-scale forensic computing. Advances in Digital Forensics V, 2009: p. 201-214.

[13] Hay, B., K. Nance, and M. Bishop. Storm clouds rising: security challenges for IaaS cloud computing. in System Sciences (HICSS), 2011 44th Hawaii International Conference on. 2011. IEEE.

[14] Hooper, C., B. Martini, and K.-K.R. Choo, Cloud computing and its implications for cybercrime investigations in Australia. Computer Law & Security Review, 2013. **29**(2): p. 152-163.

[15] Reilly, D., C. Wren, and T. Berry. Cloud computing: Forensic challenges for law enforcement. in Internet Technology and Secured Transactions (ICITST), 2010 International Conference for. 2010. IEEE.

[16] Wolthusen, S.D. Overcast: Forensic discovery in cloud environments. in IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on. 2009. IEEE.

[17] Taylor, M., et al., Digital evidence in cloud computing systems. Computer Law & Security Review, 2010. **26**(3): p. 304-308.

[18] Biggs, S. and S. Vidalis. Cloud computing: The impact on digital forensic investigations. in Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. 2009. IEEE.

[19] Baryamureeba, V. and F. Tushabe. The enhanced digital investigation process model. in Proceedings of the Fourth Digital Forensic Research Workshop. 2004.

[20] Marty, R. Cloud application logging for forensics. in Proceedings of the 2011 ACM Symposium on Applied Computing. 2011. ACM.

[21] Dykstra, J. and A.T. Sherman, Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 2012. **9**: p. S90-S98.

[22] Delport, W., M. Köhn, and M.S. Olivier. Isolating a cloud instance for a digital forensic investigation. in ISSA. 2011.

[23] Greamo, C. and A. Ghosh, Sandboxing and virtualization: Modern tools for combating malware. IEEE Security & Privacy, 2011. **9**(2): p. 79-82.

[24] Lin, C.-H., C.Y. Lee, and T.-W. Wu, A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics. International journal of security and its Applications, 2012. **6**(2): p. 241-244.

[25] Sang, T. A log based approach to make digital forensics easier on cloud computing. in Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on. 2013. IEEE.

[26] Lu, R., et al. Secure provenance: the essential of bread and butter of data forensics in cloud computing. in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. 2010. ACM.

[27] Grispos, G., T. Storer, and W.B. Glisson, Calm before the storm: the challenges of cloud. Emerging digital forensics applications for crime detection, prevention, and security, 2013. **4**(1): p. 28-48.

[28] Jones, R., Safer live forensic acquisition. Computer Science Laboratory, University of Kent at, 2007.

[29] Miranda Lopez, E., S.Y. Moon, and J.H. Park, Scenario-Based Digital Forensics Challenges in Cloud Computing. Symmetry, 2016. **8**(10): p. 107.

[30] Ruan, K., et al. Cloud forensics. in IFIP International Conference on Digital Forensics. 2011. Springer.