

Cloud Computing Forensics; Challenges and Future Perspectives

Dr. Ranjan Kumar Mondal

Assistant Professor, Department of CSE, Swami
Vivekananda University, Kolkata, WB

ranjankm@svu.ac.in

Abstract

In recent years, cloud computing has grown in popularity and developed into an efficient and economical computing paradigm. It might be among the technologies that have had the most influence in the whole history of computing. Unfortunately, cloud service providers or clients have not yet created significant forensic tools that may help investigate criminal activity in the cloud. Given the difficulty of preventing criminal targeting and cloud vulnerabilities, it is essential to understand the potential procedures for conducting digital forensic investigations into the cloud. This is due to the difficulty in avoiding criminal targeting and cloud vulnerabilities. Within this framework, the present research looks at cloud forensic tools, cloud forensic methodology, and future developments in cloud forensics. The study also examines cloud forensic methodologies, with the aim of providing valuable insights and solutions to the challenges in cloud computing forensics.

Keywords: software as a service, cloud computing, cloud forensics, and forensic tools.

1. Introduction

The cloud has not changed much since it was initially developed, nor has it made notable advancements in several vital areas [1]. The idea of cloud computing is the way of the future and will provide businesses with enormous financial

advantages. Numerous new opportunities have emerged with the advent of cloud computing, some more advantageous than others [2]. Because of this growth, cloud computing has become a new front in the fight against cybercrime, bringing new risks and problems that might endanger enterprises [3]. Users with bad intentions may exploit serious security flaws in the cloud. Most cloud products may be accessed remotely by logging onto virtual computers, carrying out tasks related to those services, and then wiping the virtual machines [4]. This is made feasible because cloud goods don't need physical infrastructure users to own. Cloud criticisms increased as cloud computing became more widespread [5]. When investigating crimes committed in the cloud, the methodology differs somewhat from that used in traditional settings. Many forensics topics, such as trust, network forensics, evidence collection, privacy, and data provenance, emerged throughout the previous ten years of study. When dealing with this kind of computing, investigators specializing in digital forensics have a particular set of difficulties [6]. Furthermore, it emphasizes how important it is to create specialized forensic tools that can be used to collect and examine digital evidence in the digital age—including a range of service models and structural configurations—sometimes even before the evidence is wholly destroyed [7]. These variables have also created new challenges for digital forensic investigators trying to get total access to and control over the distribution of cloud resources. Operating systems that operate on top of another operating system as if running on its hardware are referred to as “virtualization” in computing. Cloud computing emerged as a consequence of virtualization [8, 9]. These and other emerging computer paradigms open the door for new types of cybercrime. Although research efforts in digital forensics for conventional computer paradigms, including virtual environments, have shown better results, these methodologies may not immediately apply in the cloud. When operating in a cloud environment, user data is scattered and often lives in inaccessible places to forensics investigators. The next sections of this article are structured as follows: first, an overview of current and future advancements in cloud forensics is given; second, a review of

tools and techniques for cloud forensics is given; and third, an introduction to cloud incident management is given [10].

Businesses are moving toward migrating their data to the cloud as they become more aware of the advantages of cloud computing. Because of this change, there is an increased danger connected with using cloud resources, which makes cyber criminals more interested in taking advantage of them [11]. The size of an average digital forensic case is growing at a rate of 35 percent per year, which indicates that the number of digital crimes is increasing quickly [12]. Consequently, it is critical to prioritize cloud computer security and cloud computing forensic investigation. It should not be shocking to learn that conversing about either subject requires a basic comprehension of cloud infrastructure and digital forensic investigation [13–17].

The National Institute of Standards and Technology (NIST) of the United States 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” [18–20]. In the modern world, cloud computing can be divided into three main service categories: platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS). Infrastructure as a service (IaaS) provides customers with a virtualized machine, an environment somewhat similar to a physical machine but with some limitations. Platform as a service (PaaS) typically offers customers access to an Application Programming Interface (API) [21–24].

2. A SHORT GUIDE TO CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) describes cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of resources.”

Configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or

interaction from service providers. Cloud A is the flexibility to scale up or down computational requirements to client requirements. The flexibility to access a network from anywhere at any time is called connectivity. Multi-tenancy refers to the capacity to accommodate multiple tenants on a single set of physical resources, such as shared memory, storage space, and network connections. Visibility is the capacity for customers to fully comprehend and manage the details, use, and costs of their cloud deployments. Measured service allows customers to be charged based on the amount of offered items they utilize [25–30].

The various advantages of cloud computing have contributed significantly to its rapid growth. The main benefit of cloud computing is realizing economies of scale due to the flexible and effective use of available resources and specialization. Cloud computing offers a wide range of deployment and service delivery options. Public cloud deployment is one of the deployment strategies. This method uses the internet to make computer tools and services available to the general populace. A cloud owned and managed by a separate third party and offering cloud services is called a public cloud [12]. A private cloud is a computer environment a firm owns and controls entirely, internally or through a third party. Private clouds are created to support a single tenant and allow more control over all computing resources [31]. As an alternative to private cloud computing, community cloud involves the pooling and sharing data storage and processing capacity across several companies that uphold the same privacy, security, and other legal criteria. A hybrid cloud is a combination of two or more clouds that are connected via standardized or proprietary technologies to enable interoperability. 1. Software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS) are three paradigms for cloud services that are widely accepted, according to Jansen and Grance (2011) [32, 33]. Software-as-a-service (SaaS) is a software deployment method in which one or more applications are made available on demand as turnkey services that can be accessed through a thin client with the computing resources necessary to operate them. This strategy aims to reduce the overall cost of creating hardware and software, as well as that

of maintaining and using them. In this paradigm, consumers have limited rights, such as the ability to alter application settings and their data, but CSPs have total authority over the apps and the underlying infrastructure. Platform-as-a-Service, or PaaS for short, is a method of deploying software. The computing platform is made available as an on-demand service and used as the basis for developing and deploying applications [34]. Its main goal is to make acquiring, setting up, and managing the platform's underlying hardware and software components—such as databases, operating systems, and development tools—more straightforward, minimizing costs and complexity. IaaS, or infrastructure-as-a-service, is a software deployment paradigm in which the essential components of a computer system, such as servers, software, and networking hardware, are made available as a service that can be accessed whenever needed. This method enables the construction of a foundation for the development and execution of applications. Because they obtain those resources as virtualized objects that can be managed through a service interface, customers of infrastructure as a service don't need to worry about purchasing, storing, or managing basic hardware and software infrastructure components [35-39].

3. A SUMMARY OF CLOUD FORENSICS

The term “cloud forensics” refers to the application of digital forensics on cloud computing platforms; this field is being explored through interdisciplinary research. The newly established NIST cloud forensic working group defined “cloud computing forensic science” as “the application of scientific principles, technological practices, and derived and proven methods to process past cloud computing events through identification, collection, preservation, examination, and reporting of digital data to facilitate the reconstruction of these events.” The CSPs swapping services further complicates the situation and makes it more difficult to follow the evolution of events; therefore, forensic procedures that would be appropriate in a traditional setting—one that does not involve cloud computing—would not be applicable here.

The technical, organizational, and legal dimensions comprise cloud forensics [41]. The forensic investigation process in the context of cloud computing necessitates the use of specific techniques and tools, which are referred to as the technical dimension as a whole. This includes gathering data, real-time forensics, separating evidence, and preventative actions. On the other hand, the organizational component looks at the forensics aspects of the organization. The participants included CSPs, clients, legal counsel, and issue handlers. It also covers legally binding service level agreements (SLAs), rules, and regulations [41,42]. Last, the legal aspect includes creating rules and agreements to guarantee that forensic activities don't break the laws and regulations in the countries where the data is stored or collected while protecting co-tenants' privacy with the same infrastructure. This is achieved by ensuring that forensic procedures don't violate the rules and laws of the countries where the data is stored or gathered [43].

4. CLOUD FORENSIC STEPS [43–48]

- **Analysis:** The following procedures are used while using cloud forensics to investigate.
- **Identification:** Examiners must determine whether potentially harmful activity or improper behavior has occurred within the cloud-based services. Such activities include suspicious cloud events, individual complaints, anomalies found by intrusion detection systems, and monitoring and profiling resulting from audit trails.
- **Preservation and Collection:** In this stage, data is gathered from all available sources in a way that does not compromise its integrity in compliance with forensic and legal criteria. For the sake of a future investigation, every piece of information and evidence has been stored safely. There is a possibility that the gathering of data may be needed to store vast volumes of data. As a consequence, investigators must consider the laws and regulations that regulate data protection and privacy and the consequences these laws and regulations have for evidence stored in the cloud. When obtaining data from the cloud vendor side, you should always consider the data of

any other users or organizations. An accurate representation of the data stored in the cloud must be gathered before continuing the investigation. An investigator can attempt to get and keep data saved in the cloud by serving the cloud service provider with a court order.

- **Detection: After collecting data:** various strategies and algorithms (such as pattern matching and filtering) are used to find potentially dangerous code or questionable behavioral patterns.

- **Analysis:** Following detection, forensic techniques are used to assess and investigate the data and the crime committed. Law enforcement officials may focus their investigation on a specific organization or person to gather evidence. Following data analysis, the testimony must be shared with law enforcement officials and the victim organization or person.

- **Presentation:** The last phase entails presenting the evidence gathered before a judge or legal authority. This is accomplished using an adequately prepared report, the conclusions of which must be provided by testimonies regarding the research topic.

- **Documentation:** It is difficult to persuade the court that the evidence collected throughout the investigation was accurately recorded and that no modifications were made to it in the first phases of the process.

5. IS CLOUD SIMULATING A LOOMING STORM OR A POSSIBLE RAY OF SUNSHINE?

Software, the computing platform, and the computing infrastructure can all be considered services without considering how or where they are provided because there is no distinction between them. Cloud computing strives to the idea of computers as a utility, providing services like water, gas, electricity, and telephones. It also symbolizes the desire to use computational resources to provide accurate services.

Major industry players have realized the potential of cloud computing, as evidenced by the fact that each of the top five software companies has a sizable cloud product portfolio in

terms of sales revenue. Although there is a lot of material in the community that illustrates the basic concepts, the phrase “cloud computing” is not yet understood by everyone. Several authors have put forth the idea that cloud computing is a development of cluster computing. Cloud computing is called cluster computing with software as a service [49-53]. There are five key characteristics of cloud computing, three delivery options, and four deployment models. This is a concept that is simple to comprehend. As of this writing, perspectives on whether cloud computing might promote or oppose computer forensics investigations are divided. One group thinks cloud computing might support such inquiries, while the other thinks it will hinder them. In the next section, we will analyze the topic’s good and bad elements in more detail after providing a high-level summary of both sides of the argument [54-56]. On the one hand, to accommodate investigations conducted on cloud-based systems, the computer forensic process model would need to be modified, and a new set of procedures would need to be put in place. On the other hand, using the resources and services made available by cloud computing might be advantageous for computer forensic investigations to support the inquiry [57, 58]. The main benefit of cloud computing is its capacity for centralizing data storage; having all of one’s data in one place enhances forensic readiness, leading to a quicker and more well-coordinated response to crises. When IaaS providers can access centralized data, they can build a dedicated forensic server within the cloud. When needed, this server is available for usage. The services and resources that cloud computing platforms may offer, or, more precisely, the scope and power of these services, confer further benefits to the discipline of computer forensics. A huge advantage for the computer forensic investigator is the availability of potentially petabytes of storage and highly available compute-intensive tools. These two elements both influence the research process. During an investigation, a detective may gather many images of hard discs. Infrastructure as a Service, or IaaS, might potentially be used to store these pictures on the cloud. Second, forensic investigators may use the high availability of compute-intensive resources for compute-intensive activities

[59,60]. Forensic investigators, for example, may need to break passwords or encryption keys or review many photos, which may be time-consuming and taxing on a computer's processing power and memory [61, 62]. For instance, an MD5 hash is created when a piece of data is stored in Amazon S3. This indicates that it is no longer necessary to generate the time-consuming MD5 checksums that were previously required. The various log files that might be discovered on a computer can be a useful source of information during a forensic examination. However, logging is occasionally treated as an afterthought, and as a result, insufficient disc space is provided, or no logging occurs at all. Due to the scale at which cloud storage is used, logging may be done and configured to the proper level, and logs can be made available upon request. This is made feasible by the cloud's scalability [62, 63]. A C2 audit trail represents the enhanced logging capabilities of modern operating systems. However, due to worries that it can impede performance and increase log volume, this option is rarely used. Better logging may be achieved with cloud computing, and the granularity of logging can be changed to suit specific needs. Virtualization, which has been considered differently as both a benefit and a drawback, is the final area of concern. As was previously said, in cloud computing settings, virtualization is used to enable several users to use the same resources. Software, platforms, and infrastructure are just a few resources that may all be virtualized. It was also highlighted that a bit-by-bit copy of a disc image must be made using the required software for forensically sound data collection. Recording memory images during live investigations takes extra effort and time because memory must be frozen before the copied host loses power. However, these steps are unnecessary in a virtual environment because administrative tools like snapshots and other functionality make taking photos of the disc and memory easy. However, law enforcement authorities (i.e., the guidelines set by ACPO) have not yet determined the forensic validity of this form of acquisition. Data collecting is cloud computing's worst drawback when considered from a forensic angle. This is the procedure of locating the precise location of data storage and then physically retrieving it. The search

and seizure tactics used in traditional computer forensics are not feasible since the evidence is kept in cloud data centers. These methods are used to gather evidence. Additionally, it is exceedingly difficult, if not impossible, to maintain a chain of custody about collecting the evidence [64]. It is nearly hard for investigators to adhere to the ACPO advice since employing cloud computing makes it difficult, if not impossible, to uphold ACPO standards. Cloud computing is to blame for this [65]. The four guiding principles for the procedures and level of knowledge required for evidence management are laid forth in the ACPO manual. These requirements cannot be met since clouds function as remote data centers, making the ACPO advice unnecessary. Due to this, the validity, integrity, and admissibility of the evidence in a British court process would thus be called into doubt [66]. There is a general loss of control throughout the forensic investigation since the data are stored elsewhere where access is impossible. Overall, this is the situation. Due to a lack of knowledge of where data is held, it is harder to assemble a sequence of events and build a timeline. This, in turn, makes it more difficult to recreate a crime scene. Various other issues discussed further down the page can potentially hinder the study. The gathering of data and the loss of control are two drawbacks. the disposal of important objects, some of which would have served as key pieces of evidence. In cloud data centers, it could be difficult, if not impossible, to access items like registry entries, temporary files, and RAM (often because virtualization is utilized) [67-69]. There is a potential that the metadata will be lost when data is downloaded from the cloud. It is useful for the investigator to access metadata, such as when the file was created, edited, and accessed while performing a forensic investigation. Many investigators still prefer to carry out their authentication rather than depending on the cloud storage service's hash authentication, even though certain cloud storage providers, including Amazon S3, offer a mechanism to confirm data (using MD5 checksums). This occurs as a result of the inconsistency of cloud storage services. Another restriction is the absence of tool support for using cloud data centers. Although computer forensics is still a young subject of study, it has advanced to the point where tools

are suitable for handling typically localized investigations [70-72]. The forensic investigator may utilize instruments like EnCase, Helix, and FTK to help with tasks like initial data gathering, which produces acceptable written evidence in a court environment. Forensic investigators can utilize various instruments to help them with these duties. The last concern results from computer forensics' legal and ethical components. This problem results from the requirement that all digital evidence gathered during an inquiry be presented to a jury, who will

Render a verdict on the matter. In traditional computer forensics, the investigators must present their findings to the jury. Consequently, investigators often find themselves awkward in explaining how evidence was gathered and what it suggests about the case in terms specific to their field. This is especially true when working with conventional, locally based computer systems; cloud data centers, which may be thousands of miles away, run 40,000 virtual machines (VMs) across 512 servers and are accessed by 1000 tenants, of which the accessed is one, present their findings to the jury. This may be too much information for the average juror to process, especially considering they only know how to use a home computer [73-75].

6. The difficulties that cloud forensics faces

As expected, the cloud forensics field presents several unique hurdles. These challenges include technical as well as legal concerns [76]. Some possible problems that may arise while performing a forensic investigation in the cloud include the following:

- **Problems:** Relating to the user's home jurisdiction: Cloud services are frequently hosted in states or countries other than the user's location. While users may occasionally be able to select their preferred location, this is not always the case. For example, Google maintains cloud servers in Australia, Europe, Asia, North America, and South America. This may complicate determining which jurisdiction over the offense [77].

- **Unstable:** In traditional digital forensics investigations, the IT environment is typically “frozen” to prevent disruptions or new problems while investigators finish their work. This ensures that the probe proceeds without a hitch. Still, since public cloud providers may serve millions or even hundreds of thousands of users, this is frequently impossible, leaving the environment dynamic and potentially unstable [78].

- **Physical access:** In some instances, forensics can benefit from physically inspecting a cloud server. However, large cloud providers can find this challenging because they enforce strict security policies to keep unauthorized individuals out of the building. Furthermore, as previously mentioned, the cloud server is not guaranteed to be physically close to the investigator [79].

- **Decentralization:** Cloud organizations often store files across several servers or data centers to increase availability and dependability. This fragmentation and decentralization makes it more challenging to identify the issue and do forensics [80].

- **Data deleted or unavailable:** The information cloud providers give investigators can differ. For example, log files might not always be available. If data is deleted due to criminal activity, it can be challenging to recover it, identify its owner, and utilize it for cloud forensic analysis [81].

7. What’s New In Cloud Forensics And What’s Hot Right Now

Digital forensics, network forensics, and hardware forensics are only a few of the many different forms of forensic investigation that collectively go under the umbrella phrase “cloud forensics” [82]. Various cloud stakeholders (such as cloud providers, cloud customers, cloud brokers, cloud carriers, and cloud auditors) must interact with one another to simplify internal and external investigations. Basic features of cloud computing include a high degree of virtualization, data duplication, jurisdiction, and multi-tenancy. These characteristics increase the complexity of cloud forensics to various degrees [83]. Due to the apparent resources it gives and its low cost, wide availability, and flexibility, cloud

forensics have become widely used in the area of forensics. There are several options for database security, software integration, and application development in cloud forensics, including private, hybrid, and public models [84-86]. Governments and organizations of all sizes may benefit from various advantages thanks to cloud computing, including high scalability, decreased IT expenses, backup, and speedy installation [1]. Similarly, to achieve the objectives of low latency and scalability, cloud-based telecommunications service providers are moving their data centers to a range of various geographic locations. However, the rise in online criminal behavior and the broadening impact of cloud computing pose a more significant threat. Security experts have expressed concern about how challenging cloud forensics are to do. Cybercriminals' primary objective is to exploit the cloud's weaknesses. An example of a potential application in digital forensics is an external inquiry conducted in a cloud-based environment [87,88]. In this area, events in the cloud are processed, and the results are retrieved using academic standards and norms, conventional practices, and cutting-edge technology. Additionally, cloud storage offers a wide range of virtualization, replication, and multi-tenancy capabilities. Additionally, the technique used in cloud forensics depends on how the software platform is installed and operates. There are a lot fewer possibilities for monitoring techniques and services in Platform as a Service (PaaS) and Software as a Service (SaaS) implementations [89-93].

Despite the complexity of cloud forensics, the growth of cloud computing has undoubtedly led to concerns about users' security and privacy. Many currently hired forensics officers have witnessed a significant increase in their engagement in authorization, authentication, and accounting (AAA) due to the advent of cloud technology. This is so that malicious assaults may be looked into and identified using digital proof. It has high precision and contrasts sharply with other forensic techniques that employ the data, making it equivalent to traditional forensic methods for extracting evidence from log data. Legal, organizational, and technological forensics are the three subcategories that comprise cloud forensics. Laws and

agreements have been made to guarantee that digital forensic methods do not violate the rules regulating their usage [94,95]. Instead, a wide range of corporate policy factors is involved in computer forensics organizations [96]. Last, the technological scope describes the procedures and methodologies used to conduct a cloud investigation. Cloud forensics has become a regular procedure in digital forensics. It facilitates the use of forensics as an investigative tool by integrating cloud capabilities like remote analysis, monitoring, and scaling, such as the ability to manage huge workloads. Now, forensics may be employed as a research tool.

Predicted Developments and Changes in Cloud Computing: A Multi-Tenancy Cloud trust model with Quality of Service (QoS) monitoring. This model mainly focuses on the Infrastructure as a Service (IaaS) platform and shows why it.

It is imperative to provide cloud solution users with an avenue to gauge the reliability and caliber of services offered by cloud service providers before committing to such services; the recommended methodology necessitates continuous, real-time service quality monitoring. This builds customer trust and guarantees customers enroll in cloud services meeting predetermined standards and metrics. It also facilitates the assessment of cloud service providers.

Security for Logging Service provided: To undertake investigations that help expose unlawful or fraudulent activities perpetrated by rivals and aid in their prosecution, logs in cloud infrastructures are crucial [97]. Although cloud platforms are advantageous computing models, Zawoad et al. discovered that the computational power and storage resources made available by computer clouds might also tempt dishonest users to carry out attacks via the platforms. This realization came about during the development of their Secure Logging as a Service model. This was brought up as Zawoad et al. developed their Secure Logging as a Service approach [98]. Other researchers point out difficulties with using the Secure Logging as a Service Scheme (SecLaaS) to perform cloud forensics, such as a decreased degree of control when users of cloud services heavily depend on service providers to collect logs from computer clouds [99].

They explore these concerns about the Secure Logging as a Service Scheme (SecLaaS). The results of this study show that relying excessively on cloud service providers might lead to a loss of confidence in their investigators, many of whom are unqualified. They caution that bad actors may manipulate the logs using their power over the created logs if cloud service providers are compromised. Additionally, they warn that cloud service providers can refuse to comply with requests for all required logs if such requests clash with their internal data protection requirements. The main goal of the proposed framework was to overcome the difficulties caused by the lack of logging standards, the erratic nature of logs, and the multi-tenancy feature of cloud platforms. These issues emerge because shared hardware, which could also store the logs of multiple other users, may be used to provide virtualized services. Architecture for the Cloud with Forensic Capabilities Forensic Supported To support a trustworthy digital forensics operation on cloud systems, cloud architecture emphasizes the importance of securely preserving produced logs, proof of data custody, and provenance information in addition to timestamp data [100]. According to Zawoad et al., any data collected should be accessible to cloud users, investigators, and legal authorities [101-103].

Conclusion

One of the most revolutionary innovations in computer history may very well be cloud computing. Both cloud service providers and users have yet to develop suitable forensic tools that may help with cloud-based criminal activity investigations. About crimes using computers, mobile devices, and the Internet, computer forensics is a crucial area of computer science. Computer forensics' primary function is to conduct criminal investigations by examining any evidence discovered in digital forms. Because there have been so many recent reports of cybercrimes, it is now more important than ever to create specialized forensic tools for gathering and analyzing digital evidence in the digital world, sometimes even before it has been lost or erased. Digital forensic investigators now face a more significant barrier in gaining complete access to and control over the dispersed

cloud resources due to the new cloud computing paradigm's distinctive architecture and variety of service models. While the present chapter begins by outlining the significance of digital forensics in general, it concentrates mainly on their function in cybercrime investigations in the digital cloud. This review defines the cloud computing paradigm's fundamental ideas, structures, and service paradigms. The key benefits, drawbacks, difficulties, and strategies for digital forensic processes are then discussed, along with methods for supporting the isolation and preservation of digital evidence. The review article highlights several issues in cloud forensic analysis that require more study.

References

Federal Bureau of Investigation (FBI), "Regional Computer Forensics Laboratory (RCFL)", Program Annual Report for Fiscal Year 2007, Washington, DC, 2008

Ben Kepes, "Understanding the Cloud Computing Stack SaaS, Paas, IaaS", Diversity Limited, 2011, [URL] <http://broadcast.rackspace.com/hosting-knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf>

Dominik Birk, Christoph Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments", Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE Sixth International Workshop on, vol., no., pp.1-10, 26-26 May 2011, [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=6159124>

ACPO E-Crime Working Group, "Good Practice Guide for Computer-Based Electronic Evidence", 7safe information security website, [URL] <http://7safe.com/electronic-evidence/index.html>

Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication, Spetember 2011, [URL] <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

Hyunsang Kim, Sangjin Lee, Jongin Lim, "Digital evidence collection process in integrity and memory information

gathering", *Systematic Approaches to Digital Forensic Engineering*, 2005. First International Workshop on, vol., no., pp. 236- 247, 7-9 Nov. 2005, [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=1592536>

Brezinski,D, Killalea,T, "Guidelines for Evidence Collection and Archiving", RFC-3227/BCP-55, The Internet Engineering Task Force (IETF), Feburary 2002, [URL] <http://www.ietf.org/rfc/rfc3227.txt>

Shaftab Ahmed, M. Yasin Akhtar Raja, "Tackling cloud security issues and forensics model", *High-Capacity Optical Networks and Enabling Technologies (HONET)*, 2010, vol., no., pp.190-195, 19-21 Dec. 2010 [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=5715771>

Stephen Biggs, Stilianos Vidalis, "Cloud Computing: The impact on digital forensic investigations", *Internet Technology and Secured Transactions*, 2009. ICITST 2009. International Conference for, vol., no., pp.1-6, 9-12 Nov. 2009, [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=5402561>

Reilly.D, Wren.C, Berry.T, "Cloud computing: Forensic challenges for law enforcement", *Internet Technology and Secured Transactions (ICITST)*, 2010 International Conference for, vol., no., pp.1-7, 8-11 Nov. 2010 [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=5678033>

Cheng Yan, "Cybercrime forensic system in cloud computing", *Image Analysis and Signal Processing (IASP)*, 2011 International Conference on, vol., no., pp.612-615, 21-23 Oct. 2011, [URL] <http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber=6109117>

Gary C. Kessler, "Anti-Forensics and the Digital Investigator, Champlain College Burlington", 5th Australian Digital Forensics Conference, December 2007, [URL] <http://ro.ecu.edu.au/adf/1/>

Hong Guo, Shang, Bo Jin, "Forensic Investigations in Cloud Environments", *International Conference on Opto-Electronics Engineering and Information Science (ICOEIS)*

2011), December 23-25, Xian, China, 2011, [URL] <http://www.asaas.org/ICOEIS2011/N774.pdf>