Journal of Digital Investigation

Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results

Keyun Ruan, Joe Carthy, Tahar Kechadi, Ibrahim Baggili

Center for Cybersecurity and Cybercrime Investigation, University College Dublin, Dublin 4, Dublin,Ireland

Zayed University, Abu Dhabi, United Arab Emirates

Abstract

With the rapid growth of cloud adoption in both private and public sectors globally, cloud computing environments have become a new battlefield for cyber crime. In this paper, the researchers present the results and analysis of a survey that had been widely circulated among digital forensic experts and practitioners worldwide on cloud forensics and critical criteria for cloud forensic capability in order to better understand the key fundamental issues of cloud forensics such as its definition, scope, challenges, opportunities as well as missing capabilities based on the 257 collected responses of the survey.

Keywords: Cloud forensics; cloud computing; digital investigation; survey; definition

1. Introduction

Cloud adoption has seen rapid growth in both private and public sectors globally. Gartner estimates that by 2014 “Personal Cloud” will replace “Personal Computer” (Kleynhans 2012). Cloud computing environment is inevitably becoming a new battlefield of cybercrime. The term cloud forensics was first introduced in Ruan et al. 2011A to identify the rapidly emerging section in digital investigation and its various challenges.

Based on the concept proposed in Ruan et al. 2011A, researchers then carried out a survey in order to better understand the key fundamental issues of cloud forensics such as its definition, scope, challenges, opportunities as well as forensic capabilities to be assessed and developed in cloud environments.

The survey had gained a high volume of interest immediately after launching and received 156 responses by March 2011. A preliminary analysis of the survey results based on the 156 responses was presented in Ruan et al. 2011B in order to share findings with the research community. Up to 1 January 2012, the survey had received 257 responses. This paper presents the results and analysis based on these 257 responses.

2. Methodology

The survey was hosted by Zayed University, United Arab Emirates (UAE). Before filling out the survey, all participants are required to agree to a consent form, which specifies the voluntary nature of participation and confidentiality of the survey results. Demographic information of the participants is collected at the beginning of the survey.

The main body of the survey is divided into three sections:

- Part I Background
- Part II Cloud forensic research and techniques
- Part III Critical criteria for forensic capability

In Part I, the questions cover the definition of cloud computing, cloud computing as a trend, the definition of cloud forensics, the significance of cloud forensics, the impact of cloud forensics, the dimensions of cloud forensics, and the usage of cloud forensics.

In Part II, the questions cover the challenges and opportunities of cloud forensics, valuable research directions of cloud forensics, as well as parties involved in a cloud investigation.

In Part III, the questions cover parties need to be assessed on cloud forensic capability, importance of procedures, toolkits, staffing, policy, agreement, and guideline for cloud forensics.

As one of the first widely circulated survey on the topic of cloud forensics, the researchers believe the questions were designed to cover a comprehensive range of key issues for discussion.

3. Demographics

216 participants answered the question of age, and results are shown in Table 1 below. 7% of the respondents are between 19 to 24 years old, 15% of the respondents are between 25 to 30 years old, 34% of them are between 31 to 40 years old, and 37% of them are above 40.

Table 1. Demographics: age

Age	Percentage
None	7
19-24	7
25-30	15
31-40	34
Above 40	37

198 participants answered the question of gender, and the results are shown in Table 2 below. 15% of the respondents are female and 85% of the respondents are male.

Table 2. Demographics: gender

Age	Percentage
Male	85
Female	15

202 participants answered the question of level of education, and the results are shown in Table 3 below. 32% of the respondents hold Bachelor (or Diploma) degrees, 41% of the respondents hold Master degrees, and 19% of the respondents hold Doctoral degrees.

Table 3. Demographics: education

Age	Percentage
Bachelor (or Diploma)	32
Master	41
PhD	19
None	8

199 participants answered the question of years of experience in digital forensics field, and the results are shown in Table 4 below. 15% of the respondents have 1 to 2 years of experience, 14% of the respondents have 3 to 4 years of experience, and 51% of the respondents have more than 5 years of experience.

Table 4. Demographics: years of experience in digital forensics

Years of experience in digital forensics	Percentage
None	9
Less than 1 year	11
1-2 years	15
3-4 years	14
More than 5 years	51

205 participants answered the question "How familiar are you with digital forensic tools?" and the results are shown in Table 5 below. 76% of them claim to be "very familiar" or "familiar" with digital forensic tools.

Table 5. Demographics: how familiar are you with digital forensic tools?

Level of familiarity	Percentage
Very unfamiliar	5
Unfamiliar	5
Neutral	14
Familiar	31
Very familiar	45

The demographic results of the survey show that the participants are experienced, well educated, and relatively have good knowledge as well as sufficient practical experience in the field of digital forensics.

4. Cloud computing and cloud forensics

4.1. Cloud computing definition

126 participants answered the question on the definition of cloud computing. 83.2% of the respondents agree (59.2%) or strongly agree (24%) with the widely cited NIST definition of cloud computing version 15:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell and Grance 2010)

83.2% of the respondents agree (64.80%) or strongly agree (18.40%) with the Gartner definition of cloud computing:

"Cloud computing is a style of computer where scalable and elastic IT-related capabilities are provided 'as a service' to multiple external customers using Internet technologies." (Gartner 2009)

70.97% of the respondents agree (52.42%) or strongly agree (18.55%) with the statement that has frequently appeared in industry whitepapers "cloud computing is an evolution, not revolution". 68% of the respondents agree (43.20%) or strongly agree (24.80%) with the definition by the Cloud Security Alliance (CSA):

"Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing."(CSA 2009)

62.61% of the respondents agree (42.28%) or strongly agree (20.33%) that "cloud computing is a new way of delivering computing resources, not a new technology." Only 30.64% of the respondents agree or strongly agree with Oracle CEO's famous remark "cloud computing is redefined to include everything we already do" (Farber 2008), while 37.90% of the respondents remain neutral.

Since cloud computing started to emerge as a business and service model, it has been shaping a major disruptive technological transformation towards delivering computing power as a service. It brings a range of significant advantages compare to traditional models of computing such as cost effectiveness, scalability, etc. By being a mixture of several existing technologies and a natural phase of the evolution of computing technology, cloud computing is something new rather than merely a business or marketing concept. The respondents of this question have agreed on cloud computing definitions proposed by several leading organizations, and the NIST definition has gain critical mass. Late 2011, NIST released its final version of definition for cloud computing with minor amendments to the 15th version of definition:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to 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."(Mell and Grance 2011)

Despite that the definition of cloud computing may keep evolving as it matures, in this paper the NIST Final Definition of Cloud Computing (Mell and Grance 2011) is used as a reference.

4.2. Cloud computing as a trend

122 respondents answered the question on cloud computing as a trend. 60% of the respondents agree (54.17%) or strongly agree (5.83%) that cloud computing as a trend is "a part of the evolving process since early years of computing towards using computing power as utility (such as electricity, gas, etc.)". 47.93% of the respondents agree (39.67%) or strongly agree (8.26%) that cloud computing as a trend "reduces cost and compromises security". 39.17% of the respondents agree (34.17%) or strongly agree (5.00%) with the Gartner statement (Gartner, 2009) that cloud computing as a trend is "a movement expanding the role of IT decision making outside the IT organization and redefining the value of IT organization as service enablers", while 41.67% remain neutral. Only 33.06% of the respondents agree (30.58%) or strongly agree (2.48%) that cloud computing as a trend is "a result of the recession for reducing IT cost".

Cloud computing is still a rapidly emerging trend. Gartner projects that revenue for cloud services will approach $152.1 billion in 2014 (Gartner 2010). The concept of cloud computing was born in the 1960s from the ideas of pioneers like J.C.R. Licklider, who was instrumental in the development of ARPANET and envisioned computation in the form of a global network (Bolt et al. 1981) and John McCarthy, who coined the term "artificial intelligence", framed

computation as a public utility. Significant cost reduction is one of the benefits of cloud computing, e.g., U.S. organizations that move to the Cloud could save $12.3 billion in energy costs and equivalent of 200 million barrels of oil, as estimated. (CDP 2011) At the mean time security is still the top concern of cloud adoption (CSA 2011). Some argue that the rapid growth of cloud computing is driven by cost reduction with known risk and sacrifice of security. This popular argument among early-adopters does not seem to be supported by the respondents of this question. As cloud adoption growing worldwide, many start to believe cloud computing is a natural and positive phase of evolution leading to more efficient and enabling computing, and security is the only major issue to be resolved and will be resolved.

4.3. Cloud forensics definition

123 participants answered the question on the definition of cloud forensics. 60.97% of the respondents agree (49.59%) or strongly agree (11.38%) that cloud forensics is "an application of digital forensics in cloud computing". 60.51% of the respondents agree (43.70%) or strongly agree (16.81%) that cloud forensics is "a mixture of traditional computer forensics, small scale digital device forensics, and network forensics". 56.67% of the respondents agree (45.00%) or strongly agree (11.67%) that cloud forensics is "an interdisciplinary area between digital forensics and cloud computing, although both definitions of digital forensics and cloud computing are still under discussion" (Ruan et al. 2011A). 55.46% of the respondents agree or strongly agree that "cloud forensics is network forensics". 49.17% of the respondents agree or strongly agree that "cloud forensics is Internet forensics". 41.52% of the respondents agree or strongly agree that cloud forensics is "a brand new area". Only 25.42% of the respondents agree or strongly agree "cloud forensics is classical computer forensics".

Digital forensic science has been defined at the first Digital Forensic Research Workshop (DFRWS) in 2001 as:

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and preservation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." (DFRWS 2001)

Alternatives and amendments have been proposed, however the DFRWS definition is still widely accepted.

The definition of cloud forensics subjects to the definition of cloud computing. According to the result of this question, the respondents have reached consensus on cloud forensics is an application of digital forensics in cloud computing, and is a mixture of traditional computer forensics, small scale digital device forensics, and network forensics. As cloud computing is usually delivered through network or Internet, a wide range of cloud forensic techniques should overlap network forensic and "Internet forensic" techniques. However as discussed previously, cloud computing is something new by being a mixture of existing technologies and it is still rapidly evolving, thus it is possible that cloud forensics can grow into a new area.

Ruan et al. 2011A also proposed a three-dimensional model to structure the complex domain of cloud forensics. It includes technical dimension, organizational dimension and legal dimension.

Base on analysis above and the later released NIST Cloud Computing Reference Architecture (Liu et al. 2011), the researchers revisited the definition proposed in Ruan et al. 2011A, and hereby propose a working definition of cloud forensics as follows:

Cloud forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.

4.4. Significance of cloud forensics

122 participants answered the question on the significance of cloud forensics. 80.84% of the respondents agree (49.17%) or strongly agree (31.67%) that cloud forensics is "an important component of cloud security". 77.5% of the respondents agree (50.00%) or strongly agree (27.50%) that cloud forensics is "as important as cloud security". 76.67% of the respondents agree (45.00%) or strongly agree (31.67%) that cloud forensics "needs more funding and investment in

R&D than it has got at the moment." 71.08% of the respondents agree (40.50%) or strongly agree (30.58%) that "there will be a general lack of awareness until a major critical incident happens".

The results of this question show that the respondents have reached consensus on the significance of cloud forensics. On the contrary, leading organizations driving cloud security standards (e.g., NIST, Cloud Security Alliance) still largely neglect the importance of integrating forensic capabilities into cloud security in their most recent releases such as Hogan et al. 2011. There is no international body driving collaborative efforts on developing cloud forensic standards and sharing resources that is comparable to the scale and influence of Cloud Security Alliance. Most of the challenges posed by cloud computing as analyzed in Ruan et al. 2011A are still need to be further researched and addressed.

4.5. Impact of cloud computing on digital forensics

101 participants answered the question on the impact of cloud computing on digital forensics. 46% of the respondents agree that "cloud computing makes forensics harder". 37% of the respondents agree that "cloud computing makes forensics easier".

When asked why "cloud computing makes forensics harder", comments from the participants can be concluded into following issues:

- Reduced access to remote and distributed physical infrastructure and storage
- Lack of physical control and physical location of data
- Lack of standard interfaces
- Legal issues including multiple ownership, multiple jurisdictions, and multiple tenancies
- Lack of collaboration from the cloud provider(s)
- Evidence segregation
- Data recovery

When asked why "cloud computing makes forensics easier", comments from the participants can be concluded into the following aspects:

- Cloud investigations can leverage characteristics of cloud computing, e.g., computing power on demand, elasticity, distributed forensic processing, as well as scalable auditing, reporting, logging, imaging and testing. Forensic implementations in the cloud can also be cheaper.
- Cloud investigations will be highly dependent on provider providing digital evidence through centralized administration and management, so there will be less work for the investigator/law enforcement side.
- Evidences in cloud environments are harder to destroy by the criminals as they maybe mirrored to multiple locations
- Investigative functionalities can be integrated in cloud implementations, e.g., hashing and imaging are easier in the Cloud

4.6. Cloud forensics Dimensions

139 participants answered the question on the dimensions of cloud forensics. 80% of the respondents agree that there is a "technical" as well as "legal" dimension for cloud forensics. 69% of the respondents agree that there is an "organizational/administrative dimension" for cloud forensics. 43% of them agree that there is a "social dimension" for cloud forensics. 14% of the respondents clicked "other" dimensions. "Political" and "personal" dimensions are mentioned in the comments.

This question was asked in order to validate the multi-dimensional nature of cloud forensics proposed in Ruan et al. 2011A. The three major dimensions of cloud forensics, i.e., technical, organizational and legal dimension, have reached consensus among the respondents according to the survey results, and they are thus included in the cloud forensics definition proposed in Section 4.3.

4.7. Cloud forensics usage

139 participants answered the question on the uses of cloud forensics. 80% of the respondents agree that cloud forensics can be used for "investigations on digital crimes, civil cases, policy violations, etc.", 51% of the respondents agree that it can be used for "regulatory compliance". 46% of the respondents agree that it can be used for "data and system recovery". 40% of the respondents agree that it can be used for "due diligence". 34% of the respondents agree that it can be used for "log monitoring". 21% of the respondents agree that it can be used for "troubleshooting". Among the 10% "other uses", several respondents added that cloud forensics can also be used to generate security policy feedback.

As cloud forensics is an application of digital forensics in cloud computing as discussed previously, its usage consequently should be similar to the usage of digital forensics in general. When applied in cloud computing environments, the spilt of control among cloud actors has made forensics a shared

responsibility which adds to the organizational complexity of cloud forensics. Based on the results of this question, the researchers propose the following categories for the usage of cloud forensics:

- External investigation
  - Criminal case
  - Civil case
- Internal investigation
  - Security incidents
  - Policy violations
  - Regulatory compliance
  - Event management: to investigate and understand the when, where, how, why, who of any event happened in the cloud environment

An external investigation is an investigation initiated by an external party to the cloud environment shared among cloud actors, e.g. law enforcement, for investigating criminal or civil case.

An internal investigation is an investigation initiated internally by one or more cloud actor(s) sharing the cloud computing environment, for the purpose of investigating security incident or policy violation, or auditing the regulatory compliance, or managing events (i.e., understanding the when, where, how, why and who of any event that happened or is happening) in the cloud environment.

5. Cloud forensics techniques and research

5.1. Challenges

106 participants answered the question on the challenges for cloud forensics. Only 2 out of the 17 listed challenges have less than 50% of the respondents agreed on being significant or very significant. These 2 challenges are "Single points of failure" (27.88% significant, 10.58% very significant) and "Ineffective encryption key management makes it easier to lose the ability to decrypt forensic data stored in the Cloud" (38.10% significant, 9.52% very significant). The researchers can thus conclude that cloud computing does pose significant challenges to digital investigations at current stage, and the top 5 challenges for cloud forensics are:

(1) Jurisdiction (89.43% significant or very significant, 59.62% very significant)

(2) Lack of international collaboration and legislative mechanism in cross-nation data access and exchange (84.77% significant or very significant)

(3) Investigating external chain of dependencies of the cloud provider (e.g., a cloud provider can use the service from another provider) (80.96% significant or very significant)

(4) Decreased access to and control over forensic data at all levels from customer side (78.3% significant or very significant)

(5) Lack of law/regulation and law advisory (76.19% significant or very significant)

Simple role management (e.g. admin, user) makes it difficult to categorize suspects (51.43% significant or very significant)

The rest of the listed challenges and are as follows

- Segregation of forensic data in an infrastructure shared by multiple users (multitenant environment) (72.11% significant or very significant)
- Exponential increase of digital (mobile) devices accessing the cloud (76.19% significant or very significant)
- Lack of forensic expertise (75.24% significant or very significant)
- Lack of legislative mechanism facilitating evidence retrieval involving confidential data (75.24% significant or very significant)
- Missing terms and conditions in SLA (Service Level Agreement) regarding investigations (72.38% significant or very significant)
- Limited investigatory power given to the investigators or consulting firms to legally obtain data under respective jurisdictions in civil cases (69.23% significant or very significant)
- Different providers have different approaches to cloud computing (66.66% significant or very significant)
- Synchronization of timestamps (59.61% significant or very significant)
- Unification of log formats (57.14% significant or very significant)

5.2. Opportunities

Compared to the challenges, more respondents chose to remain neutral towards the opportunities of cloud forensics. 105 participants answered this question. 59.62% of the respondents agree or strongly agree that "establishment of a foundation of standards and policies for forensics that will evolve together with the technology" is an opportunity for cloud forensics. 55.34% of the respondents agree or strongly agree that "forensics-as-a-service" is an opportunity for cloud forensics. 54.81% of the respondents agree or strongly agree that "dedicated forensic implementations are more cost-effective when applied on a larger scale and offered as part of

the cloud infrastructure" is an opportunity for cloud forensics. Researchers thus believe standardization groups, industrial leaders and policy makers should take forensic standards, forensic-as-a-service and integrated forensic implementations into considerations as key opportunities while cloud computing keep evolving as an emerging technology.

62.5% of the respondents disagree, strongly disagree or remain neutral towards "there are more chances to find critical evidence left in the Cloud due to data abundance". 53.84% of the respondents disagree, strongly disagree or remain neutral towards "default technologies provided in the Cloud such as automatic MD5 checksums can improve the overall robustness of forensics in the Cloud". 52.89% disagree, strongly disagree or remain neutral towards "the scalability and flexibility of the Cloud enables elastic and unlimited storage of logs and increases efficiency of indexing, searching and various queries of logs, etc.".

5.3. Valuable research directions

106 participants answered this question. The respondents consider all of the listed research directions important or very important, which is in alignment with the significant challenges faced by cloud forensics as analyzed previously. 86.67% of the respondents agree that "designing forensic architecture for the cloud" is important or very important. 83.02% of the respondents agree that research and development on "law" is important or very important (45.28%). 82.86% of the respondents agree "extending current investigative tools into the Cloud" and "policies and mechanisms" are important or very important. 80.95% of the respondents agree "international collaboration" is important or very important (44.76%). 63.81% of the respondents think that research and developments on "novel approaches" are important or very important.

6. Critical criteria for cloud forensic capability

6.1. Parties to be assessed for cloud forensic capability

111 participants answered the question on who should be assessed for cloud forensic capability. 78% of the respondents think the Cloud Service Provider[1] should be assessed. 53% of the respondents think the cloud customer[2] should be assessed. 38% of the respondents think the Internet service provider should be assessed. 36% of the respondents think the cloud end user should be assessed. Other comments include that the investigators and law enforcement need to be assessed.

According to the NIST cloud computing reference architecture released after the survey, there are five major actors in the cloud architecture, i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, and cloud auditor. In the shared cloud computing environment, the investigation of any security incident or criminal activities has become a shared responsibility among cloud actors, especially cloud provider and cloud consumer, thus there is a need to access the forensic capability for all actors involved in a cloud environment. Considering the survey results, the researchers suggest the following list of parties to be assessed for cloud forensic capability:

- Cloud provider
- Cloud consumer
- Cloud carrier
- Cloud broker
- Cloud auditor
- Law enforcement
- Forensic professionals

6.2. Procedures and toolkits

101 participants answered this question. Similar to the challenges for cloud forensics, all of the listed procedures and toolkits have gained more than 50% of agreement from the respondents on their importance. It shows an urgent need and demand in cloud forensic research and development. The list of procedures and toolkits is listed as follows

(1) 90.09% of the respondents agree that "a procedure and a set of toolkits to preserve the soundness of digital evidence in the Cloud" is important or very important (46.53%).
(2) 88% of the respondents agree that "a procedure and a set of toolkits to retrieve forensic data that contains confidential data under jurisdiction(s) and agreement(s) under which services operate" is important or very important.

[1] The term Cloud Service Provider was used in the survey, and the term cloud provider is used in this paper to be in line with the NIST definitions.

2 The term Cloud Consumer was used in the survey, and the term cloud consumer is used in the paper to be in line with the NIST definitions.

(3) 86% of the respondents agree that "a procedure and a set of toolkits in the cloud organization to obtain keys for encrypted data in the Cloud" is important or very important.
(4) 85.15% of the respondents agree that "a set of toolkits to investigate external chain of dependencies (a cloud provider using services from another cloud provider)" is important or very important (41%).
(5) 83.16% of the respondents agree that "a procedure and a set of toolkits to collect forensic data from various data sources in the Cloud with appropriate order with consideration of their reliability" and "a procedure and a set of toolkits to preserve volatile data in the Cloud" is important or very important (41.58%), respectively.
(6) 81% of the respondents agree that "A procedure and a set of toolkits to proactively collect forensic-relevant data in the Cloud" is important or very important.
(7) 78% of the respondents agree that "A procedure and a set of toolkits to study and analyze forensic data collected from the Cloud following methodical approaches " is important or very important.
(8) 77% of the respondents agree that "A procedure and a set of toolkits to record and maintain the chain of custody in an investigation" is important or very important (41%).
(9) 77% of the respondents agree that "A procedure and a set of toolkits to correlate forensic data collected with unsynchronized timestamps and different log formats" is important or very important.
(10) 75.24% of the respondents agree that "A procedure and a set of toolkits to perform large-scale live forensics in the Cloud" is important or very important.
(11) 70.29% of the respondents agree that "A procedure and a set of toolkits to identify the range of possible data sources in the Cloud" is important or very important.
(12) 59.4% of the respondents agree that "A procedure and a set of toolkits to generate forensic reports in a consistent and standard fashion" is important or very important.

6.3. Staffing

102 participants answered the question on staffing importance and they have reached majority consensus as for cloud forensic staffing. 84.16% of the respondents agree that to have "a team of forensic staff in the cloud organization or externally assisting the cloud organization on forensic investigations in the Cloud" is important or very important. 83.16% of the respondents agree that to have "forensic staff in the cloud organization provided with up-to-date training on cloud forensic knowledge" is important or very important. 75.24% of the respondents agree that to have "legal experts in the cloud organization or externally assisting the cloud organization on multi-jurisdiction/multi-tenant issues regarding forensic investigation" is important or very important.

6.4. Policies

102 participants answered the question on policy importance, and they have also reached majority consensus. 84.84% of the respondents agree that to have "a policy in the cloud organization to ensure all forensic procedures are performed in a standard fashion" is important or very important, and 84% of the respondents agree that "a policy in the cloud organization to reinforce proactive collection of forensic-relevant data in the Cloud" is important or very important as for forensic policies within the cloud organization.

6.5. Agreements

100 participants answered the question on agreement importance. A mass majority of 87.76% of the respondents agrees "an agreement on the recording of the chain of custody among all parties in an investigation" is important or very important. 81.82% of the respondents agree that "tools provided, techniques supported, access granted regarding forensic investigation should be included in the SLA (Service Level Agreement)" is important or very important. 76 % of the respondents agree "an agreement on the division of responsibilities among all parties involved (cloud organizations, law enforcement, etc.) in cases of investigation" is important or very important. And 72.72% of the respondents think that "an agreement on the access and control over forensic data at all levels between cloud organizations" is important or very important. A list of key terms to be included in the SLA between cloud provider and cloud consumer is suggested in Ruan et al. (2012)

6.6. Guidelines

Lastly, 103 participants who answered the question on guideline importance have reached majority consensus. 83.33% of the respondents agree that "a guideline on external collaboration between the cloud organization and other cloud organization(s), law enforcement, etc. in cases of investigation" is important or very important. 80.2% of the respondents agree that "a guideline on internal collaboration between various functional teams in cases of investigation in the cloud organization" is important or very important. 70.87% of the respondents agree that "a guideline on forensic reporting to ensure reporting follows consistent and standard format" is important or very important.

7. Limitations

This survey was circulated when cloud computing was still rapidly emerging as a concept, and before the NIST Final Definition of Cloud Computing (Mell and Grance 2011) and the NIST Cloud Computing Reference Architecture (Liu et al. 2011) were released, thus some of the terms and questions are not relevant anymore. Half of the respondents did not finish the survey, and it could be due to the fact that the survey questions were designed too long.

8. Conclusion

In this paper, the results of a widely circulated survey on fundamental issues in the emerging area of cloud forensic are presented and analyzed. Compare to 1st preliminary analysis in Ruan et al. 2011B, most of the results show consistency. A working definition of cloud forensics is proposed. Areas of critical importance for research and development are identified and agreed among respondents of the survey. Cloud forensics poses various challenges to digital forensics. There is an urgent need in the establishment of cloud forensic capabilities including a set of toolkits and procedures for cloud investigations. However, cloud forensics also brings opportunities especially in terms of standard acceleration, which should not be neglected.

9. Future work

The working definition of cloud forensics need to be further refined and validated. A list of cloud forensic capabilities need to be developed based on some of the survey results as well as the NIST Cloud Computing Reference Architecture (Liu et al. 2011).

References

Hogan, M., Liu, F., Sokol, A., Tong, J. (2011) 'NIST Cloud Computing Standards Roadmap' National Institute of Standards and Technology, Special Publication 500-291

Bolt, Beranek, Newman (1981) A History of the ARPANET: The First Decade. Defense Advanced Research Projects Agency

Carbon Disclosure Project [CDP] 2011, 'Cloud Computing – the IT Solution for the 21st Century', Carbon Disclosure Project Study 2011

Cloud Security Alliance [CSA] (2009), Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, San Francisco, California

Cloud Security Alliance [CSA] (2011), Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, San Francisco, California

DFRWS (2001). 'DFRWS Technical Report: A Road Map for Digital Forensic Research' Digital Forensic Research Workshop. G. Palmer. Utica, New York.

Farber, D. (2008) Oracle's Ellison nails cloud computing. CNET September 26

Gartner (2009) Gartner Highlights Five Attributes of Cloud Computing. Gartner Press Releases June 23

Gartner (2010) Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency

Kleynhans, S. (2012) 'The new PC era: the Personal Cloud', Gartner

Mell, P., Grance, T. (2010) 'The NIST Definition of Cloud Computing Version 15' National Institute of Standards and Technology

Mell, P., Grance, T. (2011) 'The NIST Definition of Cloud Computing' National Institute of Standards and Technology, Special Publication 800-145

Ruan, K., Carthy, J.,Kechadi, T., Crosbie, M. (2011A) 'Cloud forensics: An overview' Advances in Digital Forensics VII

Ruan, K., Baggili, I., Carthy, J., Kechadi, T. (2011B) 'Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis', The Journal of Digital Forensics, Security and Law

Ruan, K., James, J.I.,Carthy, J., Kechadi, T., (2012) 'Cloud forensics: key terms for the Service Level Agreement' Advances in Digital Forensics VIII