May 27th, 10:45 AM

Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis

Keyun Ruan
University College Dublin, keyun.ruan@ucd.ie

Ibrahim Baggili
Zayed University, ibrahim.baggili@zu.ac.ae

Joe Carthy
University College Dublin, joe.carthy@ucd.ie

Tahar Kechadi
University College Dublin, tahar.kechadi@ucd.ie

SURVEY ON CLOUD FORENSICS AND CRITICAL CRITERIA FOR CLOUD FORENSIC CAPABILITY: A PRELIMINARY ANALYSIS

Keyun Ruan
University College Dublin
keyun.ruan@ucd.ie

Ibrahim Baggili (PhD)
Zayed University
ibrahim.baggili@zu.ac.ae

Prof Joe Carthy
University College Dublin
joe.carthy@ucd.ie

Prof Tahar Kechadi
University College Dublin
tahar.kechadi@ucd.ie

ABSTRACT

In this paper we present the current results and analysis of the survey "Cloud forensics and critical criteria for cloud forensic capability" carried out towards digital forensic experts and practitioners. This survey was created in order to gain a better understanding on some of the key questions of the new field - cloud forensics - before further research and development. We aim to understand concepts such as its definition, the most challenging issues, most valuable research directions, and the critical criteria for cloud forensic capability.

Keywords: Cloud Forensics, Cloud Computing, Digital Forensics, Survey, Cloud Forensic Capability

1. INTRODUCTION

Cloud computing has the potential to become one of the most transformative developments in the history of computing, following the footsteps of mainframes, minicomputers, PCs (Personal Computers), smart phones, and so on (Perry et al.,2009). It is radically changing how information technology services are created, delivered, accessed and managed.

Gartner estimates by 2015, 20% of non-IT Global 500 companies will be cloud service providers (Gartner, 2010). However, the rapid growth and adoption of cloud computing as a non-standard system (Beebe, 2009), is bringing digital forensics deeper into the crisis it is facing (Garfinkel, 2010). Encryption, proliferation of endpoints, multi-jurisdiction, loss of data control, to name a few, are all challenges exacerbated in cloud environments for forensic investigations due to a general lack of tools and expertise. Cloud organizations, including CSPs (Cloud Service Provider) and cloud customers, have to establish a cloud forensic capability, otherwise, they will face tremendous difficulties in carrying out investigations on critical incidents in a cloud architecture such as criminal intrusions and major policy violations in order to restore operations, data and services. They will also face difficulties when collaborating with law enforcement in cases of resource confiscation, etc., due to lack of forensic knowledge and preparation.

Ruan et al. (2011) first gave an overview of cloud forensics, introduced the cloud forensics three-dimensional model, and analyzed some of the major challenges and opportunities of cloud forensics. In order to validate the key areas covered in Ruan et al. (2011) and to study the critical criteria for cloud forensic capability, the researchers carried out this survey towards digital forensic experts and practitioners around the world on some key questions of cloud forensics, such as the definition of cloud forensics, the most significant challenges and opportunities of cloud forensics, the most valuable research direction for cloud forensics, etc. The survey was opened on 13th Feb 2011 and was widely circulated.

2. LIMITATIONS

Until 23rd Mar 2011, the survey has received 156 responses. The major limitation of the survey is the limited sample size. Only a limited number of experts (around 80) who responded to the survey have completed all the questions. According to the feedback, the reason for this can be the fact that cloud forensics is relatively a new topic. However, it is the first and only survey carried out towards the digital forensics community that is explicitly focused on cloud forensics, thus the researchers decided to share a preliminary analysis of the current survey results in this paper.

3. METHODOLOGY

In this research digital forensics experts and practitioners are surveyed on the definitions of cloud computing and cloud forensics, cloud forensics research and techniques, and critical criteria for cloud forensic capability.

The survey is hosted by Zayed University, United Arab Emirates (UAE). All participants are required to agree to a consent form, which contains key terms on the voluntary nature of participation and confidentiality of the survey results, before starting filling out the survey. Demographic data of 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 Forensics Research and Techniques
- Part III Critical Criteria for Forensic Capability

In "Part I Background", the researchers designed the following questions:

(1) What is cloud computing: as cloud computing is becoming mainstream, it still remains a confusing and evolving term in the industry. All the studies and research around cloud computing have to be based on a consensus on its definition. In this question, participants are presented with several definitions from respected organizations, such as NIST, Gartner, Oracle, Cloud Security Alliance (CSA) without the names of these organizations shown in the survey, as well as several popular views on the definition of cloud computing.

(2) Cloud computing as a trend: cloud computing has attracted massive investment and is seeing rapid adoption in both businesses and governments worldwide (INPUT, 2009). Gartner (2009A) forecasted that the worldwide cloud service market is expected to reach $150.1 billion in 2013. According Merrill Lynch (2008), the volume of the cloud computing market opportunity will amount to $160 billion by 2011. According to an October 2008 forecast by IDC (International Data Corporation)(Gens, 2008), spending on cloud services is growing at five times the rate of traditional on-premises IT. What is the underlying reason for cloud computing as a trend? Is it because of the top advantage of cloud computing, i.e., cost-effectiveness? (CSA, 2009), or it is a new phase of the evolution of computing since the 1960s

towards utility computing (Buyya et al., 2008)? By understanding better what is cloud computing as a trend, cloud forensics can be better placed in the big picture.

(3) What is cloud forensics: cloud forensics is a new area, a new way to call old techniques, or a mixture of both? By asking this question, the researchers aim to get opinions from the industry experts on the how to define cloud forensics.

(4) How significant is cloud forensics: is cloud forensics a component of cloud security, or an independent segment in parallel to cloud security with the same importance? This question is designed in order to understand the significance of cloud forensics in the cloud architecture.

(5) What is the impact of cloud computing on forensics: some say cloud computing makes forensics harder (Sawyer, 2009), while others say cloud computing makes forensics easier (Morrill, 2008). The researchers want to survey the digital forensic experts on their opinions on the impact of cloud computing on forensics: whether it is making forensic harder or easier, or both?

(6) What are the dimensions of cloud forensics: the emerging cloud computing, with its worldwide availability and resource sharing environments, has introduced much complexity into digital forensics, which is traditionally a technical discipline. The legal concerns have been further strengthened due to the default multi-jurisdiction setting. The organizational paradigm has become much more complex, when collaborations on all levels are needed among CSPs, cloud customers and law enforcement, compare to a single organization coping with its own on-premise networks, thus cloud forensics is a multi-dimensional discipline. Ruan et al. (2011) defined the three-dimensional model for cloud forensics, i.e., technical dimension, organizational dimension and legal dimension. In this question, the researchers aim to validate the three-dimension model from the opinions from the experts.

(7) What are the uses of cloud forensics: this question is important in order to attract more funding and investment on cloud forensic research and development. It is crucial to make both CSP and cloud customer understand the various uses of cloud forensics and how it can benefit their service availability and overall robustness of operations.

In "Part II Cloud Forensics Research and Techniques", the researchers designed the following questions:

(1) What are the challenges of cloud forensics: this question is valuable for understanding what are the most challenging issues regarding cloud forensics.

(2) What are the opportunities of cloud forensics: this question is valuable for understanding what are the biggest opportunities for cloud forensics.

(3) Valuable research directions of cloud forensics: this question is valuable for designing a research agenda for cloud forensics so that researchers and developers can focus on the most valuable research directions.

(4) What are the parties involved in a cloud investigation: this question is valuable for reaching a consensus on who should be involved in a cloud investigation.

In "Part III Critical Criteria for Forensics Capability", the researchers designed the following questions:

(1) Who should be assessed for the cloud forensic capability: this question is valuable for reaching a consensus on who should be assessed for cloud forensic capability.

(2) Importance of procedures and toolkits: in the technical dimension of cloud forensics (Ruan et al., 2011), a set of tools and procedures need to be developed to address the need for forensic investigations in the Cloud. From this question we can understand what are the most important tools and procedures and direct efforts to developing them.

(3) Staffing importance: this question is valuable for researching a consensus on the staffing structure in the organizational dimension (Ruan et al., 2011) of cloud forensics.

(4) Policy importance: this question is valuable for understanding what policies are more important than the others within cloud organizations to facilitate cloud forensic investigations.
(5) Agreement importance: this question is valuable for understanding what legal agreements are more important than the others among all parties involved in cloud forensic investigations.
(6) Guideline importance: this question is valuable for understanding what guidelines are most needed internally or externally for cloud organizations in the organizational dimension of cloud forensics.

4. RESULTS

4.1 Demographics

133 respondents answered the question of age. 36% of them are above 40, 34% between 31 and 40, 17% between 25 and 30, 5% between 19 and 24. 121 respondents answered the question of gender. 83% of them are male, 17% female. 126 respondents answered the question of education. 44% of them have obtained a master degree, 23% have obtained a PhD, and 28% have obtained a bachelor degree or a diploma. 124 respondents answered the question "years of experience in computer forensics field". 46% of them have more than 5 years experience in computer forensic field, 16% have 3 to 4 years experience, and 17% have 1-2 year experience. 127 respondents answered the question "how familiar are you with digital forensic tools". 76% of them are "very familiar" or "familiar" with digital forensic tools. According to the demographics results, the researchers believe that the respondents of the survey have good knowledge and sufficient experience in digital forensics.

4.2 Cloud Computing and Cloud Forensics

4.2.1 Definition of cloud computing

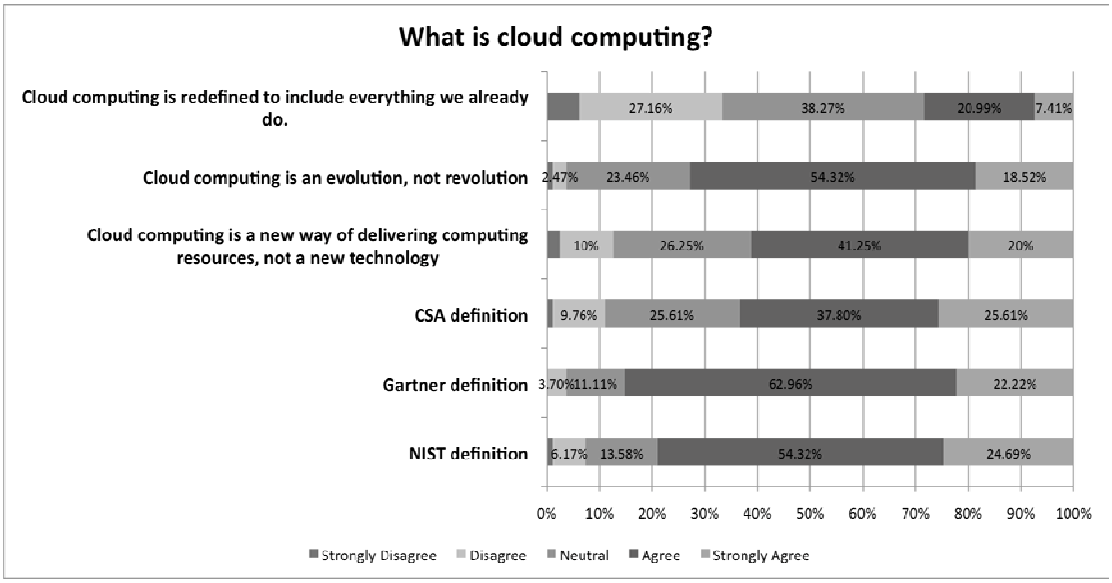

Fig 1. What is cloud computing?

On the definition of cloud computing, 82 respondents answered the question. As shown in Fig 1 above, 85.18% of them agree or strongly agree with the definition from Gartner (2009B):

> *"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".*

79.01% of them agree or strongly agree with the 15th version of NIST definition of cloud computing (Mell and Grance, 2009):

> *"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".*

63.41% of them agree or strongly agree with the definition from Cloud Security Alliance (CSA, 2010):

> *"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"*

72.84% of them agree or strongly agree that "cloud computing is an evolution, not revolution." 61.25% of them agree or strongly agree that "cloud computing is a new way of delivering computing resources, not a new technology". Only 28.4% of them agree or strongly agree with Oracle's CEO's famous remark "cloud computing is redefined to include everything we already do" (Farber, 2008), while 38.27% remain neutral.

4.2.2 Cloud computing as a trend

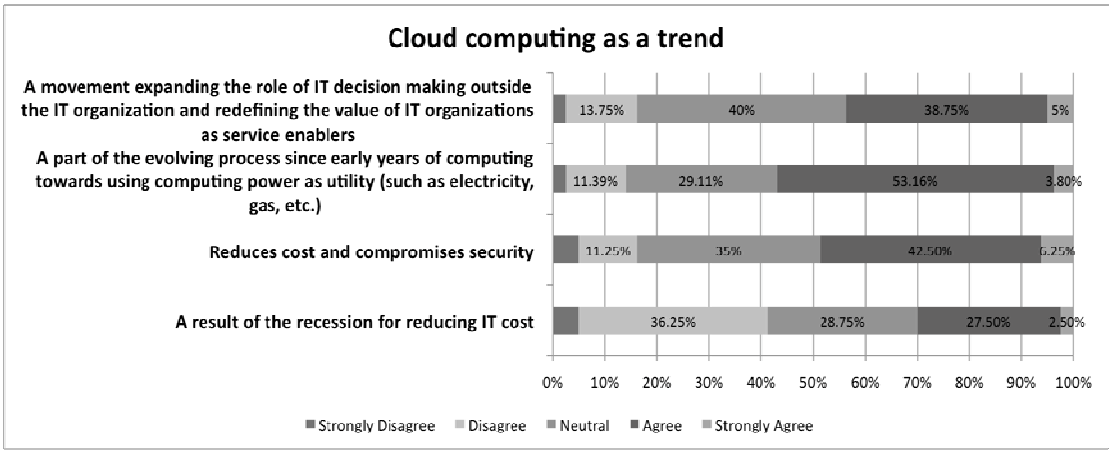

Fig 2. Cloud computing as a trend

82 respondents answered the question "cloud computing as a trend". As shown in Fig 2 above, 56.96% of them agree or strongly agree 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.)". 48.75% of them agree or strongly agree that cloud computing as a trend "reduces cost and compromises security". 43.75% agree or strongly agree with the Gartner statement (Gartner, 2010) 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 40% remain neutral. Only 30% agree or strongly agree that cloud computing as a trend is "a result of the recession for reducing IT cost".

4.2.3 Definition of cloud forensics

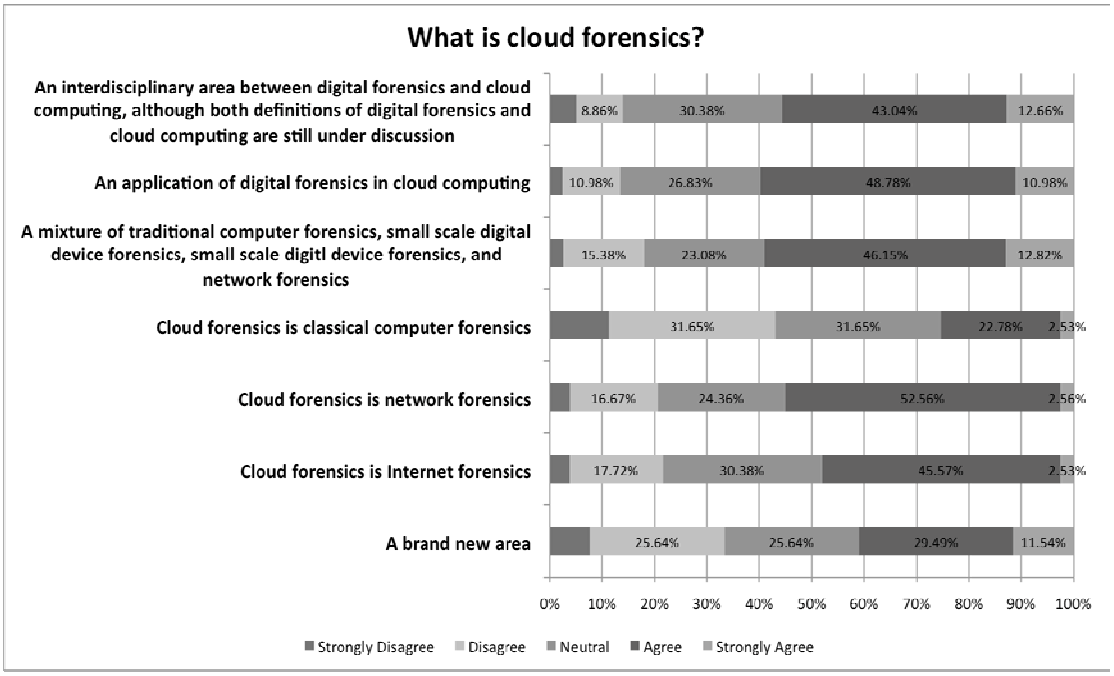

Fig 3. What is cloud forensics?

82 respondents answered the question “what is cloud forensics”. 59.76% of them agree or strongly agree that cloud forensics is “an application of digital forensics in cloud computing”. 58.97% agree or strongly agree that cloud forensics is “a mixture of traditional computer forensics, small scale digital device forensics, and network forensics". 55.7% agree or strongly agree 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., 2011). 55.12% agree or strongly agree that “cloud forensics is network forensics”. 48.1% agree or strongly agree that“cloud forensics is Internet forensics”. 41.03% agree or strongly agree that cloud forensics is “a brand new area”. 25.31% agree or strongly agree that “cloud forensics is classical computer forensics”.

4.2.4 Significance of cloud forensics

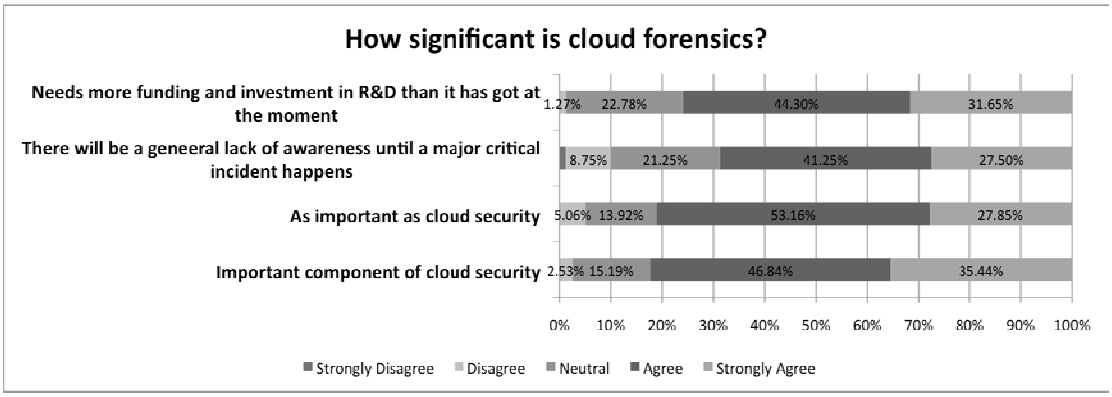

Fig 4. How significant is cloud forensics?

82 respondents answered the question on the significance of cloud forensics. 82.28% of them agree or strongly agree that cloud forensics is "an important component of cloud security". 81.01% agree or strongly agree that cloud forensics is "as important as cloud security". 75.95% agree or strongly agree that cloud forensics "needs more funding and investment in R&D than it has got at the moment." 68.75% agree or strongly agree "there will be a general lack of awareness until a major critical incident happens".

4.2.5 Impact of cloud computing on digital forensics

81 respondents answered the question on the impact of cloud computing on forensics, 50% of them agree that "cloud computing makes forensics harder", while 42% agree that "cloud computing makes forensics easier".

When asked why "cloud computing makes forensic harder", comments from the participants are heavily focused on following issues:

- Loss of data control
- No access to physical infrastructure
- Legal issues of multi-jurisdiction, multi-tenancy and multiple ownership
- Lack of tools for large-scale distributed and virtualized systems

Other issues mentioned in the comments are

- No standard interfaces
- Data ownership
- No provider cooperation
- Difficulties in producing forensically sound and admissible evidence in court

When asked why "cloud computing makes forensics easier", comments from the participants mentioned the following aspects

- More computing resources and processing power can be used for forensic investigation
- Cloud resources and computing power can be used for forensic research and development
- Rapidly scalable auditing, reporting, and testing analysis can be used for larger datasets and distributed applications
- Forensic implementations and activities can be centrally administered and managed
- Investigations can be provided as a service by the CSP
- Running forensic applications in the cloud may reduces cost

4.2.6 Dimensions of cloud forensics

88 respondents answered the question on the dimensions of cloud forensics, 84% of them agree there is a technical dimension for cloud forensics, 84% agree there is a legal dimension for cloud forensics, 75% agree there is an organizational/administrative dimension for cloud forensics, 42% agree there is a social dimension, and one respondent also added the 'political' dimension.

4.2.7 Uses of cloud forensics

88 respondents answered the question on the uses of cloud forensics, 83% of them agree that cloud forensics can be used for "investigations on digital crimes, civil cases, policy violations, etc.", 51% agree that it can be used for "regulatory compliance", 43% agree that it can be used for "due diligence", 43% agree that it can be used for "data and system recovery", 36% agree that it can be used for "log monitoring", 26% agree that it can be used for "troubleshooting", comments were made to add

"security policy feedback" and "presentation of legal matters in legal venues" to the uses of cloud forensics.

4.3 Cloud Forensics Research Techniques

4.3.1 Challenges for cloud forensics

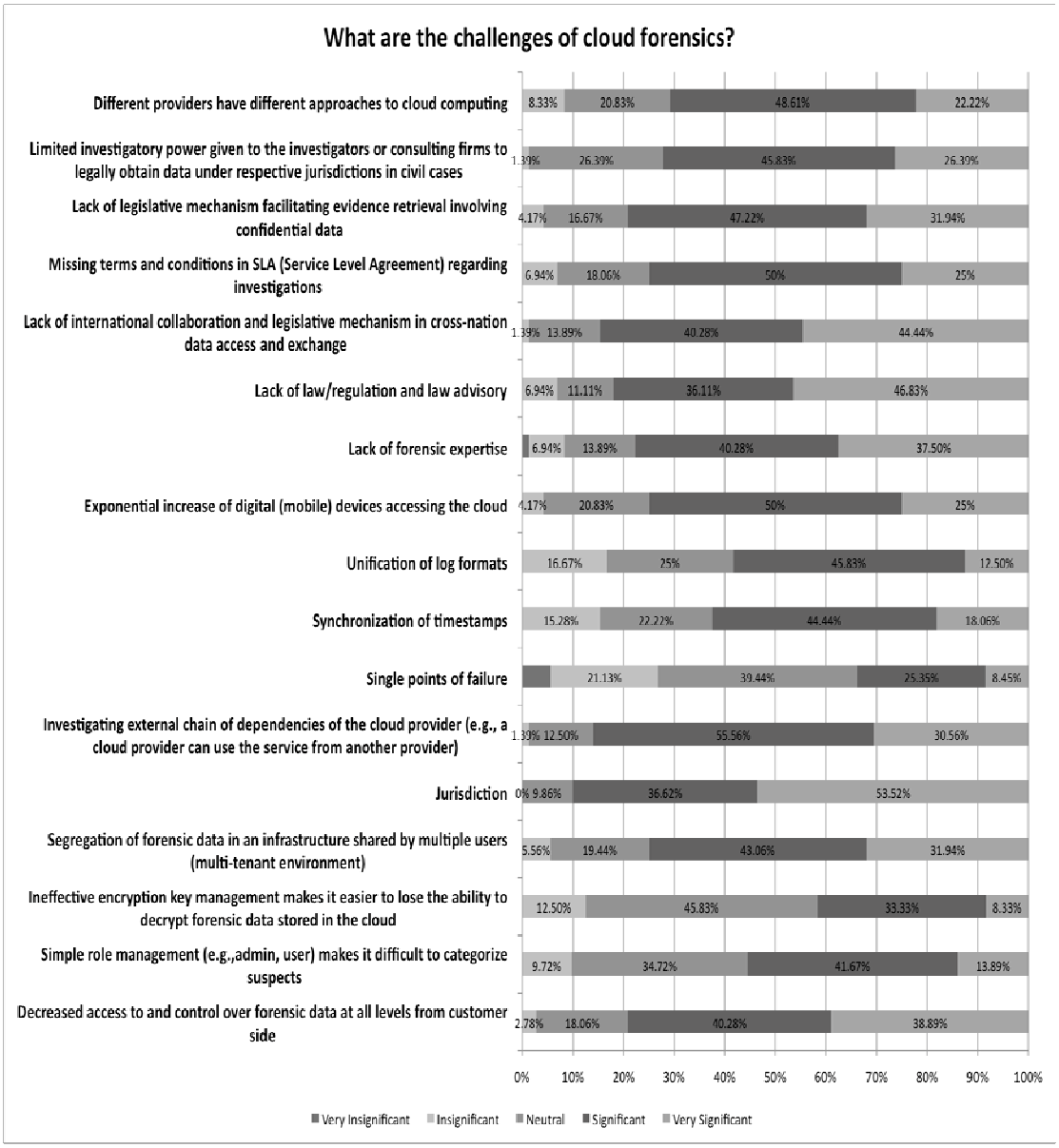

Fig 5. What are the challenges for cloud forensics?

72 respondents answer the question on the challenges for cloud forensics. As we can see from the survey results in Figure 5 above, the top 5 challenges for cloud forensics are:

(1) Jurisdiction (90.14% agree or strongly agree, 53.52% strongly agree)
(2) Investigating external chain of dependencies of the cloud provider (e.g., a cloud provider can use the service from another provider) (86.12% agree or strongly agree)

(3) Lack of international collaboration and legislative mechanism in cross-nation data access and exchange (84.72% agree or strongly agree)
(4) Lack of law/regulation and law advisory (82.94% agree or strongly agree)
(5) Decreased access to and control over forensic data at all levels from customer side (79.17% agree or strongly agree)

4.3.2 Opportunities for cloud forensics

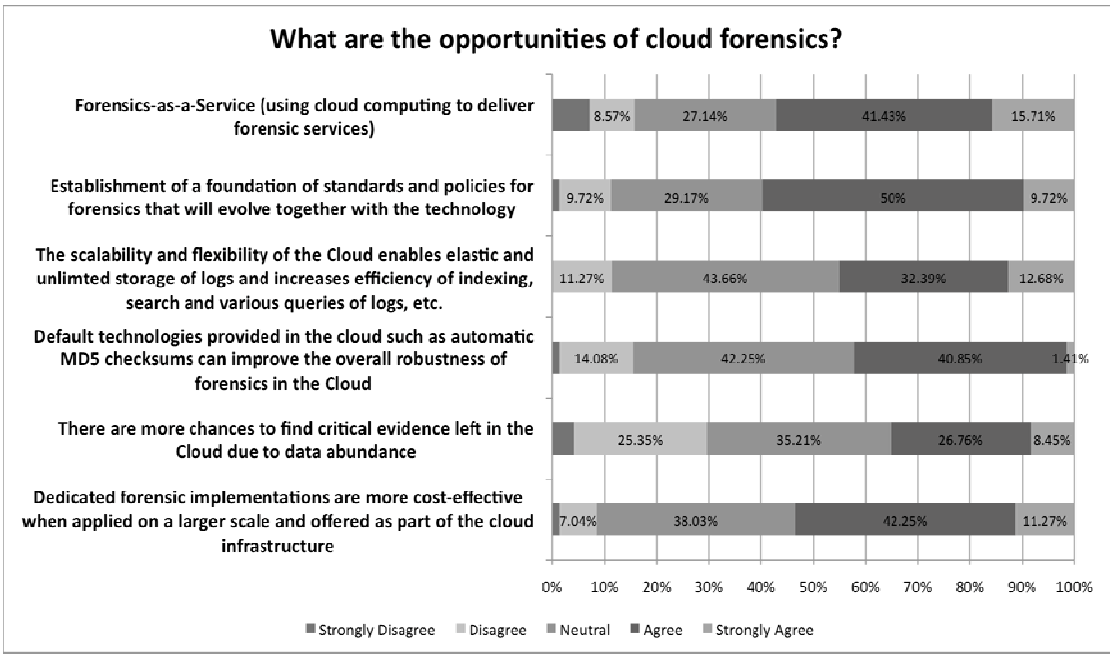

Fig 6. What are the opportunities of cloud forensics?

Compared to the challenges, more respondents chose to remain neutral towards the opportunities of cloud forensics. 72 respondents answered this question. As shown in Fig 6 above, 64.79% of them disagree, strongly disagree or remain neutral towards "there are more chances to find critical evidence left in the Cloud due to data abundance". 57.74% 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". 54.93% 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.". However, 59.72% and 57.14% of them agree or strongly agree that the "establishment of a foundation of standards and policies for forensics that will evolve together with the technology" and "Forensics-as-a-Service (using cloud computing to deliver forensic services)" are opportunities for cloud forensics.

4.3.3 Valuable research directions for cloud forensics

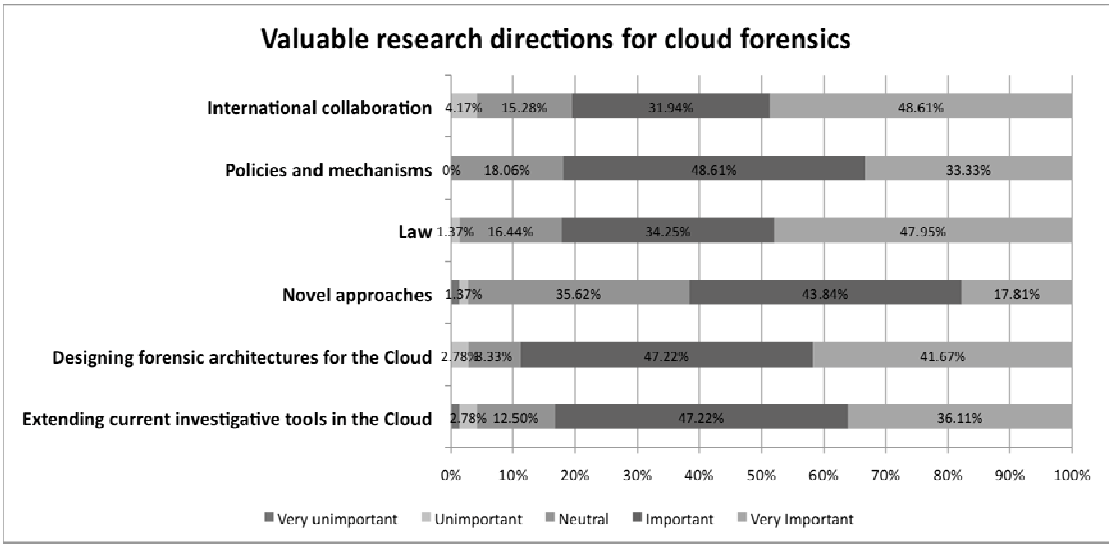

Fig 7. Valuable research directions for cloud forensics

As we can see from the survey results shown in Fig 7 above, the top 3 most important research directions are

(1) Designing forensic architectures for the Cloud (88.57% agree it is important or very important)
(2) Extending current investigative tools into the Cloud (82.86% agree it is important or very important)
(3) Law (82.2% agree or strongly agree, 47.95% strongly agree).

73 respondents answered this question.

4.4 Critical Criteria for Forensic Capability

4.4.1 Parties to be assessed for cloud forensic capability

74 respondents answered the question on who should be assessed for cloud forensic capability. 78% of them think the CSP should be assessed. 54% of them think the cloud customer should be assessed. 38% of them think the Internet service provider should be assessed. 32% of them think the cloud end user should be assessed. Several comments were made to add that the investigators also need to be assessed.

4.4.2 Importance of procedure and toolkits

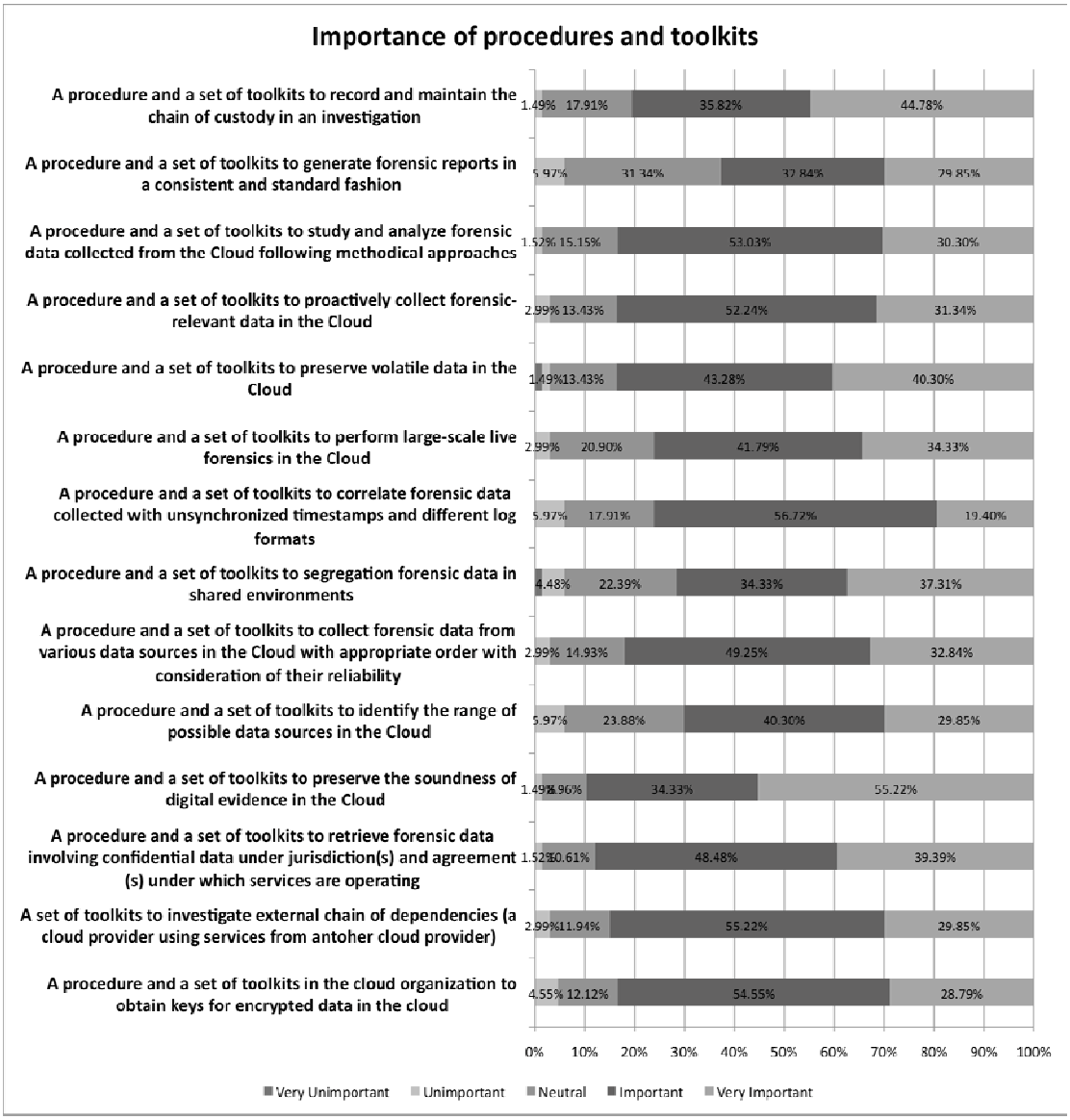

Fig 8. Importance of procedures and toolkits

Despite the close results, according to the survey results shown in Fig 8 above, the most needed tools and procedures for cloud forensics are:

(1) A procedure and a set of toolkits to preserve the soundness of digital evidence in the Cloud (89.55% think it is important or very important, 55.22% think it is very important)
(2) A procedure and a set of toolkits to retrieve forensic data involving confidential data under jurisdiction(s) and agreement(s) under which services are operating (87.87% think it is important or very important)
(3) A set of toolkits to investigate external chain of dependencies (a cloud provider using services from another cloud provider) (85.07% think it is important or very important)
(4) A procedure and a set of toolkits to preserve volatile data in the Cloud (83.58% think it is important or very important, 40.30% think it is very important)

(5) A procedure and a set of toolkits to proactively collect forensic data in the Cloud (83.58% think it is important or very important, 31.34% think it is very important)

67 respondents answered this question.

4.4.3 Staff importance

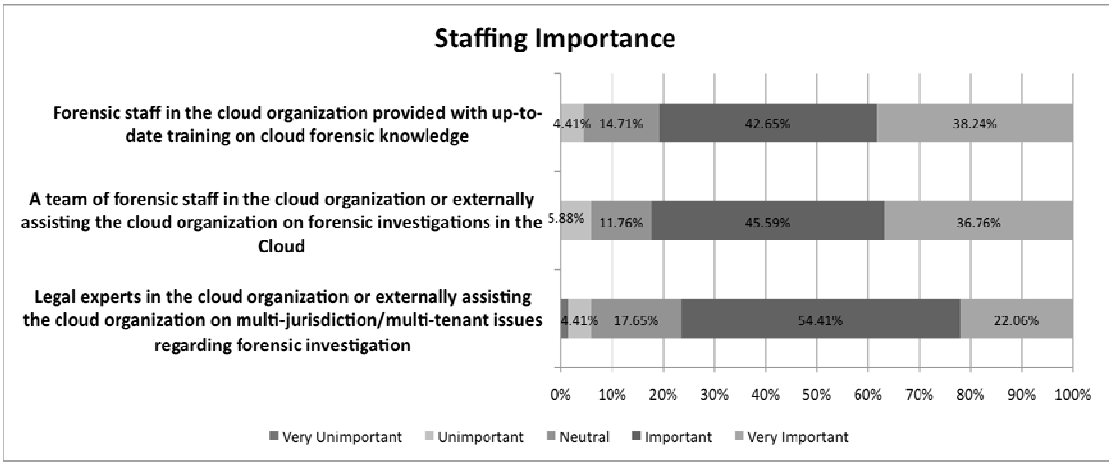

Fig 9. Staffing importance

69 respondents answered the question on staffing importance and they have reached majority consensus as for cloud forensic staffing, as shown from the results in Fig 9 above. 82.35% of them 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. 80.89% 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. 76.47% 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.

4.4.4 Policy importance

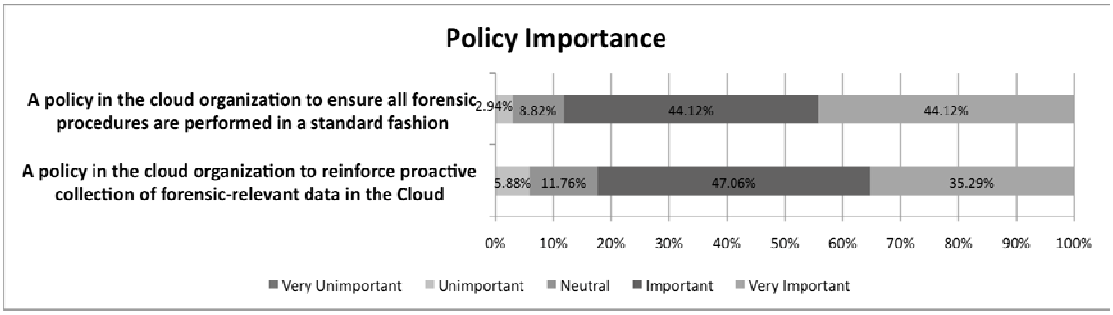

Fig 10. Policy importance

69 respondents answered the question on policy importance, and they have also reached majority consensus, as shown in the survey results in Fig 10 above, 88.34% of them 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 82.35% 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.

4.4.5 Agreement importance

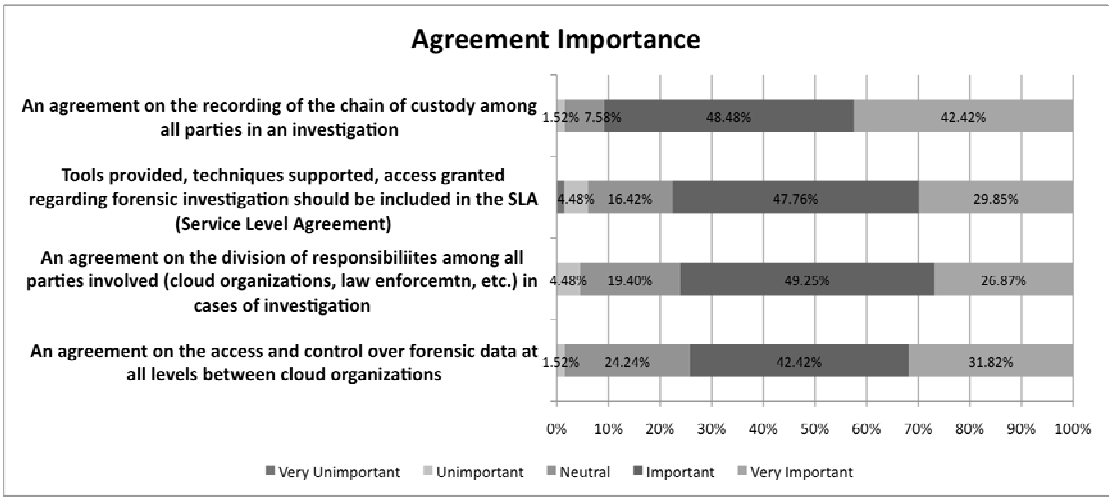

Fig 11. Agreement importance

As for agreements between various parties regarding cloud forensics, as shown in Fig 11 above, a mass majority of 90.9% 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, and 42.42% think it is very important. 77.61% 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. 76.12% 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 74.24% 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. 67 respondents answered this question.

4.4.6 Guideline importance

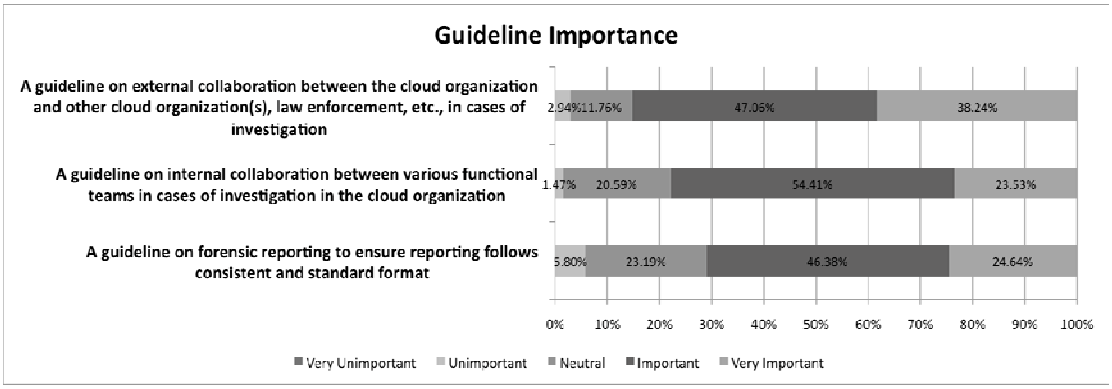

Fig 12. Guideline importance

Lastly, 68 respondents who answered the question on guideline importance have reached majority consensus, as shown in Fig 12 above. 85.3% 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. 77.94% of the respondents agree that "a guideline on forensic reporting to ensure reporting follows consistent and standard format" is important or very important. 71.02% 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.

5. CONCLUSION

In this paper, we presented the results and a preliminary analysis on the survey 'cloud forensics and critical criteria for cloud forensic capability' towards a group of digital forensic experts and practitioners who have good knowledge and sufficient experience in the field of digital forensics. From the survey results, we found out the majority of our respondents agree that 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. The respondents are more concerned about the challenges for cloud forensics, such as jurisdiction issues, and the lack of international collaboration, than optimistic about the opportunities of cloud forensics. As a result, a forensic architecture needs to be developed for cloud computing environments. Furthermore, the respondents have reached a consensus on what kind of tools, procedures, staffing, agreements, policies and guidelines are required for a cloud forensic capability.

6. FUTURE WORK

We will continue running this survey for a longer period of time in order to get more responses so that analysis can be made in depth. Base on the survey results we will start working on a framework of critical criteria for cloud forensic capability to suggest to the cloud computing industry as the next step.

7. REFERENCES

Buyya, R., Chee Shin Yeo, Venugopal, S (2008) 'Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilites' in Proceedings of 10th IEEE International Conference on High Performance Computing and Communications

Cloud Security Alliance [CSA] 2009 Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.

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

Garfinkel, S.L. (2010) 'Digital forensics research: The next 10 years' Digital Investigation 7: pp64-73

Gartner (2009A) Worldwide Cloud service revenue will grow 21.3 percent in 2009.

Gartner (2009B) 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

Gens, F. (2008) IT Cloud services forecast – 2008 to 2012: A key driver of new growth. IDC

INPUT (2009) Evolution of the Cloud: The future of cloud computing in government.

Merrill Lynch (2008) The Cloud wars: $100+ billion at stake.

Morrill, D. (2008) Cloud Computing Making Forensics Easier, CloudAve September 22

Perry, R., Hatcher, E., Mahowald, R.P., Hendrick, S.D. (2009) Force.com Cloud platform drives huge time to market and cost savings. IDC

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

Sawyer, J.H. (2009) Hazy Forecast for Cloud Computing Forensics, Darkreading March 9