Cloud Forensics Issues and Opportunities

[1] Asou Aminnezhad, [2] Ali Dehghantanha, [3] Mohd Taufik Abdullah, [4] Mohsen Damshenas
Faculty of Computer Science and Information Technology University Putra Malaysia
[1]Asou.aminnezhad@gmail.com, [2] alid@fsktm.upm.edu.my, [3] mtaufik@fsktm.upm.edu.my,
[4] damshenas@gmail.com

Abstract

Cloud computing technology is a rapidly growing field of study, which relies on sharing computing resources rather than having local servers or personal devices to handle applications. Most of the growth in this field is due to transfer of the traditional model of IT services to a novel model of cloud and the ubiquity of access to electronic and digital devices. Cloud computing posed a critical risk and challenges to digital investigators, but provides plenty of opportunities to investigators for improving the digital forensics. Moreover, cloud service providers and customers have yet to establish adequate forensic capabilities that could support investigations of criminal activities in the cloud. Notwithstanding the cloud presents some promising technical and economic benefits, users still resist to use cloud mainly due to security issues because it poses a challenge in doing cloud forensic investigations. Regarding this some research has been done, which propose solutions in doing forensic investigation. In this review paper, we take the first step towards reviewing the cloud forensics works that have been done by other researchers, and then do some discussion and analysis based on our findings to consider the opportunities and challenges confront the cloud forensics based on our findings.

Keywords*: Cloud Computing, Digital Forensic, Information Security, Forensic Challenges*

1. Introduction

The internet has travelled from the concept of parallel computing to distributed computing, grid computing and recently to cloud computing. Cloud computing has become one of the most controversial issues in information technology field that cause to shift many organizations toward transferring their data to the cloud as it presents many promising technical and economic benefits. Google, Microsoft Azure Services Platform and Amazon Web Services are some of the examples of commercial cloud service providers. Besides, there are some open source cloud systems such as Sun Open Cloud Platform and Eucalyptus that impress users to use the cloud more than past [1]. The word “cloud” originates from telecommunications world when providers started offering virtual private network. Back in the 1960s, the underlying concept of cloud computing was introduced by McCarthy [2]; his idea was that “computation may someday be organized as a public utility. Initially before VPN, telecom companies provided dedicated point-to-point data circuits, which waste bandwidth. Therefore, VPN services are used to switch the traffic to balance utilization of the overall network, that cloud computing extends this to cover servers and network infrastructure.

In this Paper, we review some papers on digital forensic, cloud forensics and the associated challenges that users may confront in a cloud environment. In section 2 in order to conduct research we evaluate and assess some related papers to undergo research nature and keyword analysis, after that in section 3, the necessary literature of the cloud computing and digital forensic models and related challenges will be discussed in order to broaden the reader's horizon of cloud knowledge. Furthermore, in section 4 we have discussion and analysis part. Finally in section 5 concluding remark shows that for having a proper implementation in cloud environment we need global standards in cloud to improve forensics investigator performance.

2. Data Analysis

In order to conduct this research, we collected a total of 47 related papers about cloud forensics to undergo research nature analysis, keywords analysis and literature review which provides a data

doi:10.4156/ijipm.vol4.issue4.9

collection method. This is essential to research as it provides a clear view of some works done by other researchers in this field.

As demonstrated in Figure 1 research nature analysis shows that the current trends of research pertaining to cloud forensic is mainly having laid in issues and risks in cloud computing and challenges that posed in cloud forensic. In this regard some of papers have either two of the research nature. There is a total of 22 papers mentioning these issues alone which indicate that the awareness of cloud security issues is increasing through the years of development of cloud computing.

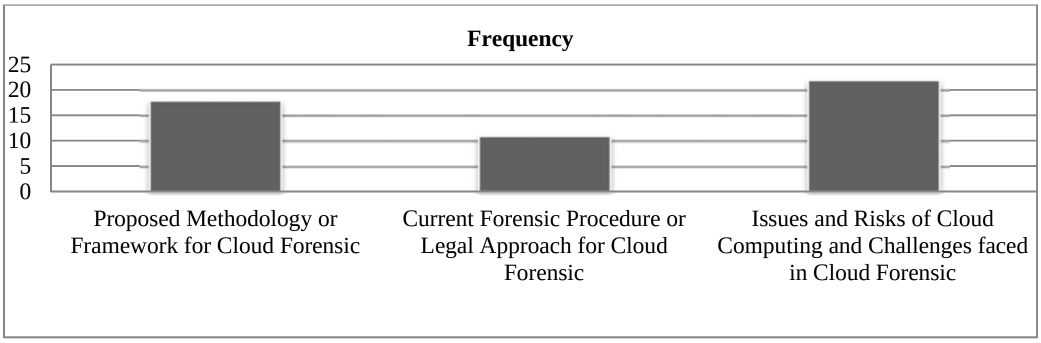

Figure 1. Research Nature

Papers that demonstrate current forensic procedures and legal approach toward the cloud platform has the lowest amount of research focus, this might indicate that the current forensic approach has faced shortcoming against cloud computing. On the other hand, researchers are proposing new standards, methodologies and framework as well to enhance the capability to perform cloud forensic that 18 paper of our studied paper regarding this matter. Furthermore keywords represent the general idea of a paper to the readers per se. As depicted in Figure 2 keyword analysis was done in this research for identifying the frequency of appearance of certain keywords in the cloud forensic field among the reviewed papers.

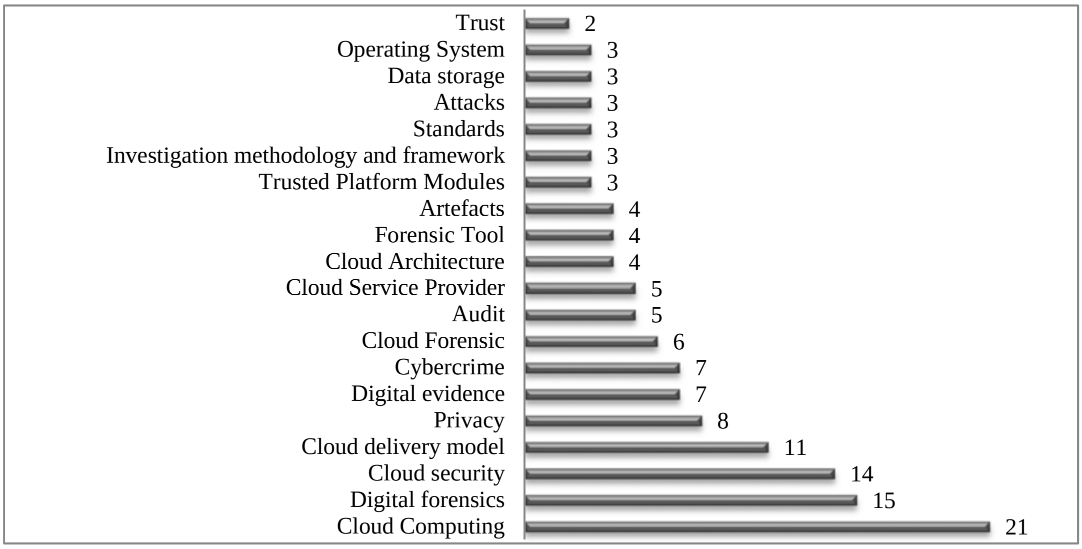

Figure 2. Keyword Frequency Analysis

Among all of the papers, cloud computing has a match of 21 times out of 47 papers. Digital forensics and cloud security are close as well standing at 15 and 14 times respectively. In the other hand, specific keyword such as digital provenance, event regeneration and 16 other keywords have been discussed just once. The significance of results show the most concentrate of researchers that given into the general area of cloud forensic instead of a specific one. All of collected papers have been read and summarized aim to give a comprehensive picture about cloud forensics to readers.

3. Literature Review

This section explains the concepts of digital evidence in cloud computing, also the risks and threats that may pose to users by working in a cloud environment. Furthermore, we discuss issues, opportunities, and challenges in cloud computing and some trust and privacy models for cloud forensics that categorized them into five groups as follows: security and trust model in a cloud, cloud forensic issues and challenges, cloud forensic, cloud model and privacy and pertaining risk in cloud computing.

3.1 Security and Trust Model in Cloud

Apart from a general audit, many related researches produced different models for cloud forensics in recent years especially in security and trust area. Among the people that using the cloud there also exists those who are not necessarily expert in the field of computing. The striking problems that identified are that traditional companies handle all the sensitive data internally and has complete control over the employees.

In a public cloud environment, data is accessible by privileged third parties, and the users cannot specify where their data should be located. So, in order to apply some form of control cloud suggests data encryption. At the start of using the cloud for more risky and sensitive data, one solution for the company is building their own private cloud. However, the cost of infrastructure is immense, hence a more feasible option is for the cloud provider to enhance the cost and provide a good secure service. Apropos of this matter Sato [3] proposes a trust model for cloud as a solution to these problems, which consists two layers, the internal and contracted layers. Internal trust refers to having a trusted platform module within the hardware systems; moreover, contractual trust refers to the organization and the cloud vendor coming to terms and establishing certain documents in the form of a contract.

As stated by Dimitrios et al. [4] relocation to the cloud, has deteriorated the productivity of traditional protection mechanisms. This being re-evaluated because the characteristic of the cloud differs from the traditional architecture. So, in order to ensure the confidentiality and authenticity of data, using a proposed trusted third party recommended; that it can be considered as a security solution in a cloud to provide a web of trust forming.

In this regard [5] suggests that if the cloud model no be entirely public, vendors can practice some amount of transparency to sketch what is being done in a particular area. Further, [6] explains the importance of cloud provider to propose the security policies and the various kinds of issues surrounding security. Regarding privacy issues, companies are responsible for all its confidential data even; furthermore, there is a critical flaw of companies that are not familiar with handling the store of data and control over it. As demonstrated in Figure 3, Chen and Zhao [7] pointed out that the primary inhibitor for acquiring cloud services is the data security and privacy protection issues surrounding the cloud, that across seven stages of data life cycle which are data generation, transfer, use, share, storage, archival, and destruction.

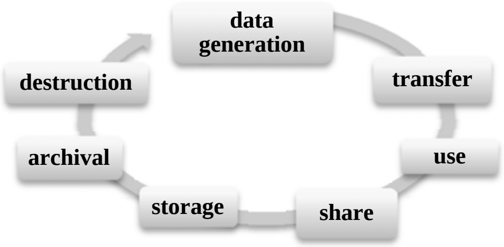

Figure 3. Data Life Cycle

Nonetheless, they provide a few security solutions which are currently existed. As enterprise boundaries have been extended to the cloud, traditional mechanism approaches are not suitable for applications and data in the cloud. They further highlight the cloud computing security issues.

According to Geethakumari et. al. [8] statement everyone who utilizes cloud computing will not see the lack of resources as a hindrance to their purposes anymore, but the security issues of cloud computing lie ahead. They also claim that cloud forensics emphasize on the accounting of the Authentication, Authorization and Accounting (AAA) Protocol and are used to analyze, investigate and reconstruct an event of a cloud attack in order to recover from it as soon as possible. Traditional method which uses log files and isolate system snapshot are not enough for the information extraction process but gave the events a blurred view. They also propose a technique that using a threshold value as the trigger of a series of snapshot which gives exact details of the changes that made in the system and indicates the beginning and the end of the attack.

In the paper [9], Ahmed and Raja raise the issues of security model in the cloud when a system migrates to the cloud environment. In the matter of this case end users or consumers should have a better understanding or in-depth knowledge of how the environment works in order to protect their rights properly.

3.2 Cloud Forensic Issues and Challenges

To address these issues researchers [10] have tried to propose conceptual frameworks; however, a few of them agreed with guidelines when it comes to data acquisition and forensic investigation in the cloud. They propose an iterative framework which is based on the currently used McKemmish and NIST that has similar names but the processes that take place are different. They suggest that the forensic investigators should develop evidence based on framework alongside the existing forensic practices. Regarding the trust in a cloud environment [11] highlights that for enhancing the trust of services in a cloud there should be a security based accreditation that covers technology. They also show that the current usage of SAS 70 (II) certification as an industry standard is only a beginning but it still is unable to provide the customers with the security features that they require. Stephens and Stilianos say that aside from end users who benefit from the services offered by cloud service provider, criminal users will also look into cloud computing to exploit possible loopholes that may exist within this new design and business model [12]. They claimed that Service level agreements (SLA’s) must be robust to combat cybercrime. Also they insist that security must be a part of the cloud solution and the engineers need to focus on the governance, risk and control while including it in the architecture. There seems to be a trend as the current standards are moving towards understanding the cloud environment and catering industry standards towards them. [13] stated that despite of utilizing cloud services for various aims, it can also be abused by users with malicious intents; for example, one could utilize the cloud service to perform a Distributed Denial of Service attack (DDoS) on other users or on the cloud itself which would make the services go offline. This is hard to distinguish legitimate content requests that have malicious intend, but at least the cloud providers can provide resources instantaneously to expand on the event a DDoS occurs. The cloud is vulnerable to similar kind of attacks as other applications on the internet and this caused to difficulty in managing it properly. The authors suggest that the cloud providers should implement strict access controls to prevent unauthorized access of users that tend to misuse the service and control accessibility to users' data for enhancing the security and privacy.

Birk and Wegener [14] assert that cloud computing has a great opportunity in terms of technology and the economy; however, many businesses are still reluctant to migrate their system to the cloud environment due to the security issues of the cloud and unknown threats. The researchers have analyzed different environments of the cloud and have suggested solutions to overcome the weakness of these environments. As a conclusion, the security issues in cloud environment are mostly caused by the absence of a unified global standard of cloud environment.

3.3 Cloud Forensic

Nowadays, digital devices devices are advancing rapidly, data generated by these devices require an enormous amount of computational power to analyze them. The concept of ‘Forensic Cloud’ is proposed and aims to allow an investigator to focus solely on investigation processes. Although the definition of cloud computing is defined, Svantesson and Clarke evaluate and reveal the risks in cloud computing from the perspective of consumer and privacy [15].

Regarding a cloud forensics Biggs and Vidalis [16] stated that criminal users posed striking problems and threats to end users who benefit from the offered services by the cloud service provider. The attackers will also look into cloud computing in order to exploit possible loopholes that may exist within this new concept, design and business model in cloud forensic. They claimed that Service level agreements (SLA's) must be robust to combat cybercrime. Further, they indicate to the cross-border legislation as a significant issue. That due to the many locations of cloud data centers coupled with the potential for data to be stored across those countries has the potential impact on digital investigator and their ability to conduct effective investigations. Also they analyze the impact of cloud computing with respect to forensic investigations and identified that while attempting to be secure, cloud computing is still not geared towards forensic readiness.ChengYan [17] discussed the threats in the current cloud environment, which contains data storage issue, personal privacy issue and trust of a Cloud Service Provider (CSP) issue. He stated that the cloud environment is faced with a cybercrime threat and needed for digital forensic more than past. Regarding the CSP he asserted that end users' data is stored and hosted cloud service provider's data center; that is to save costs of an enterprise such as equipment and maintenance expenses. The legal implications on how CSP handles the data handed over by end users are unclear to some companies and they are the main reasons to designate private cloud for retaining the benefit of cloud computing. He revealed that cloud environment also faces cybercrime forensic issue and evidence preservation issue.

Further, he proposed a framework designed with dynamic data monitoring system and data acquisition and analysis engine in the paper for the cloud environment to tackle these issues as well.

Mason and George [18] explain the flow of control of digital evidence and performing forensic investigation on cloud computing as the trend. That it has attracted more attention in recent years and inevitably causes confusion of the current judiciary system, which has not catered for cloud computing. The researchers clearly demonstrate in the paper on how to perform investigation based on the judicial system in the United Kingdom and how to obtain evidence from other jurisdictions as well.

As stated by Taylor [19] there are currently no established digital forensic guidelines for investigating cloud computing systems. He points out some noteworthy issues; for example, the cloud environment could be backed up and put into the cloud for the investigators if it is necessary to preserve a computing environment for an investigation. However, the migrated data would only represent a snapshot of when it was sent into the cloud. The data of cloud could be stored in different locations. So, the cloud data could be dispersed to a country where privacy laws are not enforced. It is not easy to establish the chain of custody for such data. A company may not know where the data is located. It is not practicable to image data from all the "computers" in the cloud.

3.4 Cloud Model

Regarding the cloud model one can be claimed that for evidence acquisition don't exist any feasible approach for the cloud computing model except for the IaaS cloud service model which resembles the environment of a machine [19]. As shown in the Figure 4 Hong Guo et al. claimed that SaaS and PaaS are not possible for collecting the system status since they do not provide access to the operating system commands. They also analyze and investigate the problems posed to investigators in each forensic investigation stage like identification, collection, preservation, analysis, reconstruction and reporting. Nevertheless, they proposed a model to address the problem and as well analyzed the proposed model. They state that there is a need to extend the applications of investigation processes in the cloud.

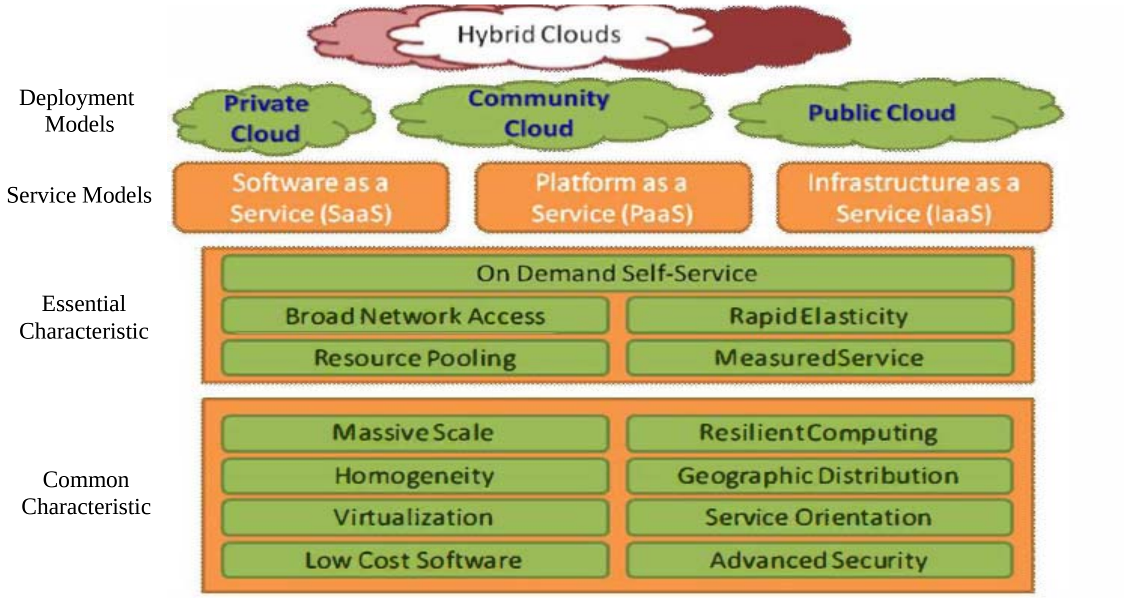

Figure 4. The Cloud Definition Framework

[20] Compares the process of traditional forensic investigations and forensic investigations in the cloud. They claim that the forensic process should be broken into four distinct steps. Step 1 is to determine the purpose of the forensic requirement. Step 2 identifies the cloud service model. Step 3 determines the type of background technology used. Step 4 further classified into three areas which are client side, server side and developer side. In concluding the paper, they suggest the computer forensic examiners have a broader range of technical knowledge. Instead of proposing a forensic method to overcome security issues of cloud computing, Lee and Hong proposed a service concept to fully utilize the computing power of the cloud to facilitate the computer forensic investigation process.

3.5 Privacy and Pertaining Risk in Cloud Computing

Cloud computing often refers to a technical arrangement where users rely on third parties who host the users' data on a remote server. As indicated in [22] just a little amount of attention has been given to cloud computing from the private and legal perspective. As stated by Hou et el. there are obvious privacy and consumer risks associated with cloud computing and need to be addressed. Remote forensics or cloud forensics enables investigators to harvest evidence remotely without travelling to the location and accessing the hard-drives physically

The disparate data on a cloud may belong to multiple data owners while part of the data is irrelevant to a computer crime investigation. Evidential data may scatter and make the cloning of data will lead to exposure of irrelevant data to investigator without permission of data owners. If a warrant is presented, the server administrator can retrieve the relevant information and handing it to the investigator but it defeats the purpose of confidentiality of the criminal case. To solve these issues he proposes a technique which utilizes multiple keywords to search for evidential data over encrypted data which preserve confidentiality of the investigation and just harvest the necessary data for investigation.

In this regard Yan Zhu et al. [23] proposed the notions of proof of retrievability (POR) and provable data possession (PDP) that audit services are critical to ensure the integrity and availability of data. They mentioned that a cryptographic technique like PDP can be used to realize audit services. They also discussed the current issues faced on auditing the correctness of data in a cloud environment. They said that based on hash functions and signature schemes, the traditional cryptographic technologies for data integrity and availability cannot work on the outsourced data without a local copy of the data.

In order to implement public auditability they assert that most existing schemes cannot give security proof against un-trusted CSP's deception and forgery; however, POR/PDP schemes offer a publicly accessible remote interface to check and manage data. So, they claimed that in cloud audit services, a new framework is desirable to enable the security of public verification protocol. For verifying the integrity of outsourced storage in the cloud based on cryptographic verification protocol, they proposed architecture of audit service outsourcing. To evaluate the proposed approach, they also implement a prototype of an audit system. Their experimental results have validated the effectiveness of the mentioned approaches and algorithms. The results also show that their system has a lower computational cost and a shorter extra storage for verification. They proposed architecture of audit service outsourcing to evaluate the proposed approach, also they perform a prototype of an audit system. Their experimental results have validated the effectiveness of the intimated approaches and algorithms. They are convinced that it is vivid that the nature of cloud computing is in direct conflicts with a digital forensic investigation by knowing the common digital forensic investigation practices that associated with privacy.

4. Discussion and Analysis

Before getting into the nut and bolts of cloud, studying the cloud forensic issue and any related papers would also be interesting and recommended. There were several works on analysis of cloud forensic, social network and virtualized environments [24-30], also in pervasive and ubiquitous systems some researcher work on this topic [31-35]. With growing usage of cloud several researchers tried to provide privacy sound models for investigation in these environments [36-40], in addition it is worthwhile that mention a few papers that work on malware investigation [41, 43]. Finally, there were models for forensics log protection while considering user privacy in log access occasions and the privacy and pervasive systems [44- 47] that can lead us to better comprehension of cloud environment. We identified several issues pertaining to cloud and why there is a growing resistance among major corporations to adopt the cloud. We then discuss how forensic investigations are currently carried out in the cloud and the issues associated with them and present an overview of the solutions seem in the various papers that were reviewed.

4.1 User Resistance to Cloud Adoption

We tried to analyze the various reasons why companies and others were not willing to adopt most convenient cloud services and arrived at the following findings: We found that cloud providers were unable to fulfil their customers’ needs when it came to aspect of assuring their capability to provide security, they focus on making their services convenient while security takes a back seat. Due to this users feel a sense of insecurity when using their services and do not take the risk of handling sensitive or mission critical data in the cloud. Another reason is that since the data is stored in multiple locations and is accessible to various users, sensitive data is processed outside the company perimeter and bypasses most of the security measures implemented internally. To mitigate this risk encrypting data are currently used, but one cannot rely on data encryption alone. Another potential solution to this problem is to have a private cloud, which allows the owner to manage the infrastructure within the organization and implement sufficient security policies, and trust is still withheld, as the owner would possess ownership of the data. This multiple user access issue also brings forth another concern. Further, cloud services are equally prone to constant attacks by cyber criminals. With more points of attack, these criminals have more access points that can be abused to grant them access to user data. They can use the same cloud services to initiate further attacks or to distribute, collaborate, share and store data accumulated from their criminal activities.

4.2 Current Cloud Forensic Investigations

Computer forensics investigations are often carried out by various law enforcement agencies in the event of cybercrime or other criminal activities. They follow guidelines which list out the procedures and principles that are required to be followed while dealing with digital evidence. This is necessary to ensure that the evidence that would be collected in the process would satisfy the legal requirements and be presentable in court. Investigations in the cloud present a particular new challenge to these forensic investigators due to its ephemeral nature.

4.3 Issues during Forensic Investigations Involving the Cloud

We elaborate the various kinds of issues that are posed to investigators in dealing with the cloud and found that investigating cloud services with the current methods was infeasible to be executed efficiently. The most prominent issues seemed to be the geographical, privacy and legal constraints that are faced by the investigators. With investigations involving the cloud, this can be even more challenging as it includes several thousand virtual machines, multiple servers and a large amount of cloud users amongst which only one of them is relevant to the case. It would lead to an interruption of service for other users not involved in the case. The computers are part of the cloud infrastructure and interoperate within the network without the user’s knowledge. Further, the only identity management that is done with the lack of physical interaction is commonly usage of user ID’s and password that can potentially be intercepted and abused by unauthorized users due to the open nature of the cloud. So, there is a huge void when it comes to tools that are available to support forensic investigators in dealing with cloud data centers. There is a lot of cross-platform development and a lack of standardization of infrastructure that makes it difficult to develop these tools for forensic data extraction.

4.4 Summary of Solutions Presented

On reflection, in this part we indicate some solutions that have been presented in the selected papers. First, we found the solutions that cater to the forensic investigations in the cloud. Cloud vendors provide infrastructure as a service that include a dedicated forensic server to assist the investigators. They also provide forensics as a service as the investigators would have to deal with large hard drives. This service can provide peta-bytes of storage to the investigators to handle multiple images, also help them crack encryption passwords. One of the frameworks that were proposed had combined the preservation and identification phases that help data to be preserved; uniqueness of this framework lies in its iterative step which is required for analyzing a client device as evidence. Another proposed framework introduced the use of a dynamic data monitoring system, is relevant to the constantly changing cloud environment, and data acquisition and analysis engine to counter the issues faced with the cloud. We also found solutions pertaining to individual phases of the traditional forensics frameworks. For identification phase problems, it was suggested that for Software as a Service model a feature to check the status of client’s usage and logging. Some interesting techniques were also discussed like the use of a threshold value in a monitoring system. Next, are solutions to security, trust and privacy concerns in the cloud, the solutions that were suggested is a secure aware cloud that adopts a cloud trust model. It has the component of internal trust, which is implemented using the trusted platform module within the hardware system. In brief, a most of the security problems that arise in cloud are mostly due to the lack of a unified standard model, which can improve forensic investigators' ability to perform investigations by proper implementation of global standards.

5. Conclusion

On reflection, the literature indicates the importance of cloud computing and cloud forensics in the cyber space, advantage and architecture and cloud models. The rapidly expanding cloud and digital economy may be disrupting many industries, but is also creating great opportunities. Further, the pervasive models in cloud show that from the cloud provider’s view point the immense data center structure with low price utilizing commodity computing, store data and required networking that reveal the marginal cost of resources that sold, in addition from the customer’s point of view of it would help users to build a data center. But as mentioned in the analysis section, currently there are no formalized cloud security standards in place. Also, we found out that investigation phase of cloud forensic has caused critical problems in the current judicial mechanism since data might be located where different legislation applies.

Notwithstanding, governments can try to make arrangements to preserve data for the purpose of investigation across borders, it becomes difficult to decide the appropriate court or legal system to represent the case. On the other hand, the tool that are available to support a forensic investigation cannot fully apply to do forensic investigation in cloud forensic. So a proper implementation of global standards helps to improve the ability of forensic investigators to better performance of cloud.

6. References

[1] M. Taylor, J. Haggerty, D. Gresty, R. Hegarty, “Digital Evidence in Cloud Computing Systems,” Computer Law & Security, pp. 304-308, 2010.

[2] Y. Jadeja, K. Modi, “Cloud Computing - Concepts, Architecture and Challenges,” International Conference on Computing, Electronics and Electrical Technologies [ICCEET], pp. 877-880, 2012.

[3] H. Sato, A. Kanai, S. Tanimoto, “A Cloud Trust Model in a Security Aware Cloud,” Annual International Symposium on Applications and the Internet, pp. 121-124, 2010.

[4] D. Zissis, D, Lekkas, “Addressing Cloud Computing Security Issues,” Future Generation Computer Systems, pp. 583-592, 2012.

[5] C. Everett. “Cloud computing - A question of trust,” Computer Fraud & Security, pp. 5-7, June 2009.

[6] F. Sabahi, “Cloud Computing Security Threats and Responses,” pp. 245-249, 2011.

[7] D. Chen, H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” International Conference on Computer Science and Electronics Engineering, pp. 647-651, 2012.

[8] A. Belorkar, G. Geethakumari, “Regeneration of events using system snapshots for cloud forensic analysis,” India Conference (INDICON), pp. 1-4, 2011.

[9] S. Ahmed, M. Yasin Akhtar Raja, “Tackling Cloud Security Issues and Forensics Model,” pp. 190-195, 2010.

[10] B. Martini, K. R. Choo, “An integrated conceptual digital forensic framework for cloud computing,” Digital Investigation, pp. 1-10, 2012.

[11] D. Reilly, C Wren, T. Berry, “Cloud Computing: Forensic Challenges for Law Enforcement,” pp. 1-7, 2010.

[12] R. Morrell and A. Chandrashekar, “Cloud computing: new challenges and opportunities,” Network Security, pp. 18-19, 2011.

[13] M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Shamsuddin, “Forensics Investigation Challenges in Cloud Computing Environments,” Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 190-194, 2012.

[14] D. Birk, C. Wegener, “Technical Issues of Forensic Investigations in Cloud Computing Environments.” pp. 1-10, 2011.

[15] D. Svantesson, R. Clarke, “Privacy and Consumer Risks in Cloud Computing,” Computer Law & Security Review, pp. 391-397, 2010.

[16] S. Biggs, S. Vidalis, “Cloud Computing: The Impact on Digital Forensic Investigations,” Institute of Electrical and Electronics Engineers, 2009.

[17] C.Yan, “Cyber crime Forensic System in Cloud Computing,” Image Analysis and Signal Processing (IASP), pp. 612 – 615, 2011.

[18] S. Mason and E. George, “Digital Evidence and ‘cloud’ computing,” Computer Law & Security Review, pp. 524-528, 2011.

[19] T. Moore, "The economics of digital forensics," Fifth Annual Workshop on the Economics and Information Security, 2006.

[20] H. Guo, T. Shang, B. Jin, “Forensic Investigations in Cloud Environments.” Computer Science and Information Processing (CSIP), pp. 248 – 251, 2012.

[21] J. Lee and D. Hong, “Pervasive Forensic Analysis based on Mobile Cloud Computing,” International Conference on Multimedia Information Networking and Security, pp. 572-576, 2011.

[22] S. Hou, T. Uehara, S.M. Yiu, L. C. K. Hui, K. P. Chow, “Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics,” International Conference on Multimedia Information Networking and Security, pp. 595-599, 2011.

[23] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multi-cloud storage," 2012.

[24] C. Kessler. “Anti-Forensics and the Digital Investigator,” Proceedings of the 5th Australian Digital Forensics Conference, 2007.

[25] D. Liu, J. Lee, J. Jang, S. Nepal, J. Zic, “A Cloud Architecture of Virtual Trusted Platform Modules,” IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 804-811, 2010.

[26] M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Bin Shamsuddin, “Forensics investigation challenges in cloud computing environments,” Cyber Warfare and Digital Forensics (CyberSec), pp. 190-194, 2012.

[27] F. Daryabar, A. Dehghantanha, F. Norouzi, F Mahmoodi, “Analysis of virtual honeynet and VLAN-based virtual networks,” Science & Engineering Research (SHUSER), pp. 73-70, 2011.

[28] S. H. Mohtasebi, A. Dehghantanha, “Defusing the Hazards of Social Network Services,” International Journal of Digital Information, pp. 504-515, 2012.

[29] A. Dehghantanha, R. Mahmoud, N. I Udzir, "Towards Green Frameworks for Digital Forensics Investigation,” Journal of Convergence Information Technology (JCIT), Vol. 8, No. 2, pp. 669 ~ 678, 2013.

[30] M. Sidheeq, A. Dehghantanha,G. Kananparan, "Utilizing Trusted Platform Module to Mitigate Botnet Attacks", International Journal of Advancements in Computing Technology(IJACT), Vol. 2, No. 5, pp. 111 ~ 117, 2010.

[31] A. Aminnezhad, A. Dehghantanha, MT. Abdullah, “a survey on privacy issues in digital forensics,” International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2013.

[32] H. Salehi, R. Boostani , A. Aminnezhad, “A New Hybrid Algorithm to Solve the Task Scheduling Problem in Grid Computing,” International Journal of Computer Applications, 2013.

[33] A. Dehghantanha, R. Mahmod, N. I Udzir, Z.A. Zulkarnain, “User-centered Privacy and Trust Model in Cloud Computing Systems,” Computer And Network Technology, pp. 326-332, 2009.

[34] A. Dehghantanha, “Xml-Based Privacy Model in Pervasive Computing,” Diss. University Putra Malaysia, 2008.

[35] C. Sagaran, A. Dehghantanha, R Ramli, “A User-Centered Context-sensitive Privacy Model in Pervasive Systems,” Communication Software and Networks, pp. 78-82, 2010.

[36] A. Dehghantanha, N. Udzir, R. Mahmod, “Evaluating user-centered privacy model (UPM) in pervasive computing systems,” Computational Intelligence in Security for Information Systems, pp. 272-284, 2011.

[37] A. Dehghantanha, R. Mahmod, “UPM: User-Centered Privacy Model in Pervasive Computing Systems,” Future Computer and Communication, pp. 65-70, 2009.

[38] S. Parvez, A. Dehghantanha, HG. Broujerdi, “Framework of digital forensics for the Samsung Star Series phone,” Electronics Computer Technology (ICECT), Volume 2, pp. 264-267, 2011.

[39] S. H. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, “Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone,” International Journal of Digital Information and Wireless Communications (IJDIWC),volume 1, issue 3, pp. 651-655, 2012.

[40] F. N. Dezfouli, A. Dehghantanha, R. Mahmoud ,”Volatile memory acquisition using backup for forensic investigation,” Cyber Warfare and Digital Foresnsic, pp. 186-189, 2012.

[41] M. Ibrahim, MT. Abdullah, A. Dehghantanha , “VoIP evidence model: A new forensic method for investigating VoIP malicious attacks,” Cyber Security, Cyber Warfare and Digital Forensic , pp. 201-206, 2012.

[42] F. Daryabar, A. Dehghantanha, HG. Broujerdi, “Investigation of Malware Defence and Detection Techniques,” International Journal of Digital Information and Wireless Communications (IJDIWC), volume 1, issue 3, pp. 645-650, 2012.

[43] F. Daryabar, A. Dehghantanha, NI. Udzir, “Investigation of bypassing malware defences and malware detections,” Conference on Information Assurance and Security (IAS), pp. 173-178, 2011.

[44] N. Borhan, R. Mahmod, A. Dehghantanha, “A Framework of TPM, SVM and Boot Control for Securing Forensic Logs,” International Journal of Computer Application, pp. 65-70, 2009.

[45] A. Dehghantanha, N. I Udzir, R. Mahmod, “Towards a pervasive formal privacy language,” Advanced Information Networking and Applications Workshops (WAINA), pp. 1085-1091, 2010.

[46] A. Dehghantanha, R. Mahmod, N. I Udzir, “A XML based, User-centered Privacy Model in Pervasive Computing Systems,” International Journal of Computer Science and Networking Security, Vol.9, Issue 2, pp. 167-173, 2009.

[47] A. Dehghantanha, R. Mahmod, N. I Udzir, Z.A. Zulkarnain, “User-centered Privacy and Trust Model in Cloud Computing Systems,” Computer And Network Technology, pp. 326-332, 2009.