Investigation on the Services of Private Cloud Computing by Using ADAM Method

By Imam Riadi

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 5, October 2016, pp. 2387~2395
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i5.11527

Investigation on the Services of Private Cloud Computing by Using ADAM Method

Nur Widiyasono[1], Imam Riadi[2], Ahmad Luthfi[3]
[1]Departement of Informatics, Siliwangi University, Indonesia
[2]Departement of Information Systems, Ahmad Dahlan University, Indonesia
[3]Department of Informatics, Indonesia Islamic University, Indonesia

Article Info

Article history:

Received Jun 13, 2016
Revised Aug 19, 2016
Accepted Sep 7, 2016

Keyword:

ADAM
Cloud
Evaluation
Forensic
Investigation

ABSTRACT

Cloud services are offered by many cloud service providers, but most companies generally build a private cloud computing. Cloud systems abuse can be done by internal users or due to misconfiguration or may also refer to the weaknesses in the system. This study evaluated ADAM (Advanced Data Acquisition Model) method. Referring to the results of the investigation process by using ADAM Method, it can be verified that there are several parameters of the success investigation; therefore the investigation by using ADAM can be succesed properly and correctly. Another contribution of this study was to identify the weaknesses of the service system that used owncloud in users list of the same group can change another's user's password.

Corresponding Author:

Imam Riadi
Ahmad Dahlan University
Jl. Prof. Dr. Soepomo, Janturan, Yogyakarta 55164
Email: imam.riadi@is.uad.ac.id.

1. INTRODUCTION

Cloud computing is a technology services that are offered by the cloud service provider (CSP), among other types of deals platform as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS). This service provides a wide range of facilities and benefits for consumers, among others, is the provision of self-service, elasticity, and pay per use. Cloud services are divided into four parts including private cloud, public cloud, public cloud and hybrid cloud [1].

Private cloud is built to the needs of organizations that include the entire cloud infrastructure including hardware resources owned by the organization. Community cloud is a cloud that is used collectively by organizations that have the same type of business. Public Cloud is the cloud that was built and used by the Organization publicly to his business interests. Hybrid Cloud is a combination of private, community and public cloud [2].

Cloud services offered include hosted desktop is a virtual machine on a cloud. This service has applications and data that reside on a remote data center. The owner of this service can access applications and data via computer desktop. This desktop hosted service can be abused to commit cyber crime [3]. Abuse of this service can also occur due to the presence of flaws (bugs) from the side of the security of the system. According to NIST, the stages on cloud computing forensics is the identification, collection, preservation, examination, interpretation and reporting of digital evidence [4].

The handling of cyber crime techniques required the acquisition of data, where the data acquisition technique can be done on a live system or write-block system [5-7]. The second data acquisition techniques are not only done cloud computing services, but can also be done on the client computer, server, notebook and a smartphone. Live data acquisition process system means the process for getting a digital proof is

carried out when the system is in a State of life while the write block system is the data acquisition process is done when the system is in a State of death for example the process of acquisition of data on the hard drive.

Process data acquisition does cloud computing services can be treated the same because of the characteristics of those services is not the same [8]. The solution given in the problem of cloud forensics is utilized by the logging framework. It is used to ensure that the log data was successfully collected can be used for forensic investigation process [9]. There are several methods offered, among others, by the method of ADAM (The Advance Data Acquisitions Model). This method was developed to address the problem within the framework of data reabilitas how the evidence was obtained by digital data and this will be of particular concern in the Council but unfortunately ADAM method has never done an evaluation independently [10].

Cloud Computing is the application of Forensic Science digital forensics which is cloud computing environment, and technically conducted forensic approach consisting of a hybrid such as remote, virtual, network, live, thin-client against digital evidence and organizationally involved the interaction between actor cloud computing for internal and external investigations, as well as legally imply multiple-jurisdiction and multiple-tenant situation [11].

A report from the National Institute of Standards and Technology noted that the Guide to obtaining and performing forensics on cloud computing services and suggested that guidelines are the best there is and still applies to do a digital forensics in cloud computing environment [12]. Digital forensics methods that exist, it is not suitable for cloud computing environment [13].

The guidelines on the collection of digital evidence are already scarce and outdated. There are no specific guidelines for collecting digital evidence on Cloud Computing [14], [15], [16],[17]. The research found on this little cloud computing, such as how to retrieve data from the cloud service in forensic voice [18].

Similar observations were undertaken by a number of digital forensic practitioners, including the Director of the US Department of Defense Computer Forensics Laboratory and Chief Scientist at the U.S. Air Force Research Laboratory Information Directorat which suggests that "research is required in the cyber domain, especially in cloud computing, to conduct the identification and classification of the unique aspects of doing where and how digital evidence can be found. The end point of such mobile devices also increases the complexity of this domain. Trace evidence can be found on the servers, switches, routers, cell phones, and others [19],[20].

The legal point of view, the system of cloud computing has the potential for high levels of difficulty doing forensic computer analysis process as well as to obtain and perform analysis of digital evidence with the same standard as in traditional server systems [21]. It is due to the difficulty in establishing data stored or processed by special software. The stage of "Collection" becomes a much more complicated process in cloud computing environments due to the physical location of the data, the distribution of data across multiple servers or storage devices and jurisdiction, and others [22], [23].

Research conducted in the NIST Framework, discusses the identification (identification) and preservation (preservation) as part of the phase of collection (Collection) so that it indicates that the identification phase in cloud computing is more important, whereas phase preservation should work closely with cloud service providers, both steps are important in investigation on cloud computing. Phase identification and preservation phase are the source of the evidences that must be simultaneously and as quickly as possible. For example if the data source already identified, then it should immediately contact the cloud service provider to begin the preservation.

The role of artifacts (e.g. metadata) in forensic analysis and (prospective) is loss of this artifact when data collected from the cloud computing environment. If the metadata (e.g. creation/modification date of a file, and log the user's ownership) that is lost during the process of collecting. It influences the ability of researchers to conduct a forensic investigation to the standards required by the court [24].

Digital forensics process can be divided into four distinct, they are:

[1] Collection of artifacts (both digital and material evidence of the accomplice) that is considered to have potential value to collected.
[2] Preservation of the original artifacts in a way that is reliable, complete, accurate, and verifiable.
[3] Analysis of artifact filtering to eliminate or entry of goods that are considered valuable.
[4] Presentation where evidence is presented to support the investigation of.

Traditionally, there are two categories of digital forensics there-they are, static digital/write "block" and "live from", in which these two categories become a result of the evolution of forensic specialists to create and document incidents in sophisticated.

2. RESEARCH METHOD

Process flow stages of research can be described in Figure 1. Previous research studies are conducted to know the problems that exist in the process of investigating cloud computing services are mainly related to the acquisition process data cloud computing service, the methods used to make the process of data acquisition, as well as the background behind the issues behind ADAM'S methods, so that it can support on the ultimate purpose of doing this research.

Figure 1. Research process flow

Preparation system is the stage building of the private cloud computing services by using a Microsoft Windows operating system platform 2008 Advances server, VirtualMachine (VMware), OwnCloud-5.0.5 Server by providing ip public then this private cloud services can be accessed through the internet, as well as local networks and hotspots. This service can also be accessed by using the pc-desktop, notebook or a smartphone, while the network topology as shown in Figure 2.

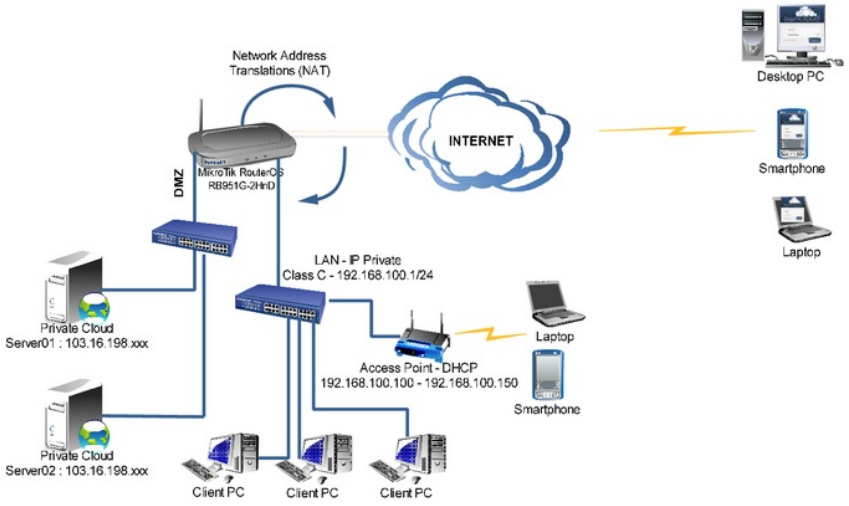

Figure 2. Conceptual Access Service Private Cloud

Case studies are used in the simulation of the computer network in the laboratory is the case of hospital in Tasikmalaya town whose name is camouflaged into XYZ hospital. This case is an example of the occurrence of abuse by an employee who leaked secret these companies to the competitor. Digital Private Investigator has a duty to get the digital evidence that very potential when it is on the side of the private cloud services, desktop PC or Smartphones that use the suspect. Knowing by every employee incompany XYZ hospital can use this private cloud service facilities so that it is possible to abuse the facility occurred to divulge company secrets to its competitors.

Investigation into the case simulation using the services of private cloud computing. The investigation was conducted beginning on private cloud computing service or from the server side, then from the side i.e. monitoring network against data traffic exiting/entering into private cloud computing service server and get the digital evidence sessions in layer (layer 5 OSI 7 layers) Using Wiresharks or Network

Minner tool, then an investigation against desktops or notebook and Smartphones connected on the services is done. A benchmark of success in performing the investigation is able to know the location or position of the digital evidence either side private cloud servers, desktop PCs, notebook or Smartphones, besides other parameters areip source, mac-address, username and password, log data systems, can open the file encryption, and other resources can be used as an additional digital evidence, then the digital proof verification and compliance between digital evidence found on the side of the private cloud server, pc desktops, notebooks and Smartphones. Investigation on this case is an example in using the method of ADAM (The Advance Data Acquisitions Model) which has 3 stages, they are:

a) Initial Planning: a senior investigator and the team should understand the task or the case that will be faced that is they should have the capability of details about computer systems/cloud system, the number and location of data, the type of hard disk and the operating system being used, the other must be able to determine the overall picture about the case at hand, determine the desired end results on the case at hand, determine the parameters. Then there are some which must be considered viz. the existence of constraints such as authorisation internally, externally, and legal constraints phisik related access to property which is the location of many related time constraints, the court order against the property by private or commercial, i.e. data constraint type and number of locations identified, so that such things should be made as well as logistic planning and preparation are required. Simulation study on the case of this study, a senior investigator and the team must understand some cases which occurred in the service of private cloud computing by making American including forming teams that have expertise as stated above. Some of the sheets have been prepared form signed by a senior investigator and thereafter conducted planning will be undertaken with respect to the incidence of litigation.
b) The On Site Planning: the Second Stage of the process, i.e. when ADAM method is what Genesis matters then the senior investigator and the team made a major acquisition plan, as this relates to the location of the data, the size and format of the data. Safety concerns at the moment in the scene details, team and personnel data would require equipment that can do the isolation, accompanied by an update or maintain against the documentation of all the activities that take place (contemporary records of all activities), conducted a preliminary survey to ascertain the location of the data, determine the technical identities, and define acquisition mix on the scene things or brought to the digital forensic laboratories. Then perform updates against the planning that will be used on the next stage of the process method of ADAM.
c) Digital Data Acquisition: the Third Stage of the method of digital data acquisition ADAM is done in these devices which will be done on the server side data acquisition service private cloud computing, from the side of the computers as well as from the side of your smartphone device used by the suspect. Process data acquisition carried out by digital forensics practitioners should consider several things, such as digital data evidence is very fragile because of its nature that is easily damaged (associated with the accompanying hardware device), integrity is highly vulnerable to changes (quite possibly modified), even damage could have occurred because of a technical fault or human error. Handling is very carefully done, mistakes and failures would be distorting the end result even eliminate it. It needs careful handling and protection will the authenticity of digital evidence.

Analysis is the stage to do the evaluation of the process of investigating cases that occur by utilizing the methods of ADAM (The Advance Data Acquisition Model), or Implementation methods of investigative services process ADAM on private cloud computing can produce digital data appropriate evidence and is a critical issue in the data acquisition process so that it can respond to the problem of data reliability or process to get the data of the digital evidence of concern the attention in court

The documentation is the stages where each stage in the process of investigation for archiving or documentation, any changes or he obtained evidence supporting digital data recording/documentation update is done.

3. RESULTS AND ANALYSIS

Exploiting client applications OwnCloud this can be done through desktop PCs as well as Smartphones, while smartphone connections to private cloud services can be done through internet access as well as access through the access point/hotspots in the local network.

The results of the investigation process that is conducted by applying ADAM method are as follows:

a) Initial planning:
   - Making initial planning related cases "XYZ Hospital" the divulging secret information of the company which is done by a staff to another party, where such information has been obtained by exploiting the weaknesses and mistakes the governance of private cloud computing service.

- Determine the teams that will be involved in the process of investigating such cases including the fulfillment of competence IT is necessary.
- Identify Software applications and Tools that are needed for the investigation.
- Make the task letter/warrant required by the officer who will then be forwarded to the management "XYZ Hospital".
- create and perform updates against any activities conducted

b) The on Site Planning:

- Identify sources that become potential evidences such as digital data service private cloud server, datalink layer 2, layer 3 network layer, 5 Session, and layer 7 applications.
- Make plans with the method of data acquisition process Live Acquisitions or Write Block Acquisitions.
- Determine the application Software being used such as WireSharks, Network Minner, WinISO or UltraISO

c) Data acquisition:

- Obtain digital data evidences found in private cloud services system, desktop pc or smartphone, and devices such as network switches and routers.
- Create the results reports of the investigation.

Initial Planning team determines the digital forensic investigator/analyst, and consisted of a Chairman and 2-3 team members who have expertise in the field of IT competence in General, have the knowledge about the technology of virtualization/cloud computing, understand the various linux-based operating system such as windows base, base, understand the structure of folders and files, understand about network security and systems such as the network device switch, router and access-point, understand about technology-based mobile services such as Smartphones. In addition a team of investigator must also be able to determine the types and the tools that will be used to perform the process of investigation in the field as well as setting up software Wiresharks, Network Minner, UltraISO or WinISO. Then the team should also prepare documents or letters warrant duty to perform the process of investigation of the handling of cases and always update the information for every activity which is done.

The onsite planning investigation team determines potential sources of digital data evidences found on private cloud computing service and makes plans to determine the process of data acquisition acquisitions live or write-block acquisitions. Data acquisition process is shown in Figure 4 and Figure 5. Then to determine the process, it can be done by using tools or software application to perform the data acquisition process. Here is no consensus regarding specific software applications used to process data acquisition on cloud computing services. This study uses several software applications to support data acquisition either by live acquisitions or write block acquisitions.

Figure 4 is A flow process for acquisitions where live data software applications or tools that are used are grown on a private cloud service machine. Then the activation of the system log that is located on a private cloud service, router mikrotik by making rule (IPS-Firewall-Chain (Forward/Input/Output) – action log). Catching live data acquisitions done in layer 5 (session layer) by utilizing software such as wiresharks or network minner tools. Files generated from the process of arrest data on layer 5 (session layer) is this *.pcap (packet captures) or *. Cscpkt (colasoft capsa packet) then the file is analyzed to find some data types such as digital proof files, mac-address, username, password, logs, and time-stamp.

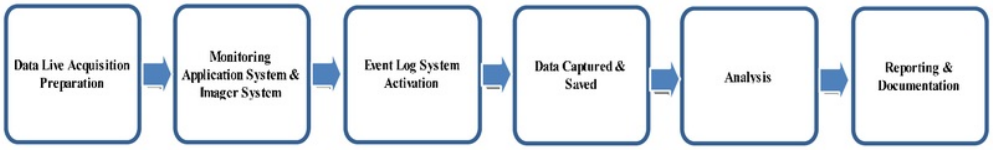

Figure 4. Live Data Acquisitions Process

Data capture is performed using by Network Minner data traffic heading towards machine private cloud and in the get that client access with ip public (202.95.128.xxx) which passes through the router device will use the mac-address of the router (D4:CA:6D:68:89:07) the case with devices (desktop pc/smartphone) via the access-point/hotspots when access to private cloud services and through the device router then it will be found to use the mac-address of the router. Using tools “network minner” will be obtained as a host,

frames, files, image, message, credentials, sessions, DNS (s), parameters, keyword, cleartext and anomalies, results data capture will be saved in the file berekstensikan. This pcap (packet captures). Utilizing features that are owned by network minner can give the required results in the data live acquisition process.

Figure 5. is a process of acquisition data is write-block, where all access that leads to the private cloud services do blocking access so that the data that will be acquired are not changed or omitted by the suspect. The process of blocking access can be done through the mikrotik router os by making the rules on the Firewall-IP-IP Destinations drop action.

Figure 5. The Process Write Block Data Acquisitions

Private cloud service systems grown applications that have the ability to process imaging file (*.iso or *.dd) or process data acquisition can be performed remotely to the machine even though the private cloud services through a local area network (LAN). Case simulation performed using UltraISO or WinISO application, after the known position of the folders and files that reside on the private cloud computing service machine then conducted the process of imaging files and do an examination of the hash value on the files. The image file next analysis and discover files that became the object of abuse or some files that were leaked to third parties on a simulated case and the next step is to make the acquisition process report data in write-block. Acquisition data process with ADAM method can be done per device that has the potential of digital data sources evidences such as servers, desktop PCs, smartphones, network devices such as router mikrotik so on simulation case study in digital data table can be compiled evidence found as presented in table 1 as follows:

Table 1. Data Acquisition Device according to Method ADAM

No.	Parameter	Private Cloud	Desktop PC	Smartphone	Router
1	IP Source	√	√	√	√
2	Mac Address Source	√	√	√	√
3	IP Destinations	√	-	-	√
4	Mac Address Destination	√	-	-	√
5	Files Folder Structures	√	√	√	-
6	Log Activity - System	√	√	-	√
7	Username dan Password	√	√	√	-
8	Time Stamp	√	√	√	√
9	Data Locations	√	√	√	-
10	Protocol & Port Access	√	√	√	√
11	Browser – artefact	√	√	√	-

With Table 1 to get the mac-address of the original source difficulties are caused when a desktop PC (Personal Computer) or smartphone device connected to a network device such as a router then the mac-address mac-address is used on the router.

Blocking Access was intended to condition the Files contained on the private cloud services did not change. Image files created are stored with the file name "DigitalEvidenceRSIAXYZ.iso", this image files then checked the MD5 hash values: 08C1707E0D100B6E9255FC35030C57F0, to ensure the originality of these files with MD5 Checksum tool & SHA as shown in Figure 6.

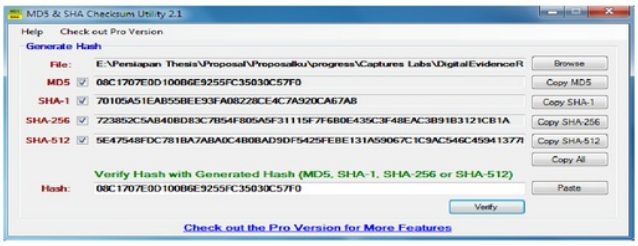

Figure 6. MD5 & SHA Checksum

Based on the results that have been obtained from the suspect, the next step is to verify the information from structure analysis of the activity log file folders, system, time stamp, or a source of digital evidence that evidence obtained from private cloud servers, desktop PCs, and Smartphones This *.pcap. The results of the verification on a smartphone can be shown in Figure 7.

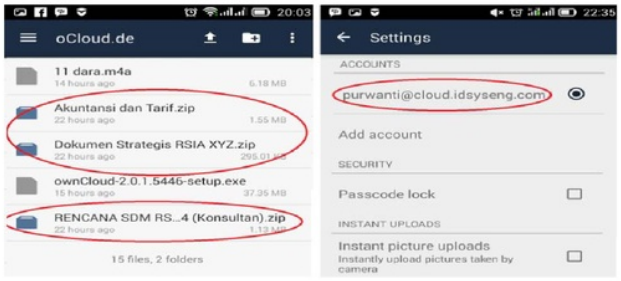

Figure 7. files on the Smartphone Verification (a)

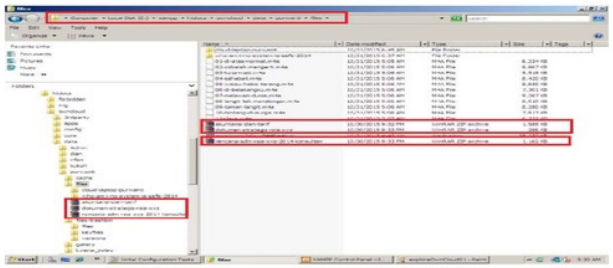

Figure 8. Structure File Folder Server Side Verification (b)

Based on the results obtained on the private cloud data file folder structure of the unnoticed digital evidence as in Figure 8. above. The image above shows the data of digital evidence found is located at c:\\xampp\htdocs\owncloud\data\purwanti\files, and the name of the files that are found are "akuntansi-dan-tarif.zip," dokumen-strategis-rsia-xyz.zip and rencana-sdm-rsia-xyz-2014-konsultan.zip, all three of these files are in the suspect becomes the object of the problem.

The ability of Network Minner in the capture data in layer 5 (session layer) as shown in Figure 9.

Figure 9. Credentials Verification (c)

OwnCloud client application can also be made verification of the suspect with log-like Figure 10. See the results of the investigation by using ADAM, obtaining the results which led to the abuse of private cloud services in XYZ hospital is a user management weaknesses on the application server version 5.0.5 ownCloud so among users in the same group can change the password. Verification of digital evidence findings of data on smartphones, desktop and private cloud computing server side, as well as process data acquisition directly or write-block acquisition can be done with the percentage of success in the process of investigation method ADAM service private cloud computing is 100%. The success investigation in the case XYZ hospital is able to locate file folder location data digital evidence, usernames and passwords, time stamps, ip address and mac-address, and the suitability of the data file digital evidence obtained from smartphones, desktop computers and on computers computing private cloud.

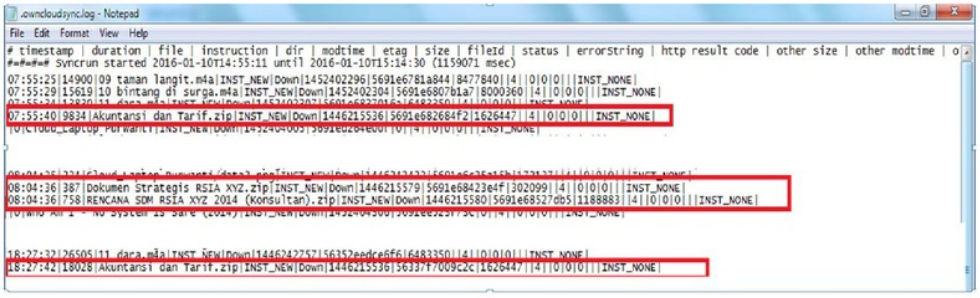

Figure 10. OwnCloud Client Log Verification (d)

To Improved the security in minimizing the occurrence of abuse can take advantage of the technology of virtual private network services, using a product that has a better user management, and policy management enterprise in using private cloud computing services to be tightened and restricted to specific users.

4. CONCLUSION

The use of the ADAM method (The Advanced Data Acquisition Model) in the process of investigating private cloud computing services has been successfully carried out. The process of data acquisition on the service can be succesed either directly or writing block acquisition per device so that the problems of reliability of evidence as digital data can be justified in court. Referring to the case of potential abuse XYZ hospital against dissemination of confidential data may occur due to the weakness of the current system, or configuration errors, this can occur because policy abuse for private cloud computing services.

Next research can be done for performing an analysis of the software or hardware used to perform data acquisition process on cloud computing services, because until now there is still no consensus on the standardization of its use.

REFERENCES

[1] Webb E.H., "Digital Investigations in the Cloud." Farnborough, UK:QinetiQ Digital Investigations Service, 2010.
[2] Carlin,Sean, and Kevin Curran."Cloud Computing technologies."International Journal of Cloud Computing and Services Science 1.2 (2012):59.
[3] Lovell H., Maxwell W., Wolf C., DCA Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions, Hogan Lovell White papers.13, 2012.
[4] National Institute of Standard and Technology (NIST) ,Challenging security requirements for US government Cloud Computing adoption, U.S. Department of Commerce, National Institute of Standards and Technology, Gaitherbug, 2011.
[5] Lessing M., Solms B.V., "Live Forensic Acquisition as Alternative to Traditional Forensic Processes", Council for Scientific and Industrial Research Meiring Naudé Road, Scientia Pretoria, South Africa, 2011.
[6] Shahzad A., Musa S., Aborujilah A., and M. Irfan, A New Cloud Based Supervisory Control And Data Acquisition Implementation To Enhance The Level Of Security Using Testbed, Journal of Computer Science 10 (4): 652-659, ISSN: 1549-3636, 2014.

[7] Cheng, Fa-Chang, and Wen-Hsing Lai."Creating the environment for the prosperity of cloud computing technology".Indonesian Journal of Electrical Engineering and Computer Sciense 10.4 (2012):864-875.
[8] Bodenheimer, D. Z., Cloud Computing Acquisitions & Cyber security. Briefing Papers, No. 12-11, 20, 2012.
[9] Marty R, "Cloud application logging for forensics," in proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 178–184, 2011.
[10] Adams R, V. H., The Advanced Data Acquisition Model (ADAM): A Process Model For Digital Forensic Practice. Journal of Digital Forensics, Security and Law, Vol. 8(4), 24, 2013.
[11] Ruan K, P. J., Cloud forensics: An overview. *IBM Ireland Ltd*, 16. 2011.
[12] Huber M, Mulazzani M, Leithner M, Schrittwieser S, Wondracek G,Weippl, E, Social snapshots: digital forensics for online social networks, In: Annual Computer Security Applications Conference – ACSAC 2011, Orlando, Florida, USA; 2011, pp. 113–122, 2011.
[13] Barrett D & Kipper G, Virtualization and Forensics: a digital forensic investigator's guide to virtual environments, Syngress, 2010.
[14] Birk D & Wegener C, Technical Issues of forensics IInvestigations in cloud computing environments, Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE, 2011.
[15] Shams Z, R Hasan, Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems, University of Alabama at Birmingham, Alabama 35294-1170, 2013.
[16] Daryabar F, Dehghantanha A, et All, A Survey About Impacts of Cloud Computing on Digital Forensics International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94, The Society of Digital Information and Wireless Communications, (ISSN: 2305-0012), 2013.
[17] Shirkhedkar D, Patil S, Design of digital forensic technique for cloud computing, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 6, ISSN: 2321-7782, 2014.
[18] Zimmerman S,and Glavach D, "Cyber Forensics in the Cloud," *IA Newsletter*, vol. 14, no. 1, pp. 4-7; http://iac.dtic.mil/iatac/download/Vol14_No1.pdf, 2011.
[19] Zatyko K & Bay J , The Digital forensics cyber exchange principle, Forensics Magazine, pp.5-13, 2011.
[20] Anwar,N, Riadi,I, Luthfie,A, Forensic SIM Card Cloning Using Authentication Algorithm, IJEIE, Vol. 4, No. 2, pp. 71-81,2016.
[21] Taylor M, Haggerty J, Gresty D, Lamb D, Forensic investigation of cloud computing systems. Network Security, (3):4–10, 2011.
[22] McKemmish R, What is forensic computing? Trends & Issues in Crime and Criminal Justice;118:1–6, 1999.
[23] Kent K, Chevalier S, Grance, T., & Dang, H., Guide to Integrating Forensic Techniques into Incident Response. In National Institute of Standards and Technology (Ed.) (Vol. 800-86): U.S. Department of Commerce,2006.
[24] Reilly D, Wren C & Berry T, Cloud Computing: Forensics Challenges for Low enforcement, International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2010.

Investigation on the Services of Private Cloud Computing by Using ADAM Method

ORIGINALITY REPORT

3%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.forensicmag.com Internet	52 words — 1%
2	files.eric.ed.gov Internet	21 words — < 1%
3	www.netsatellitetv.com Internet	17 words — < 1%
4	www.hfes.org Internet	10 words — < 1%
5	attorneyoneill.com Internet	10 words — < 1%
6	adkaptein.nl Internet	9 words — < 1%
7	"2015 Cloud Business Intelligence Market Study Now Available From Dresner Advisory Services.", Internet Wire, March 31 2015 Issue Publications	8 words — < 1%
8	Hala Albaroodi, Selvakumar Manickam, Parminder Singh. "CRITICAL REVIEW OF OPENSTACK SECURITY: ISSUES AND WEAKNESSES", Journal of Computer Science, 2014 Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		