DESIGN FRAMEWORK OF DIGITAL FORENSIC FOR CLOUD COMPUTING: A REVIEW

[1]SONAL SAOKAR, [2]SULABHA PATIL, [3]RAJIV DHARASKAR

[1]Student Mtech. 3rd Sem. CSE TGPCET Nagpur India
[2]Head Mohan Gaikwad Inventions & Research , TGPCET Nagpur India
[3]Director, Disha Group of Institutions, Raipur
E-mail: [1]saokar.sonal@gmail.com, [2]mgirc@tgpcet.com, [3]rajiv.dharaskar@gmail.com

Abstract- Digital forensics is the need of time for increasing cloud computing era. At the moment digital forensic is limited to standard traditional way of doing it to local machine and local storage. Cloud computing makes it more complex for forensics as the mode of storage has been changed and large dataset has been generated. Even in cloud computing forensic has been limited to extract the data from cloud and then process at local. We are proposing a framework to perform the forensic at the cloud environment. This will make investigators to build their custom workflow on cloud data and process on cloud. The expected result shows the improvement in analysis time.

Keywords- Cloud Computing; Digital Forensics.

I INTRODUCTION

Cloud Computing is considered as collection of clouds in World Wide Web, to provide technology enabled services cloud computing utilizes internet [4]. National Institute Of Standard and Technology (NIST) defines Cloud computing as " A model for enabling convenient, on computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released interaction". [5]

Now a day cloud computing is readily adopted by business houses and IT organizations for its unique features like convenient pay as you go services, high degree of scalability and low cost computing [3].The cloud model is composed of five essential characteristics, three service model and four deployment model [6]

Essential Characteristics:-

- On demand self – service.
- Broad network access.
- Resource pooling
- Rapid elasticity
- Measured service.

Service model:-

- Software as service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as service (IaaS)

Deployment model:-

- Private cloud.
- Community cloud
- Public cloud
- Hybrid cloud

Business organization use cloud computing for their huge data storage and computing demands, therefore the data security mechanism in cloud are necessary. Cloud in itself is connected through internal network, the business organization and other end users , uses cloud through external network. Hence cloud computing system is easy target for hackers, and other unethical online intruders. Hence digital forensic is an integral part of cloud forensic solutions.[7]

National Institute Of Standard and Technology (NIST) defines Digital forensic as " an applied science to identify an incident, collection, examination, and analysis of evidence data". [3] Digital forensic expert collect the data, process, and analyze data to investigate and prove digital crime in court of law. Traditionally digital forensic use to analysis hard drive, and flash drive which are physical storage device, but with innovative storage technologies coming in market every day processing and analysis of digital data becomes more and more complex [2]. Data acquisition, examination , analysis and reporting are the four classified phases of digital forensic. In a court of law digital forensic investigator are requested to classify the data analysis and examination process to validate trustworthiness of evidences, this is why digital forensic investigator must have updated knowledge of process and suitable tool sets used for investigation [4]
Digital forensic investigator faces four main challenges while performing investigation [7]

- Examiner don't have access to physical storage of data, so they are unable to trace the information
- Investigation tools are not easy to deploy on cloud and its configuration over different cloud architecture make it complex for configuration.
- Lack of interoperability among software
- Antiforensic technique.

The current forensic research related to cloud is limited to collection of data from cloud and perform it locally. Researchers have made efforts to make forensics cloud but this does not allow examiners to build their custom workflow analysis over cloud. Our main objective is to fill this gap and provide examiners a platform to handle such dynamic large dataset. We are designing a framework which makes examiners to deal with large dataset, software sharing and easy to deploy investigating tools. The framework allows the investigators to define their requirement in schema supported with collection of investigating applications.

The rest of this paper is organized as follows. Related work are discussed in Section II. Section III presents the proposed system. Section IV explain the algorithm and techniques. Section V concludes the paper.

II. RELATED WORK

There is rapid growth in the use of cloud base computing in recent years. Market research states that market of cloud computing will grow at rate 30% CAGR (Compounded annual growth rate) and will reach upto $270 billion in 2020.[3] There is difficulty in examining and analyzing log evidences as they are in heterogeneous format in cloud. Guidelines to over come this problem are disused in [8]

MapReduce is most popular programming model in cloud [9] it is associated with processing large data set in parallel on cluster of commodity server. For MapReduce application , the author[10]proposed and optimized cluster file system. Today's forensic tools will have to be updated or upgraded so that they fit into cloud framework [11].FROST- Forensic tools for open stack cloud are discussed in [12]. Through forensic tools it is possible to recover data from cloud instances, imaging of instances and data collection from cloud are possible discussed in paper [13].Forensic tools like Sleuth Kit, Digital Forensic framework, FTK, Encase etc. are used to analysis single drive but cloud formation is of number of nodes therefore multidrive correlation analysis becomes necessary. Cross drive analysis and forensic features is introduced in [14]. Volunteer cloud[15][16], Nebula cloud [17], Social Cloud [18] are different type of community cloud which were studied but no one of them specifically deals with digital forensic. One size fit all approach would not work for domain specific application because often customized solution built on top of cloud infrastructure are required for domain specific application.

On the top of Hadoop using MapReduce Apache Pig[19]is a platform for analysis large data set due to substantial parallelization Apache Pig handles very large data set. suspicious data can be extracted from Disk images, files, directories, by scanning Bulk extractor[20].The investigation function are provided by comprehensive tools like FTK, [21], OSForensic[22], Intella[23]but this are stand alone software which are used on local machines.

In Sleuth Hadoop[24] analysis work flow is fixed which is unable to configure and construct work flow dynamically. Sleuth Kit[25] has a cloud based version. To investigate disk images collection of command line tools s used by investigator referred as The Sleuth Kit(TSK). This command line tools (The Sleuth Kit(TSK).) allows investigator to incorporate plug-in framework which analyzes file content and build automated system.

Traditionally organization uses cloud computing for Disaster Recovery when routine interruption to services such as hardware failure, security breaches, and power line cut happens. Disaster recover can be carried out by data replication technique which is implemented on virtual machine (VM) in cloud based computing. By extracting last Restore Point (RP) data can be maintained, protected, and replicated using disaster recovery technique on a virtual machine.[26]
In digital forensic collecting digital evidences is very difficult due to inaccessibility of physical storage system. When data is on virtual machine if it s volatile in nature, data is lost when virtual machines are turned off. Due to this all data is lost and investigator cannot get image of instance. Live forensic are proposed system to detect attack like DDos attack and unauthorized file sharing[5]

The most popular operating system used in smart phones, tablets, gaming devices, televisions is Android Operating system (OS). There is unavailability of investigating tools, and limited knowledge regarding forensic in android system. The author proposed [27] efficient forensic framework for extraction of evidence from android device and also maintain the documentation.

III. PROPOSED SYSTEM

Forensic cloud is made up of two distinct layers, i.e. service layer and physical resource layer
Service layer is composed of three parts

- Forensic Data Manager
- Forensic Application Manager
- Forensic Workflow Manager

Physical storage layer consist of physical device and cloud storage [1]
Forensic Data Manager: Antiforensic approach which is referred as "Circular reference" is mitigated by forensic data manager which flattens all the directory information into one folder.
Forensic Application Manager : Application manager tags all the software required for the forensics in the app store and maintains the metadata about the

software. It generates the schema file periodically which can be used to generate user friendly web forms maintained by workflow manager and to validate XML schema.

Forensic Workflow Manager: workflow schedules all the jobs sent by investigator. The workflow manager splits the job into tasks and perform the scheduling in a sequence manner.[1]

IV. TECHNIQUES AND ALGORITHMS

HBase:- the meta data which contains useful data for files (directory structure) is maintained by data manager in HBase.[1]
MapReduce :- MapReduce programming model is associated with implementation for generating and processing large dataset on a cluster. [9] A MapReduce program is composed of a Map procedure that performs filtering and sorting and a Reduce procedure that performs a summary operation.

CONCLUSIONS

We have proposed the digital forensics technique that can be applied directly over cloud data. This includes workflow management scripts to be written directly on cloud. We have applied the technique of MapReduce which will be used to perform efficient data analysis on big data set. The expected outcome of the research is the digital forensic framework.

REFERENCES

[1] Yuanfeng Wen, Xiaoxi Man, Khoa Le and Weidong Shi *CLOUD COMPUTING 2013*

[2] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," National Institute of Standards and Technology, Tech. Rep.

[3] Shams Zawoad, Ragib Hasan, and Anthony Skjellum "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics", Department of Computer Science, University of Houston, 2015.

[4] Mahmoud M. Nasreldin, Magdy El-Hennawy, Heba K. Aslan and Adel El-Hennawy " Digital Forensic Evidence Acquisition and Chain of Custody in Cloud Computing" Volume 12, January 2015.

[5] Deoyani Shirkhedkar, Sulabha Patil, "Design of digtal forensic technique for cloud computing" IJARCSMS volume 2 june 2014.

[6] Cody Miller, Dae Glendowne, David Dampier and Kendall Blaylock "Forensicloud: An Architecture for Digital forensic Analysis in the Cloud" Journal of cyber security, Vol. 3 , 231-262, 2014

[7] Saibharath S.,Geethakumari G."Cloud Forensic: Evedance Collection and Preliminary Analysis" IEEE 2015.

[8] R. Marty, "Cloud application logging for Forensic" in Proceedings of ACM Symposium on Applied Computing, 2011 pp. 178-184.

[9] J. Dean and S. Ghemawat, "Mapreduce: simplified data processing on large clusters," Commun. ACM, vol. 51, Jan. 2008, pp. 107–113.

[10] R. Ananthanarayanan, K. Gupta, P. Pandey, H. Pucha, P. Sarkar,M. Shah, and R. Tewari, "Cloud analytics: do we really need to reinventthe storage stack?" in Proceedings of the 2009 conference on Hot topics in cloud computing, ser. HotCloud'09. Berkeley, CA, USA: USENIXAssociation, 2009.

[11] Keyun Ruan et al, "Survey on cloud forensic and critical criteria for cloud forensic capability: A preliminary analysis", 6th ADFSL Conference on Digital Forensic, Security and Law, USA.

[12] J Dykstra and AT Sherman, " Design and Implementation of FROST : Digital forensic tools for the OpenStack Cloud Computing Platform",13th Annual Digital Forensic Research Workshop 10, S87-S95.

[13] Saibharath S. Geethakumari G "Design and Implementation of a Forensic Framwork for Cloud in OpenStack Cloud Platform", International Workshop on Cloud Security And cryptography (cloudCrypto'14), Greater Noida, India. August 2014

[14] Simon L. Garfinkel, " Foremsic feature extraction na dcross drve analysis ", Elseever digital Investigation 3S (2006) S71-S81

[15] S. Distefano, V. D. Cunsolo, A. Puliafito, and M. Scarpa, "Cloud@home: A new enhanced computing paradigm," in Handbook of Cloud Computing,B. Furht and A. Escalante, Eds. Springer US, 2010, pp. 575–594.

[16] S. Caton and O. Rana, "Towards autonomic management for cloud services based upon volunteered resources," Concurrency and Computation: Practice and Experience, 2011.

[17] A. Chandra and J. Weissman, "Nebulas: using distributed voluntary resources to build clouds," in Proceedings of the 2009 conference on Hot topics in cloud computing. USENIX Association, 2009.

[18] S. Xu and M. Yung, "Socialclouds: Concept, security architecture and some mechanisms," in Trusted Systems, ser. Lecture Notes in Computer Science, L. Chen and M. Yung, Eds. Springer Berlin / Heidelberg, 2010, vol. 6163, pp. 104–128.

[19] "Apache Pig," http://pig.apache.org//, retrieved April 2013.

[20] "Bulk Extractor," https://github.com/simsong/bulk extractor/wiki/Introducing-bulk extractor, retrieved April 2013.

[21] "FTK (Forensics Toolkit)," http://www.accessdata.com/, retrieved April 2013.

[22] "OSForensics," http://www.osforensics.com/, retrieved April 2013.

[23] "Intella," http://www.vound-software.com/, retrieved April 2013.

[24] "Sleuth Hadoop," http://www.sleuthkit.org/tsk hadoop/, retrieved April 2013.

[25] "The Sleuth Kit," http://www.sleuthkit.org/, retrieved April 2013.

[26] Anand Padwalkar, Sulabha Patil, Neha Mogre, "Designing an Application for Recovery of Data in Cloud Environment: A Problem Definition.", IJARCSMS , Vol 3 feb 2015, pg. 291-295.

[27] Rizwan Ahmed, Dr. Rajiv Dharaskar, Dr. Vilas Thakre," Digital Evidence Extraction and Documentation from Mobile Devices", IJARCCE vol 2, issue 1, Jan-2013.

★★★