DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5373

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

SECURE LOG FORENSICS AS A SERVICE IN CLOUD COMPUTING

Varsha Tak
Dept. of CSE, Sardar Patel University of Police,
Security & Criminal Justice,
Jodhpur, India

Rajendra Kachhwaha
Dept. of CSE,
MBM Engineering College, Jai Narain Vyas University,
Jodhpur, India

Ram Niwash Mahia
Dept. of ECE,
MBM Engineering College, Jai Narain Vyas University,
Jodhpur, India

Abstract—With the advent of internet and technology, cloud computing is globally acceptable for each and every service in the industry. With this huge escalation in implementation, the cloud environment is exposed to an attacker with a large attack surface. So there is an emergent requirement to facilitate forensic investigators to collect, analyze and produce evidence from the cloud environment, which can be used in court cases. Logs maintain useful data regarding activities or events of system, network. This information is very expensive to prove attacks in court cases. So, protection is required and also maintained integrity, confidentially, security of logs. To collect and analyze log messages from different sources like a router, switch, virtual machine, firewalls, operating system. These logs are categorized with a regular expression and to store in particular encrypted format. To overcome threads cost and improve security, an organization should be moved towards the cloud. Using cloud-based log forensics, investigator easily gathers the log and conduct investigation. In cloud computing environment they also used in forensics to prove attacks and increase confidentiality.

IndexTerms—Cloud Computing, Cloud Security, Log Management, Cloud Forensics, Log Forensics

I. INTRODUCTION

Cloud computing is a computational model in which on-demand resources are provided with storage at a very low cost, in a very elastic and efficient manner. As a cloud user performs various activities as per requirement in the cloud environment and those activities got recorded in log files. The process of this recording is known as logging. Log files provide multiple information regarding user activity, servers, networks, operating systems, firewalls etc. Using Log files, we can optimize the performance of the system or network, perform network monitoring and investigate the malicious behavior [1]. This information is very useful for cloud forensics. This paper discusses the log generated at various events which plays a big role in the investigation and securing the cloud infrastructure. Section II defines the various logging modes and types of logs details such as user activity details, server, and network activities in the cloud. In section III and IV architecture model of cloud computing and forensics is defined. Section V discusses the previous related work in this field. Section VI derives the conclusion.

II. VARIOUS KINDS OF LOGS

Log files contain sequential steps performed during the execution and stored in different logging methods. Logging is mainly used for monitoring the system and can be used for investigation purpose. There are different types of logging methods such as linear logging and circular logging.

A. *Linear Logging*

This is used to store the log files in a linear sequential manner in system memory. Linear logging has infinite memory space of system memory. Logs are stored without overwriting the previous logs. Whenever system memory exhausted, old log files are moved to another memory.

B. *Circular Logging*

In this, log files are stored in a circular manner same as a circular queue. It is used to predefine memory space once it reaches the end of the location; it automatically performs the overwriting from the starting point and then starts storing the new files. To acquire the previous and past logs, it is necessary to identify which types of logging technique is used and also check log file format.

There are different types of sources where a user can gatherers log such as virtual machine logs, firewall logs, network logs, setup logs, system logs and application logs.

III. CLOUD COMPUTING ARCHITECTURE

A cloud computing provides virtual space to store data and also provides access from anywhere. In cloud computing, we highly depend on CSPs to gain logs and forensic investigation from clouds [2][9]. Logs are based on three models of the cloud: SaaS, Paas, and Iaas [9].

A. Software as a Service(SaaS)

All the services and application resources are provided by Cloud service provider. Cloud consumers have no control on the SaaS platform. A user can only manage the provided resources as per his convenient. Cloud users have the least control in SaaS to get application log as compare to others model [9].

B. Platform as a Service(Paas)

Cloud service provider provides a platform and using that platform user can deploy their applications and software in the cloud. In this, network and operating system management are not allowed to the cloud user. In this model only possible to get application logs, to acquire others logs we need to depend on CSPs [9].

C. Infrastructure as a Service(Iaas)

In this, the systems in terms of the operating systems, applications, storage, and network connectivity, are managed and controlled by consumers. To decompose the physical resources in an ad-hoc manner to meet the demand of the resources from cloud consumers, virtualization is extensively used [4]. In this model, we get the virtual machine image from the customer and we can perform analysis and examination [9].

IV. CLOUD FORENSIC ARCHITECTURE

With the rising fame of cloud, the attack and security concerns are also increasing as it lacks support for security and forensic investigations [5].

Cloud forensic is the combination of memory forensics and network forensics. Memory forensics is used to calculate integrity and retrieval of deleted files while network forensics is used to obtain external and internal IP addresses of cloud components [3]. The digital forensic process involves following phases: identification, collection, examination, analysis, reporting with the presentation [8], as shown in Figure 1.

A. Identification

Any malicious activity such as deletion of files, illegal use of storing files, tampering with files in a malicious way etc. are detected by identification method. Identification is the first step to start forensics process [6]. Digital evidence is identified in this first process. Cloud evidence is classified as the document stored on cloud servers, different activity records which are obtained using logs, image of virtual machines, cloud service API calls etc. and to collect those evidence there are different techniques in cloud such as remote data acquisition, management plane acquisition, live forensics and snapshot analysis [6]. Identification process involves two steps: incident identification, and evidence identification. Incident identification process gives details about any suspicious activity from any side i.e. user or service provider while evidence identification tells about the evidence which can be presented in the court i.e. mobile phones, network devices etc [6].

B. Collection

Collection phase includes identification, labeling, recording and acquiring forensic data [7]. Data collection is a very crucial phase in forensics analysis in the cloud as to collect data in the cloud is a very tedious task. In cloud environment digital evidence are present and seizure of that evidence is about to impossible as to seize the cloud servers or storage devices contain the huge number of hardware and data always flows from one jurisdiction to another jurisdiction which makes data collection process complex.

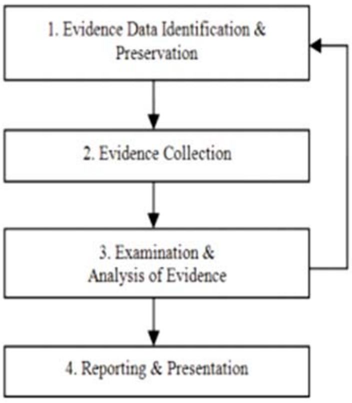
1. Evidence Data Identification & Preservation
2. Evidence Collection
3. Examination & Analysis of Evidence
4. Reporting & Presentation

Figure 1. Cloud Forensics Process

C. Examination

In the examination phase, as per type of data, suitable forensic tools and techniques are applied to identify and extract the relevant information from the collected data [17][20]. This phase plays a vital role in getting the relevant information with integrity check. To put the original information in front of the court at the time of jurisdiction, a fair examination is required to that information which is done in this phase.

D. Analysis

As per NIST, “It involves the analysis of the examination result, to take out the useful information that addresses the questions” [16]. As per examination report, an analysis is done to extract relevant information.

E. Reporting with Presentation

In this phase, using all the findings, a detailed report is created. After that, the report is submitted to the admissible court.

V. LITERATURE REVIEW

This section describes a review of available literature and techniques used for secure log and management.

Syslog was acquainting by Computer Science Research Group (CSRG) [18].The aim to design the syslog is to handle the system activities. These activities are stored in log files which are collected by a process. Administrators have the ability to view the log files and keep track of the system status [10]. Syslog messages are separated into PRI (priority), HEADER and the MSG, this format is defined in RFC3164 [10]. It uses UDP protocol for delivery of log messages. Due to disadvantage, it is replaced with the Syslog-ng [11]. Syslog-ng can send and receive a log message over TCP which provides reliability. It uses reliable Log Transfer Protocol that secures messages, lost during connection breaks and also makes sure that duplicity of the messages at the receiving end due to connection lost. Syslog-ng doesn’t secure log data modifications [13]. Syslog-sign is an additional enhancement into syslog which provides authentication, message sequencing, and integrity and also identify the missing messages using certification and signature block [13][12]. Syslog-pseud proposes a logging architecture to provide the pseudo names to the log file [13][15]. The main idea is that first log records are processed by a pseudonymizer which is used to provide pseudo names to log files, before being archived [13][15]. It identifies characteristics from specific fields in the log record and substitutes them with their pseudo names but correctness of log records does not ensure [14]. Syslog is basically used for information gathering and analysis phase of the forensic steps. But still, there are log management problems in the forensic process. To overcome this problem organizations are moving towards cloud computing to use cloud logging service [1]. Cloud computing log includes cloud application log, cloud network log, cloud system log, cloud firewall log and so on. Nowadays attacks are performed by attackers very frequently on the cloud which decreases trust among users on the cloud. Amna Eleyan et al. [5] define the forensic service environment where investigators identify various threads and vulnerabilities and attacks. A secure handover of collected and stored log data to the investigator is performed by cloud service provider [5]. Investigator uses various tools, techniques, and algorithms to determine vulnerabilities inside the log files. Cloud service provider uses encryption method to make original data invisible to the attacker. Ma D et al. [19] defined an innovative method of secure logging using authentication, which improves security. The author defined two features which are used in forwarding secure sequential. In which first, one cannot do any changes after generation. Second, it provides integrity protection to the whole message body and also satisfied correctness. Ameer Pichan et al. [20] identified collision between cloud service provider (CSP), Cloud users and investigators in cloud forensics [20]. Cloud forensic is totally depended on logs because log files record different activities on system and network. The real-time log forensics is helpful to find problems immediately. Log files are able to solve a problem regarding existing attack and also used to investigate different attacks.

VI. CONCLUSION

Log messages play a vital role for any organization to conduct network security and identify any malicious behavior. They play a big role to know about the attacks and secure the cloud environment. As cloud becoming attractive day by day and every organization is stepping forward to adopt the cloud, the number of threats is also increasing. To know about the existing threats and if in some case an attack takes place then to know about the reasons for that attack; log files provide much important information. There are multiple techniques which are adopted by cloud providers which are also very helpful to submit clues in the court cases.

REFERENCES

[1] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Muhammad Shiraz, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya, “Cloud log forensics: Foundations, state of the art, and future directions” 2016, ACM Computing Survey, vol.49, no. 1, article 7, May 2016.

[2] Jason Farina, Mark Scanlon, Nhien-An Le-Khac, M-TaharKechadi, “Overview of the Forensic Investigation of Cloud Services”, in a 10th International conference on Availability, Reliability, and Security (ARES), Aug. 2015.

[3] Saibharath S, Geethakumari G, “Design and Implementation of a forensic framework for Cloud in OpenStack cloud platform”, in International conference on Advances in Computing, Communications and Informatics (ICACCI), Sep. 2014.

[4] Santosh Kumar and R. H. Goudar, “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey”, in International Journal of Future Computer and Communication (IJFCC), Dec. 2012, vol. 1, no. 4, pp. 356-360.

[5] Amna Eleyan, Derar Eleyan, “Forensics process as a Service (FPaaS) for cloud computing”, in European Intelligence and Security Informatics Conference (EISIC), pp. 157-160, Sep. 2015.

[6] Changwei Liu, Anoop Singhal, Duminda Wijesekera, “Identifying Evidence for Cloud Forensic Analysis”, in International conference on Digital Forensics: Advances in Digital Forensics XIII, Springer, vol. 511, pp. 111-130, Aug. 2017.

[7] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, “Cloud Forensics”, in International conference on Digital Forensics: Advances in Digital Forensics VII, Springer, vol. 361, pp.35-46, 2011.

[8] Sathishkumar Easwaramoorthy, Sankar Thamburasa, Guru Samy, S. Bharath Bhushan and Karrothu Aravind, “Digital Forensic Evidence Collection of Cloud Storage Data for Investigation”, in International conference on Recent Trends in Information Technology (ICRTIT), April 2016.

[9] Shams Zawoad, Amit Kumar Dutta, and RagibHasan, “Towards Building Forensics Enabled Cloud through Secure Logging-as-a-Service”, IEEE Transactions on Dependable and Secure Computing, 2015.

[10] Jian-hua Huang, Yuan-long Jiang, Man-qi Zhang, “The design and implement of the centralized log gathering and analysis system”, in International Conference on Computer Science and Automation Engineering (CSAE), May 2012

[11] BalaBit IT Security, http://www.balabit.com/network-security/syslog-ng. Last access 2017.

[12] J. Kelsey, J. Callas, and A. Clemm, Signed Syslog Messages, Request for Comment RFC 5848, Internet Engineering Task Force, Network Working Group, May 2010.

[13] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, DieudonneMulamba, and MariappanRajaram, “Secure Logging As a Service - Delegating Log Management to the Cloud”, IEEE Systems Journal, June 2013, vol. 7, no. 2, pp. 323-334.

[14] Deepalakshmi A., Mohanraj. T, “Cloud-based Secure Log Management using Homomorphic Encryption to reduce Communication Overhead”, International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), March 2014, vol. 2, pp. 1525-1528.

[15] Prasad P Kharade, S.B.Natikar, “A Survey on Secured Logging in the Cloud”, International Journal of Research in Engineering and Technology (IJRET), July 2014, vol. 3, no. 7, pp. 151-153.

[16] The NIST. https://www.nist.gov/. Last access 2017.

[17] Computer Forensics Investigation – A Case Study; http://resources.infosecinstitute.com/computer-forensics-investigation-case-study/gref.

[18] https://www.icsi.berkeley.edu/. Last access 2017.

[19] Ma D, Tsudik G. “A new approach to secure logging”, ACM Transactions Storage (ATOS), March 2009, article 2, vol. 5, no. 1.

[20] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh, “Cloud Forensics: Technical challenges, solutions and comparative analysis”, Digital Investigation: The International Journal of Digital Forensics & Incident Response, Volume 13, June 2015, Pages 38-57.