Secure Cloud Log for Cyber Forensics

Aditya Vanjari
NBN Sinhgad School of Engineering

Shubham Sahare
NBN Sinhgad School of Engineering

Amar Sawant
NBN Sinhgad School of Engineering

Shubham Wasade
NBN Sinhgad School of Engineering

Abstract

Nowadays cloud computing has become a popular computing paradigm. There is a lack of support for cloud forensic investigation in cloud computing. The vital role in cloud computing is to analyze various logs (e.g., network log or process log or activity logs). Hence log is a valuable information source in investigations of cloud forensics. There are many other existing sources for secure log storage designed for the typical ordinary system instead of the complexity in the cloud environment. Therefore our team is proposing an another scheme for secure log data in the cloud environment.

In our proposed system we have been encrypted various log files using the unique public key of the user so that the content cannot be decrypted by other users. In order to prevent modifications of a log for unauthorized, due to such approach, the verification time can be reduced significantly.

Keywords-*Cloud Forensic; Cloud Log; Cloud Computing; Cloud Security; Proof of past log.*

I. INTRODUCTION

Cloud computing is a complex model in which provides on-demand resources with little cost for storage, in a very efficient and flexible manner. As a cloud user performs various activities as per requirement in the cloud environment and those activities got recorded in log files. The method of this recording called as logging. Log files avail various information related to user activity, cloud servers, the networks, OS, and firewalls. Using these Log files, we can optimize the system performance network, and later perform network monitoring and to probe the malicious behavior. This info is beneficial for cloud forensics.

Cloud security, storage and privacy are well established areas for research. This is not surprising considering how cloud services are being adopted widely and the potential for its exploitation by criminals. Relatively speaking cloud forensics, interestingly, is a less understood topic. In cloud service, cloud server, a client device and other network infrastructure are compromised due to malicious cyber activity. Due to this, the host's illegal contents such as radicalization materials need to be analyzed using forensic analysis. As the cloud technologies have an inherent nature, digital forensic tools and procedures must be updated in order to retain the similar kind of applicability and usefulness in a cloud environment.

The remaining paper is organized as given below.

Section II summarizes the literature survey.

Section III introduction of the proposed methodology. Design in Section IV. Result and discussion in Section V. Section VI focuses on the conclusion.

II. LITERATURE SURVEY

In this section, we have discussed different papers referred, based on cloud computing as well as how the cloud logs can be secured and preserved.Proposed Secure Logging-as-a-Service (SecLaaS) [1], Author has set up some stockpiling virtual machines logs and allows legitimate access to criminological analysts ensuring the protection of the cloud clients. Notwithstanding that, SeclaaS supports past log evidence and as needs be secures the privacy of the cloud logs from invalid examiners or CSPs. In the long run, Author effectively decided the possibility of the work by systematizing SecLaaS for arrange signs in a haze of OpenStack.

Zhihua Xia *et al.* proposed a scheme for image retrieval image retrieval helped the data owner for out sourcing the image database[11] . Local sensitive has utilized for improving the search efficiency as well as two different stages were designed for the improvement of the efficiency for search, the first stage the unique images were filtered out by pre-filter tables, and the remaining image was compared one at a time by using EMD metric for refined search results in the second stage.

Here author [3] highlights the state-of-the-art digital forensics of cloud computing. They pinpointed when the term was used as a keyword in the literature with the aid of search engine SUMMON. A keyword is known as “cloud forensics" was used and Categories it in three main dimensions based as (1) survey (2) technology and (3) forensics-procedural. The aim in the paper is not just to refer the related work on discussed dimensions but to analyze those dimensions and identify research gaps with the help of generating a map.

In [4] Indrajit Ray *et al.* drafted a thorough scheme which addressed the integrity and security issues not just during the phase of log generation, but also during the log management process like including log transmission, collection, retrieval and storage. Outsourcing log management to cloud used to arise for log privacy was the challenge. While storage or retrieval log should not be traceable, so that logs can be used or network to provide anonymous protocols on logs in the cloud.Developed protocol has the potential for usage in various areas.

Ben Martini *et al.* [5] proposed an integrated conceptual digital forensic framework which gives particular importance to the preservation of forensic data and the collection of cloud computing data forforensics. The overarching framework for conducting digital forensic investigations in the cloud computing environment, they even stated that there must be further research to develop a library of digital forensic methodologies that would best suit the various cloud platforms and deployment models[12 13].

In another work, Alecsandru Patrascu *et al.* [6] drafted a novel solution which provided investigators of digital forensic a reliable and secure method for monitoring activities of users in cloud infrastructure. Hence they mainly focused on the various field like to increase the security and safety as well as reliability of the cloud. Authors even proposed a model which allowed investigators to seamlessly analyze workloads and virtual machines while preserving scalability of large scale distributed systems.

Lightweight hypervisor introduced in [7] to acquire and preserve data for reliable live forensics. In three ways the reliability is improved: the lightweight architecture, the data acquisition mechanism, and the evidence protection mechanism. Unused device drivers are eleminated to reduce the TCB size, thereby decreasing the vulnerability of our hypervisor.

III. PROPOSED METHODOLOGY

An exploitative cloud client can assault a cloud framework outside it. He/She can likewise assault any kind of application sent in a similar cloud. An assault can be dispatched on a node controller used to control all the activities in a cloud. The log from the node controller (NC) is taken by CLASS plot (Fig. 1) in a virtual machine (VM), and its substance is concealed, and is stored in a database. These storage permits the logs can open up for additional examination nottwithstanding Virtual Machine shutdown. Also, Cloud Log Assuring Soundness and Secrecy distributes its verification with the goal that log honesty secured and suitability guaranteed. An essential term of our proposed system is defined initially. At that point assailant's capacity, potential assaults on the logs and the properties of security of a protected cloud log administrations are given

A] Architecture of Proposed Scheme

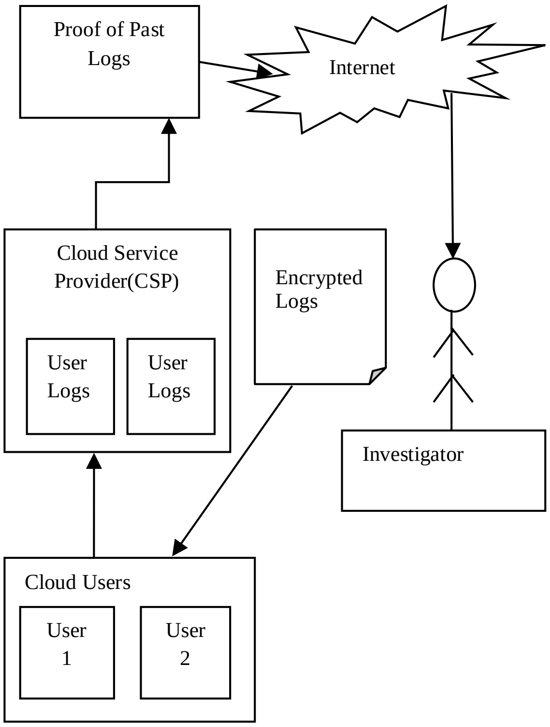

Fig. 3.1 Proposed Scheme

Log: Any generated log such as log about network, process log and OS log in the cloud for a VM can be a Log

• **Proof of Past Logs (PPL):**.The integrity of logs is ensured by proof of logs which is contained by PPL

• **Log Chain (LC):** The logs which are ordered in a chronological order for protecting them from reordering are maintained by LC

• **CSP:** Public Cloud Infrastructure is owned by CSP (Cloud Service Provider), PPL is generated by them, is made available publicly and exposes the Application Programming Interface to collect log data.

- **User:** He/She can be malicious or honest person who may be a client of CSP who can take scape from VMs on rent from CSP.

- **Investigator:** He/She is an expert in professional forensics. He/She collects the required log data from the cloud infrastructures if any malicious incident occurs.

- **Auditor:** Verifying the log's correctness by making the use of PPL and LC will be done by the court authority, i.e. an Auditor who will perform these activity

- **Intruder:** It might be any malicious person. They could be the insiders from the Cloud Service Providers who might want to leak the user activity from the Proof of Past Logs or the logs stored on the cloud.

IV. RESULT AND DISCUSSIONS

The proposed system uses a symmetric key encryption technique to avoid the leakage of any cloud logs in the system. The proposed system executes in various phases to compare with the previous schemes such as log processing and log verification. The first phase consisted of three different steps: hiding of content, PPL and generation of log chains. By applying a symmetric key and user public key hiding of the content has been assured. Log chain generation collected the previous log and concatenated them with the current encrypted logs. Sample from 4 MB to 6 MB are analyzed and compared the processing time of execution, the received result was nearly by same in some cases. The verification time of the system is lesser than compared to Secure Logging as a Service. The bloom filter concepts were used in secure logging where it inserts each entry of log in separately. In the proposed system, we have concatenated the current logs to the previous log. Hence the time taken by the system to verify the logs is less as compared to the previous system.

	Processing time in milli-seconds for 4MB log file	Verification time in milli-seconds for number of log entries around 55000
Existing	99.48	480
Proposed	99.01	380

Table 5.1 - Expected Result Analysis Table

ISSN: 2233-7857 IJFGCN

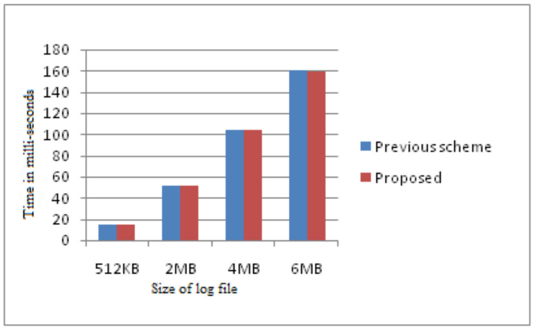

Fig 5.2 : - Time for log processing.

V. CONCLUSION

To execute a successful forensics investigation in clouds, the proposed system uses CSPs to collect logs from different sources. The system uses secure logs for the cloud which is a solution to store and provide logs for forensics purpose securely. Also, provide privacy of cloud users by encrypting cloud logs with a public key of the respective user while also facilitating log retrieval in the event of an investigation. This scheme allows CSPs to preserve the confidentiality of cloud users while storing the logs. Additionally, the integrity of the logs can be checked by an auditor using the Proof of Past Log (PPL).This cloud logs can be securely used for cyber forensics.

REFERENCES

[1] Shams Zawoad; Amit Kumar Dutta; Ragib Hasan,” Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service,”IEEE Transactions on Dependable and Secure Computing, 2015

[2] Zhihua Xia, Xingming Sun, Zhan QinandKui Ren, “Towards Privacy-preserving Content-based image retrieval in Cloud Computing,” IEEE Transactions On Computer Computing, September 2015.

[3] Sameera Almulla, Youssef Iraqi, and Andrew Jones,”A State-of-The-Art Review of Cloud Forensics,”Research Gate, Article · December 2014.

[4] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram,“ Secure Logging As a Service—Delegating Log Management to the Cloud,” IEEE Systems Journal, 2013.

[5] Ben Martini, Kim-Kwang Raymond Choo,“An integrated conceptual digital forensic framework for cloud computing,”Digital Investigation, vol. 9, pp.71-80,2012.

[6] Alecsandru Patrascu, Victor-Valeriu Patricia,” Logging System for Cloud Computing Forensic Environments,”Journal of Control Engineering and Applied Informatics, vol. 16, pp. 80-88, 2014.

[7] Zhengwei Qi, Chengcheng Xiang, Ruhui Ma, Jian Li, Haibing Guan, and David S. L. Wei, “Forensics ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics, ”IEEE Transactions on Cloud Computing, vol. 5, pp. 443-456, 2017.

[8] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, pp. 77-78, 2016.

[9] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84-96, 2017.

[10] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, pp. 77-78, 2016.

[11] Shwetambari Kharabe, C. Nalini," Robust ROI Localization Based Finger Vein Authentication Using Adaptive Thresholding Extraction with Deep Learning Technique", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018.

[12] Shwetambari Kharabe, C. Nalini," Using Adaptive Thresholding Extraction - Robust ROI Localization Based Finger Vein Authentication", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 13-Special Issue, 2018.

[13] Shwetambari Kharabe, C. Nalini," Evaluation of Finger vein Identification Process", International Journal of Engineering and Advanced Technology (IJEAT), International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S, August 2019.