RESEARCH ARTICLE OPEN ACCESS

A Survey on Cyber Forensics for Securing Cloud Logs

Amar Sawant, Aditya Vanjari, Shubham Sahare, Shubham Wasade

[1,2,3,4]Department of Computer Engineering, Nbn Sinhgad School of Engineering, Pune-41

--************************----------------------------------

Abstract:

These days cloud computing has become a mainstream processing worldview. There is an absence of help for cloud scientific examination in cloud computing. The essential job in cloud computing is to dissect different logs (e.g., organize log or procedure log or movement logs). Subsequently log can be a significant wellspring of data in cloud legal examination. There are numerous other existing secure for secure logging intended for the ordinary framework as opposed to the multifaceted nature of the cloud condition. Consequently we are proposing an elective plan for secure logs in a cloud situation. In our proposed framework different log records have been encoded utilizing the one of a kind client's open key with the goal that different clients can't decode the substance. To forestall alterations of a log for unapproved, because of such methodology, the confirmation time can be diminished altogether.

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

--************************----------------------------------

I. INTRODUCTION

Cloud computing is an intricate model wherein on-request assets are furnished with capacity at a little expense, in an entirely adaptable and proficient way. As a cloud client performs different exercises according to necessity in the cloud condition and those exercises got recorded in log documents. The procedure of this account is known as logging. Log documents give different data with respect to client action, servers, systems, working frameworks, firewalls. Utilizing these Log records, we can improve the framework execution organize, and later perform net work checking and research the malignant conduct. This data is valuable for cloud crime scene investigation.

Cloud storage, security, and protection are genuinely settled research regions, which isn't astonishing thinking about the far reaching appropriation of cloud administrations and the potential for criminal abuse (e.g., bargaining cloud records and servers for the taking of delicate information). Strikingly cloud legal sciences is a generally less gotten subject. In cloud administration, cloud server, a customer gadget and other system foundation are undermined because of malignant digital movement. Because of this, the host's illicit substance, for example, radicalization materials should be broke down utilizing criminological examination. Because of the inalienable idea of cloud innovations, regular advanced legal methodology and apparatuses should be refreshed to hold a similar helpfulness and appropriateness in a cloud situation.The rest of this paper is organized as follows. SectionIIsummariesthe literature survey. Section III introduces the proposed methodology. Section IV focuses on the conclusion.

Literature Survey

In this section, we have discussed differentpapersreferred, based on cloud computing as well as how the cloud logs can be secured and preserved. Drafted Secure Logging-as-a-Service (SecLaaS) [1], Author has put up some storage virtual machines logs and permits legal access to forensic examiners guaranteeing the privacy of the cloud customers. In additionto that, SeclaaS sustains past log proofand

accordingly protects the confidentiality of the cloud logs from invalid investigators or CSPs. Eventually, Author successfully determined the feasibility of the work by systematizing SecLaaS for network logs in a cloud of OpenStack.
Zhihua Xia*et al.*proposed a scheme for image retrievalimage retrieval helped the data owner for outsourcing the image database. Local sensitive hasutilized for improving the search efficiency as well as two different stages were designed to improve the search efficiency, the first stage the unique images were filtered out by pre-filter tables,and in the secondstage, the remaining image wascompared one by one by using EMD metric for refined search results.

Here author [3] highlights the state-of-the-art digital forensics of cloud computing. They pinpointedwhen the term was used as a keywordin 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 butto analyze those dimensions and identify research gaps with the help ofgenerating a map.

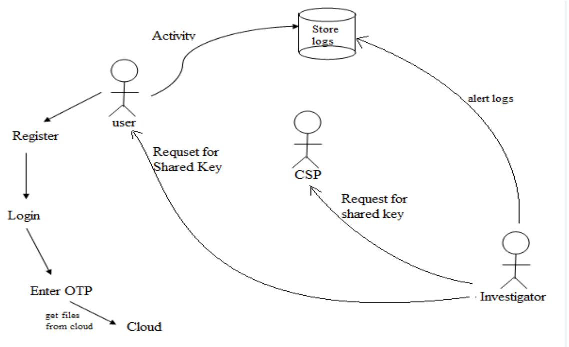
In [4] Indrajit Ray*etal.*drafted a far comprehensive scheme which tends to security and respectability issues during the log age stage, yet additionally during different stages in the log the executives procedure, including log assortment, transmission, storage,and recovery. Re-appropriating log the executives to cloud used to emerge for log security was the test. While capacity or recovery log ought not be recognizable, so logs can be utilized or system to give unknown conventions on signs in the cloud.Developed protocol has the potential for utilization in different zones.
Ben Martini*et al.* [5] proposed an incorporated theoretical computerized measurable system which gives specific significance to the protection of legal information and the assortment of distributed computing information forforensics. The all-encompassing structure for directing computerized criminological examinations in the distributed computing condition, they even expressed that there must be further research to build up a library of advanced legal systems that would best suit the different cloud stages and arrangement models.

In another work,AlecsandruPatrascu*et al.* [6]drafted a novel arrangement which gave examiners of computerized scientific a solid and secure technique for observing exercises of clients in cloud foundation. Consequently they primarily centered around the different field like to build the security and wellbeing just as unwavering quality of the cloud. Creators even proposed a model which enabled agents to consistently examine outstanding burdens and virtual machines while protecting adaptability of huge scale cloud frameworks.

Lightweight hypervisor introduced in [7] to obtain and protect information for dependable live legal sciences. In three different ways the unwavering quality is improved: the lightweight engineering, the information securing component, and the proof insurance system. Unused gadget drivers are eliminated to diminish the TCB size, along these lines diminishing the powerlessness of our hypervisor.

System Architecture

A dishonest cloud user can attack a system outside the cloud. They can also attack any application deployed in the same cloud, or an attack canbelaunch against a node controller which controls all the cloud activities. For a virtual machine (VM), CLASS scheme (Fig. 1) takes the log from the node controller (NC), hides its content, and stores it in a database. These storage allow logs to become available for further investigation despite VM shutdown. Moreover, CLASS publishes its proof so that log integrityprotected and admissibility ensured. An essential term of our proposed system is defined initially. Then attacker’s capability, possible attacks on logs, and the security properties of a secure cloud log services are provided.



System Architecture

Log: A log can be the network log, process log, operating system log, or any other log generated in the cloud for a VM.
• **Proof of Past Logs (PPL):** The PPL contains the proof of logs to ensure the integrity of logs.

- **Log Chain (LC):** The LC maintains the chronological ordering of logs to protect the logs from reordering.
- **CSP:** A Cloud Service Provider (CSP) is the owner of a public cloud infrastructure, who generates the PPL, makes it publicly available, and exposes APIs to collect logs.
- **User:** A user is a customer of the CSP, who rents VMs provided by the CSP. A user can be malicious or honest.
- **Investigator:** An investigator is a professional forensic expert, who needs to collect necessary logs from cloud infrastructures in case of any malicious incident.
- **Auditor:** Usually, an auditor will be the court authority that will verify the correctness of the logs using PPL and LC.
- **Intruder:** An intruder can be any malicious person including insiders from CSP, who wants to reveal user's activity from the PPL or the stored logs.

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 whichis a solution to store and provide logs for forensics purpose securely.Also, provideprivacy 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 store logs while preserving the confidentiality of cloud users. Additionally, an auditor can check the integrity of the logs using the Proof of Past Log (PPL).This cloud logs can be securely used for cyber forensics.

REFERENCES:

[1] Shams Zawoad; Amit Kumar Dutta; RagibHasan," 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, DieudonneMulamba, and MariappanRajaram," 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-ValeriuPatricia," 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 ReliableData 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.