Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 06, June -2019

SURVEY OF LOGGING MECHANISM FOR A CLOUD FORENSICS

Mrs.Aboli Deshpande[1], Dr. Jyoti Rao[2], Prof. Swati Nikam[3]

[1] *PG Scholar, Computer Engineering, DIT Pimpri pune.*
[2] *Associate Prof., Computer Engineering, DIT Pimpri pune.*
[3] *Assistant Prof., Computer Engineering, DIT Pimpri pune.*

Abstract — ***Cloud computing has emerged as a preferred computing paradigm these days. Existing cloud computing architectures usually lack support for forensics investigations. Analyzing different types of logs (e.g.application logs, network logs) and logging mechanism plays a vital role in forensic investigation. Storing and collecting logs from the cloud is very hard due to its multi-user whom shares the identical process and network resources.Useful data stored in User activity logs is proved to be usful in forensic investigations; keeping logs intact and trustworthy is crucial.In such environment providing secure logging system which maintains confindetiality, availability, and privacy so that it will helpful in investigation is challenging. Even different attacks and malicious behaviors can be detected by analyzing logs in the log file. The aim of this paper is to study different logging mechanisms in the existing literature which are designed for the cloud model and helps in forensic investigations.***

Keywords- *Cloud forensics, Cloud log, Log forensics, Cloud security,.*

I. INTRODUCTION

Cloud computing provides a large number of infrastructural resources, very easy pay-as-you-go service, and minimum cost computing. As a result, cloud computing has become one of the most preferred computing paradigms in the current era. Today, thousands of companies opt cloud computing services because it does not require any kind of fundamental infrastructure setup, and at the same time, it is highly cost saving scheme [1]. Cloud computing opens a new horizon of computing for business and IT organizations. However, at the same time, malicious individual scan easily exploits the power of cloud computing.

An attacker can attack applications running inside the cloud. Alternatively, they can launch attacks from machines inside the cloud. These issues are the primary concerns of Cloud Forensics. As a result, forensic experts are devising new techniques for digital forensics. There are several forensics analysis schemes and tools available in the market. Unfortunately, none of them are suitable for the dynamic nature of cloud computing. Due to the inherent nature of cloud technologies, conventional digital forensic procedures and tools need to be updated to retain the same usefulness and applicability in a cloud environment [2].

Unlike traditional client device, cloud virtual machines (VMs) can be supported by hardware so that can be located remotely and thus would not be physically accessible to a forensic expert. In addition, VMs can be distributed across multiple physical devices in a clustered environment or they can exist within a pool of VMs on the same physical components. Therefore, holding the machine for forensic analysis is not advisable in most investigations. Furthermore, data residing in a VM may be volatile and could be lost once the power is off or the VM terminates. Hence, the cloud service provider (CSP) plays a crucial role in the collection of evidential data (e.g. cloud user’s activity log from the log). For example, the CSP writes the activity log (cloud log) for each user. Thus, preventing modification of the logs, maintaining a proper chain of custody and ensuring data privacy is crucial.

II. LITERATURE REVIEW

Krati Mehto & Moriwal [3] discussed a various method of searchable encryption to secure the data in cloud storage. This scheme is for secure data accessing with maintaining its privacy by using a strong cryptographic algorithm. Proposed solution incorporates the hash table management and indexing techniques to keep track the actual data contents in terms of document features which may help for encrypting user data and identifying the user data and privacy. This paper addresses following issues like Data security, Data owner and client privacy management and Searchable data space in existing cloud storage and provide solution respectively Authentication management, Cryptographic data security, Providing the search solution over the encrypted data.

Shams Zawoad et al. [4] suggested Secure-Logging-as-a-Service (SecLaaS), which stores virtual machine’s logs and allowed rightful access to forensic examiners guaranteeing the privacy of the cloud customers. In addition to that, Seculars sustains past log proof and accordingly protects the confidentiality of the cloud logs from invalid investigators or CSPs.To determine the feasibleness of the work author successfully tested SecLaaS for network logs in a cloud of Open Stack.

Anwar et al. [5] proposed logging provided by the OS and the security logs. They set up a cloud computing environment Eucalyptus using Snort, Syslog, and Log Analyzer, they were able to audit the characteristic of Eucalyptus and to preserve all the logs of intrinsic and extrinsic cooperation of Eucalyptus objects. For their experiment, they launched a DDoS attack from two virtual machines and from the logs on the Cloud Controller (CC) machine; they were able to identify the attacking machine IP, browser type and content requested. To provide logs for a cloud in detecting cloud attacks and also it was possible to reconstruct an event that helped conduct a digital forensic investigation.

Ray et al. [6] presented a framework, where a logger or log accumulator will send a series of logs to the cloud server via some authenticated channel. Then, the cloud server will take steps to maintain confidentiality, integrity, verifiability, and the availability of secure logs. To protect logs from security breaches or privacy violation, they encrypt log entries with a chain of sequentially generated keys and to preserve integrity they use another set of keys generated in the same way. To prevent truncation error from both ends, they used a special type of logs on starting and ending points of each block of logs. However, there is no option for public verifiability due to the use of symmetric key encryption to protect confidentiality and privacy.

Ma and G Tsudik [7] proposed the concept of forwarding secure sequential aggregate (FssAgg). In this approach, two tags (known as FssAgg tags) are associated with each log entry, one is for the semi-trusted log accumulator and other is for the trusted verifier. Using FssAgg, they were able to achieve forward secure stream integrity instead of forwarding security. Also, the FssAgg tag can detect any log prior to it in a certain epoch. The last FssAgg tag of a batch can test the entire chain of log entries up to that batch. This leads to increased computational cost during the verification phase.

Tian et al.[8] recently proposed a scheme for public auditing of operational behavior in the cloud. For selective verification, they suggested block based logging. They also used widely recognized hash-chain schemes for forwarding security and append-only property. For log credibility introduced the idea of a trusted third party and remove the burdens faced by forensic investigators.MHT is vulnerable to preimage attack as a direct result of how it functions. One novel approach they used is in the authentication structure is Merkle Hash Tree (MHT) for tamper resistance.

Sophia and Gandhi[9] created a framework for a cloud resilience system, which has the ability to provide the service for the clients even when the system is flooded with multiple requests. When the incoming requests exceed the limit then the server will not be able to process the request and may crash. In STEALTHY the server monitors the number of incoming requests given by each individual user. The server is initially given a limited amount of capacity to process the request of a single IP address if user exceeds the servers limit then the entire request from that particular IP address is blocked and all the services which are provided to that IP address are also denied.

Shaikh,A.A et al.[10] address the issue of digital forensic in a cloud environment. They use a new architecture to help investigators performing the log collection. Host-based Intrusion Detection System (HIDS) is introduced to secure the data in a cloud from malicious attacks of intruders. Then, based on the feedback results of HIDS, one web server generates email alerts and Secure Shell (SSH) message to restrict further suspicious activities. Finally, a digital forensic investigator can collect reliable evidence of suspected user. In this way, HIDS and log collection will be a significant part of digital forensic in a cloud.

Gaurav Somani et al.[11] provided a detailed introduction to the attack methods, consequences, and attack dynamics. This novel work is an attempt to analyze and gather the important requirements in designing DDoS mitigation solutions for a cloud infrastructure. These requirements include optimization of five important factors governing the attack. These factors are sustainability/budget constraints, controlled auto scaling, minimization based optimization of attack traffic, MTT, and service quality and availability. We provide a multilevel alert flow-based collaborative DDoS detection solution framework that may be beneficial in designing efficient mitigation solutions.

Saibharath Geethakumari [12] proposed cloud forensic clustering model across multiple virtual machine instances. Every virtual machine contains a virtual machine disk and its RAM image. This forensic solution decreases the search space, establishes multi-drive correlation and forms a social network of virtual machine instances. Secondly addressing the variability of cloud architectures, open source cloud platforms Open Nebula and Open Stack are compared with respect to the location of evidence artifacts. The pre-processing engine which handles different architectures is designed and implemented.

Sang T[13] suggested a model for SAAS service in which the client uses an agent to send commands to SaaS. SaaS process the commands and creates logs for that, then it will send back a response. While consumer gets there response the agent may make its own logs or just processes the response to the user. It means that we should keep another log locally and synchronously. This structure allows us to check the activities on SaaS cloud without the help of the CSPs.

Sheik Khadar et al.[14] suggested a model based on a trusted third party (TTP) along with a cloud forensics investigation team (CFIT) proves to be a better solution to enhance the trustworthiness of the service provider and thereby facilitate the cloud providers to trap cyber attackers with a strong collection of evidence which might help in a further legal process. The TTP (a trusted third party) becomes the central authority of the cloud environment as CSP's are unaware of their CC's and vice versa. The total security and responsibility lie with TTP. The TTP ensures the privacy of CC.

Mitragotri and.Nirgude [15] proposed approach takes snapshots of suspected VM and consequently enhances the execution of cloud, Log file is created which contains all Log information of attacker VM such as date and time of attack, IP address, Mac address, and investigator module can prevent the attacker VM to stop further attack by blocking the IP address (attacking VMs). Intrusion Detection Systems (IDS) are incorporated in all the VMs for monitoring malicious activities. They eliminated the high time complexity using on-demand snapshot generation when malicious activity has generated. Deployment, management and monitoring the Intrusion Detection System are done by the cloud service provider.

III. Challenges of log forensics

The dynamic nature of cloud-like its distributed infrastructure, multiple resources, large running applications, hundreds of cloud users, on demand response and virtual environment makes log forensics very difficult. Collecting, analyzing, storing of logs makes forensics investigation harder than regular digital forensics. Log forensics challenges are as follows (Ko et al., 2011).

1) Security of Logs
2) cloud log access
3) Unequal log format
4) Scattered logs
5) Log a big data

3.1 Security of Logs

Log security is most important in a cloud environment, as the content of log may provide important evidence in log forensics. Confidentiality, integrity, and availability (CIA) of log files is crucial in log forensics (Zawoad et al., 2013). Investigator can reach to malicious person by analyzing log files. If log files are altered then reaching real culprit is a difficult task.

3.2 Cloud Log access

In a cloud environment the generation of cloud log is easy, but gaining access with the proper requirement is difficult (Shams et al., 2013). Access is provided to an authorized person if legal authority approved. Access is given to forensic expert if court orders to do so. Authorized access to logs leads to correct log investigation. Sometimes due to privacy and security issues, CSP does not allow log access to third-party agency or forensic examiner.

3.3 Unequal Log Format

There are number of cloud log formats depending on individual requirements as various cloud log files being generated in a cloud environment. There is no standard, unique log format which expresses various types of cloud logs. For example process log, network log, application logs have their own log format. Different cloud having the same application may have different log format. It is very hard for a forensic expert to analyze logs with a different format. If there is a standard log format, a forensic expert easily understands data in log and accurately identifies a malicious person (Khan et al., 2016).

3.4 Scattered Logs

Logs are scattered as there is no central place where all the logs are stored in a cloud[2]. Different layers in a cloud generate different logs in a different format[16]. Due to decentralization of logs investigation is difficult in real time. In addition to this, network delay availability at a different cloud, access to servers makes log forensic procedure little hard.

3.5 Log a Big Data

Analyzing a large amount of cloud log data generated at various resources is not easy for CLF investigator. The volume of cloud log data is "big data" problem [17]. More amount of time is required to analyze such big data and find malicious persons than in traditional digital forensics [18].

IV. CONCLUSION

Providing secure and reliable logs to an investigator is a necessity of cloud forensic to get an unbiased result. Different logging systems are designed to maintain confidentiality, integrity, and availability of logs. Due to the inherent nature of cloud collecting, storing and examining the logs is not an easy, so building a logging mechanism which is secure and satisfy all the security properties is a challenging task.

REFERENCES

[1] Martini, Ben, and Kim-Kwang Raymond Choo. "An integrated conceptual digital forensic framework for a cloud computing." Digital Investigation vol . 9.no.2 pp 71-80,2012.

[2] Lokhande, Prathmesh, and Vanita Mane. "Log-based privacy preservation in a cloud forensic." 2016.

[3] Mehto, Krati, and Rahul Moriwal. "A secured and searchable encryption algorithm for a cloud storage." International Journal of Computer Applications vol.120.no.5,2015.

[4] Zawoad, Shams, Amit Dutta, and Ragib Hasan. "Towards building forensics enabled cloud through secure logging-as-a-service." IEEE Transactions on Dependable and Secure Computing vol. 1, pp 1-1, 2016.

[5] Anwar, Faiza, and Zahid Anwar. "Digital forensics for eucalyptus." 2011 Frontiers of Information Technology. IEEE, 2011.

[6] Ray, Indrajit, et al. "Secure logging as a service delegating log management to the cloud." IEEE systems journal vol 7. no.2, pp 323-334,2013.

[7] Ma, Di, and Gene Tsudik. "A new approach to secure logging." ACM Transactions on Storage (TOS) 5.1 (2009): 2.

[8] Tian, Hui, et al. "Enabling public auditability for operation behaviors in a cloud storage." Soft Computing vol21.no 8,pp 2175-2187, 2017.

[9] Sophia, G. Aline, and Meera Gandhi. "Stealthy DDoS detecting mechanism for a cloud resilience system." In 2017 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1-5, 2017.

[10] Shaikh, A. A., Qi, H., Jiang, W., & Tahir, M, “A novel HIDS and log collection based system for digital forensics in a cloud environment”. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) , pp. 1434-1438, December 2017

[11] Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M, Buyya R. “Combating DDoS attacks in the cloud: requirements, trends, and future directions”. IEEE Cloud Computing vol.4,no.1,pp.22-32, Jan 2017

[12] Saibharath, S., and G. Geethakumari. "Preprocessing of evidences from cloud components for effective forensic analysis." In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 394-399, 2015.

[13] Sang, T.,“A log based approach to make digital forensics easier on cloud computing”. In 2013 Third International Conference on Intelligent System Design and Engineering Applications pp. 91-94, January 2013.

[14] Manoj, S.K.A. and Bhaskari, D.L, "Cloud Forensics-A Framework for investigating Cyber Attacks in a cloud environment", Procedia Computer Science, Vol. 85, pp.149-154, 2016.

[15] Nilima Mitragotri, M.A.Nirgude “Cloud Forensic Investigation using VM Snapshots and Log Information” , International Journal of Innovative Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2018.

[16] Zawoad, S., Dutta, A.K., and Hasan, R. (2013), "SecLaaS: secure logging-as-a-service for a cloud forensics", In Proceedings of the 8th ACM SIGSAC Symposium on Information, computer and communications security, ACM, pp. 219-230.

[17] Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A. and Khan, S.U.(2015), " The rise of “big data” on cloud computing: Review and open research issues. Information systems, Vol 47, pp.98-115.

[18] Vollmar, W., Harris, T., Long, L. and Green, R.,(2014), " Hypervisor security in a cloud computing systems", ACM Comput. Surv, pp.1-22