Volume 64, Issue 1, 2020

Journal of Scientific Research

Institute of Science,

Banaras Hindu University, Varanasi, India.

Log as a Secure Service Scheme (LASS) for Cloud

Mohd Ameen Imran*[1] and Mohd Ateeq ur Rahman[1]

[1]Dept. of CSE, SCET, Hyderabad. ameenimran16@gmail.com, mail_to_ateeq@yahoo.com

***Abstract:** Cloud computing is widely used platform now a days. Cloud computing has brought many advantages to our existing platforms like economy of scale, availability, security and other major changes to computing platforms by implementing architectures like SASS, PASS and IASS. Many types of researches are going on to make cloud computing platform more reliable to users (single or entity) and consumers. This research paper focuses on log management in cloud computing and shows how logs are used as a valuable information source on cloud platforms like AWS, Microsoft Azure, Google GCP etc. We present Lass scheme a framework that can allow the cloud platforms to save log files in non-volatile storage in a unified format which can help in virtual machine restoration and monitoring accounts for errors and can also help in forensics process. Lass provides framework to collect log from different sources depending upon the type of service used in cloud platforms. Lass provide a way through which log of the user can be protected and the privacy of the user log can be preserved.*

***Index term:** Log framework, Log service, secure log, Cloud log scheme, log as a service.*

I. INTRODUCTION

Cloud computing have become an important part of internet technology. Cloud computing have brought many advantages to users of cloud and consumers, but the security of cloud is still not considered as secure due to which organization cannot directly trust cloud platforms. Many cloud computing platforms are still in research phase for implementing security in the cloud architecture. Digital security practices are used as a process for digital security but it cannot be directly implemented on cloud platforms because the architecture of cloud are newly developed and old security practices cannot be used with cloud(Z. Xia, Y. Zhu, X. Sun, Z. Qin, &K. Ren, 2018). CSP is a cloud service providers they provide cloud platforms for cloud resource utilization. NIST (National Institute of Standards and Technology) is an organization formed to provide standards (Kent & M. Souppaya,2014; Mell & T. Grace,2011)

The NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (Mell & T. Grace,2011).

Software-as-a-Service (SaaS): saas is known as software as a service provided by cloud platforms with the aim to provide a software service directly accessible to consumer on demand and preventing consumers from managing the software on his own. The consumer has only access to software platform rather than the whole deployment platform. All the access lies in the hands of CSP. (Aniruddha S. Rumale & Dinesh N. Chaudhari , 2017).

Platform-as-a-Service (PaaS): PaaS is known as platform as a service where the consumer gets access to deployment platform through which a consumer can directly deploy their services for future use.(Gurudatt Kulkarni, Prasad Khatawkar & Jayant Gambhir, 2011).

Infrastructure-as-a-Service (IaaS): IaaS is known as infrastructure as a service where the whole server access is provided to the consumer. The consumer can manage the network, server and applications on their own. (Pragati Chavan, Pradeep Patil,Gurudatt Kulkarni, Ramesh Sutar & Shrikant Belsare 2013).

The degree of control provided by these models are different like sass only provides access to software application platform and the logs generated by them are kept away from the user of that software; whereas pass provides some level of access to logs like system log, application log etc. but does not provide access to network and server log which can be used in forensics for event recreation and understanding the usage of cloud platform and preventing the network form any attack. (A. Patrascu & V.V. Patriciu,2014)

Contributions: The contributions in the paper are:

1. We propose a scheme preserving the confidentiality of user’s logs from malicious cloud employee or external entity.

DOI: http://dx.doi.org/10.37398/JSR.2020.640143

2. We introduce framework which can collect log data from different parts of cloud platform and store in a centralized and non-volatile storage.

3. We introduce a retention process from where the log files are reformatted to achieve unified log formatting.

Organization: The paper is organized in the follow way, Different challenges and background of cloud log system is defined in section 2. Follow by a threat model and security properties in section 3. Our proposed Lass scheme and framework is presented, in Section 4. Results and discussion are provided in section 5. Final conclusion of the paper and discuss future extensions in Section 6.

II. BACKGROUND AND CHALLENGES

Log is any event that is recorded as a data to help ensure safety and security of software system. Cloud log is an emerging field of research which provides process for log files to be used for security and integrity of applications and virtual machine(vm) from any event. These log files can also be used in cloud forensics for investigation purpose and for identifying the attack and attacker. The process of analyzing cloud log files in cloud computing or through third-party analysis services is called cloud log forensics (CLF) (Thorpe et al. 2012).

Log management is important because the size of log can range anywhere from 1KB to 1GB depending the type of organization activities. Log can also be categorized as big data as every event is recorded in the platform. This helps in analyzing and identifying important part of log and neglecting the activities which are not directly linked to VM restoration. By analyzing only important parts of log we can help in reducing the time of processing a log file by a great percent. Different types of logs are generated at different levels of cloud; these logs are stored in distributed form. Lass scheme collects all the logs and centralizes the log in one location and securing logs by generating hash code that can help in verifying the log after any event damage. The following sections show how the log can be managed so that the time for identifying the event and analyzing the logs can be reduced to minimum.

A. *Log management*

Log management can help in easily managing log files by collecting all the logs that are generated by different parts of cloud platform. Log management mainly deals with how different types of log are created and stored in the memory, distributed cloud environment and how they can be centralized.

Types of log: Depending on the type of customer cloud service (for ex; sass does not generate any virtual machine log) different types of logs are created in distributed form. Examples of various logs are given in the table I.

Log Modes: Log modes are used to define the architecture of log,how different logs are created and stored in memory and which part of cloud generate what type of log. Logging modes are divided into two main types that specify how the logs should be stored in memory and what data can be recovered from logs at the time of disaster event recovery. Each of the logging modes are explained briefly, pros and cons of each logging mode are illustrated in the Table II with their comparison in Table III.

Table I. Different Logs Types

Log Types	**Examples**
Application's log	Web applications, Database programs.
System log	Syslog-ng, Log & Event Manager
Security log	Event Log Analyzer, Control case Security Event Logging and Monitoring services
Setup log	Msiexec.exe
Network log	Splunk, Log4j2
Web-server log	Nihuo Web Log Analyzer
Audit log	WP Security Audit Log, auditpol.exe
Virtual machine logs	Virtual Machine Log Auditor, JVM controller

Table II. Logging Mode Advantages and Disadvantages

Logging Mode	**Advantages**	**Disadvantages**
Circular logging	1. Recovery in Transaction 2. Not required any maintenance. 3. For application, power, and software failure. 4. Minimum intervention of human Required. 5. Re-used logs 6. Faster throughput 7. Less time require for logs formation, allocation, achieving , deletion	1. Long term storage not supported 2. Existing logs are overwritten by filling finite space 3. damage queue files recovery not available
Linear logging	1. Media recovery 2. For application failure, media failure, power and Software 3. Storage is Long-	1. Maintenance Required 2. Process is slow 3. Logs Never reused 4. Performance

	term 4. Damage files in queue can be recovered	Degradation due to periodic allocation of new logs

Table III. Comparison between Different Logging Modes

Comparison Parameters	**Circular Logging**	**Linear Logging**
Logs Allocation	Once	Periodically
Administrative Overhead	Less	More
Reusability	Yes	No
Restart Recovery	Yes	Yes
Loss Data Recreation	No	Yes
log data Overwritten	Yes	No
Capacity for Log allocation	Finite	Dynamic

B. *Challenges*

There are many challenges faced by cloud computing platforms which led researchers to research and find solutions, some of the solutions relative cloud problems are given in table IV. This paper does not focus on these problems but for understanding the problems and solutions are listed in the given table.

Table IV. Challenges and Solutions in Cloud Log

Challenges	**Solutions**
Log data represented as big data	Dependence on CSP and Data filtering mechanism
Accessibility of cloud logs	Proper access methods Encryption of log files using cryptographic key
Security in cloud log	Log analysis centralized
Decentralized cloud logs	Cloud log files Replication
Standardized log format	Single log format
Fairness of cloud log analysis	Automatic log analysis tool

III. THREAT MODEL AND SECURITY PROPERTIES

Log can also be manipulated by intruders for inserting of false log data or replacing log with other user logs, many users in cloud environment share same virtual or physical space. Log can be altered which makes hard for the CSP to monitor and recover VM during disaster event recovery. It is important to maintain confidentiality of log as organizations does not want its competitor to know the details of how their systems work or user does not want anyone to know the insights of a software system. Integrity and availability are two important things to be considered before any log is used for investigation purpose.

The attack on logs can be from users. Lass adopts trust no one policy for protecting logs confidentiality and integrity, and allowing availability of log for monitoring and maintenance purpose. Before describing the possible vulnerability for cloud log some of the terms are defined to understand the Lass scheme.

Log: Log can be from any part of cloud platform examples of log are registry log, process log, network log, application log.

Cloud Service Provider (CSP): CSP stands for cloud service provider which provide cloud computing platform for a consumer to use computing and storage resources.

User: User is a CSP customer.

Intruder: An intruder can be any malicious person including an employee of the CSP, who wants to reveal user's activity from the log storage.

A. *Possible Threats on Cloud Log*

It is important for cloud platforms to maintain some of the metrics like integrity, confidentiality and availability of cloud log data which makes these metrics an important way to analyze how secure, confidential and correct log data is. Disastrous event or an attack in any part of log framework can compromise security of log data, it is important to consider these metrics to verify a framework from every working part. Vulnerability points in previous log frameworks are given in the table V. From log creation to log storage and analysis every part of log framework is analyzed based on the metrics which conforms how secures or vulnerable any part of log framework is.

Table V. Vulnerability Cloud Log Points

log attacks on different parts of log cycle	**Integrity**	**Confidentiality**	**Availability**
Logs creation	No	No	Yes
Log collection	Yes	Yes	Yes
Network	Yes	Yes	Yes
Log analysis	No	No	Yes
Log storage	N/A	No	Yes

IV. LASS SCHEME

In this part we propose log as a secure service scheme (LASS) framework which provides an overview on how to collect the log from different sources in the cloud computing platform. Lass consider that the information in log files are in predefined format. It does not provide any new log data representation format. Lass framework helps in only collecting and securing logs after they are generated.

The above framework shows how the LASS scheme works. Log files from all the sources like servers, other devices, emails and virtual machines are collected in log retention appliance which reformats the log data in a unified format, so that processing log files can become much easier. Logs are collected in huge form so lass consider the log files as a big data for easy processing. When the log data is reformatted it is sent to central log storage represented in framework as SAN/NAS (Y. Mansouri, A. N. Toosi, & R. Buyya,2017; H. Tian, Z. Chen, C.-C. Chang, M. Kuribayashi, Y. Huang & Y. Cai, 2016).

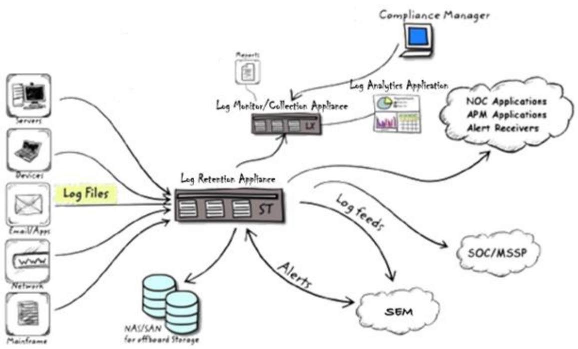

Fig.1. LASS Framework

Lass provides log monitoring service using log monitor/collection appliance where the log data can be cross checked by user using GUI appliance call log analysis. If found the log data is getting altered user can directly reach compliance and get logs audited (M. Bellare & B. Yee,1997; B. Schneier & J. Kelsey, 1999). Log retention provides log feeds to SEM which processes the data and provides alerts which can be used for information regarding system breakdown or threat to the application, network or virtual machine.(Thorpe, I. Ray, T. Grandison, & A. Barbir, 2011a; Thorpe, I. Ray, I. Ray, & T. Grandison. 2011d.)

The SOC/MSSP receives log from the log retention appliance and helps in detecting, analyzing, and responding to cyber security incidents using a combination of technology solutions and a strong set of processes. SOC stands for Security operations centers which are typically staffed with security analysts and engineers as well as managers who oversee security operations. Logs can be outsourced to an external entity called "managed security service providers (MSSPs)" as security monitoring grows more complicated and more sophisticated, there is an increased demand for outsourcing these tasks(Jianqing Zhang, Nikita Borisov & William Yurcik, 2006). Mssps handle all the logs which are outsourced from log retention appliance

SEM stands for security information and event management (SIEM) which is the state of art practice in handling heterogeneous data sources for security analysis (Marcello Cinque, Domenico Cotroneo & Antonio Pecchia, 2018). Log retention appliance sends all the log feeds to SEM for monitoring and security analysis. In case of any security threat an alert is sent to log retention appliance.

Another part of framework is NOC applications these are called as network on chip which performs network related applications. APM applications help in continuous application performance monitoring, the approach for monitoring the frame work consists of four phases Monitor, Analysis, Recommendations and Action (MARA); these phases are summarized into two segmented information panel viz. Application Health Dashboards and Corrective Action Dashboard. It allows customizing the dashboard as per the level of visibility required in order to improve the monitoring process (Mandar Sahasrabudhe, Meenakshi Panwar & Sagar Chaudhari 2013).

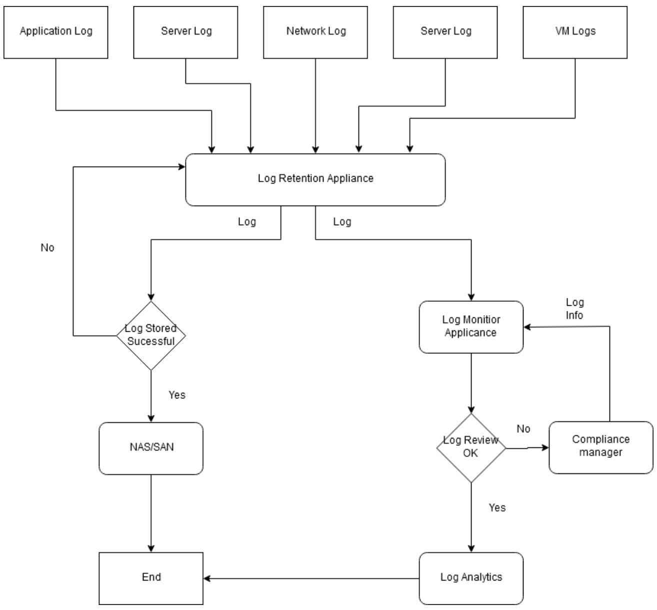

Fig.2. LASS Workflow

Lass workflow diagram shows how the logs are collected from different sources and stored in NAS/SAN storage for log backup in case of disaster recovery (Xiao-Gao Yu & Wei-Xing Li 2008). Another copy of log is sent to log monitor appliance from which user can check the log for their cloud account and review the logs in case of any modification a complaint can be registered with compliance manager. (Khan, A. Gani, A. W. A. Wahab, M. Shiraz, & I. Ahmad, 2016).

Performance Evaluation: The chart given below show the log processing time for a 5mb log file in distributed and centralized log environment.

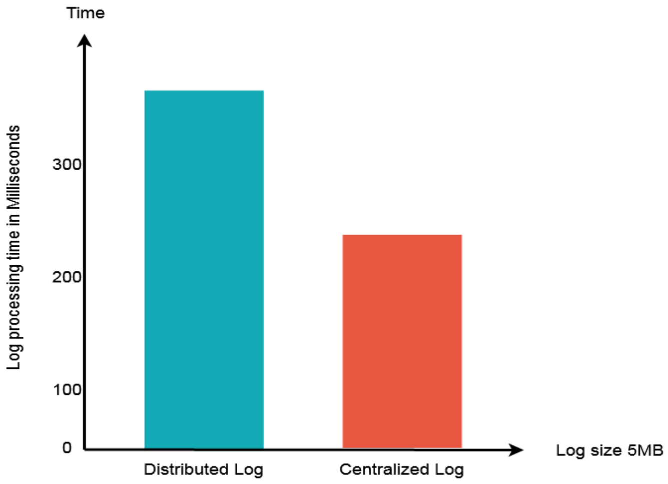

Fig.3. Compassion for Distributed and Centralized Log Storage

The above chart compares distributed and centralized log storage and processing time. The log processing time in case of distributed cloud environment is almost double to centralized log processing.

V. Results and discussion

We have provided a framework which helps in collecting log files and converting them into unified log format for faster log processing. The lass scheme helps in retaining the log files after deletion of virtual machine because the log are stored in storage area network (SAN/NAS) which acts as a backup for log files. Lass also provides a user with the log analytics application through which log files can be view with a graphical representation and actions like search, find can be performed with log analytics application. Any log which is treated as altered or modified log by user, user can contact compliance department and the log modification complaint can be registered through compliance manager. Compliance manager takes care of all the security issues of log modification complaints from any user.

VI. CONCLUSION

In this research paper, we proposed a secure log scheme framework known as “Log as a secure service scheme(LASS)” for cloud computing platforms with features that helps in the creation, collection and preservation of log security and that mitigate the damaging effects due to log vulnerability. LASS provide the privacy of cloud users by encrypting cloud logs of the respective user while also facilitating log retrieval in case of any disaster event. Moreover, it ensures accountability of the cloud by allowing the user to identify any log modification. This has the additional effect of preventing a user from repudiating entries. The framework provides an improved way of collecting and storing log in centralized storage. Potential future extensions include the following

1. Providing fast encryption technique for log files.
2. Analyzing log data from big data perspective
3. Designing and implementing Lass scheme for the real world CSPs, with aim of performance evaluation and analysis.

REFERENCES

Kent & M. Souppaya. (2014). Guide to computer security log management. National Institute of Standards and Technology (2014). 72 pages.

Mell & T. Grace. (2011). The NIST definition of cloud computing. NIST Special Publication 800–145 (2011).

F. Anwar & Z. Anwar. (2011), "Digital forensics for eucalyptus," in Frontiers of Information Technology (FIT), pp. 110-116.

A. Patrascu & V.-V. Patriciu, (2014) "Logging system for cloud computing forensic environments," Journal of Control Engineering and Applied Informatics, vol. 16, pp. 80-88.

M. Bellare & B. Yee, (1997) "Forward integrity for secure audit logs," Technical report, Computer Science and Engineering Department, University of California at San Diego.

B. Schneier & J. Kelsey, (1999) "Secure audit logs to support computer forensics," ACM Transactions on Information and System Security (TISSEC), vol. 2, pp. 159-176, 1999.

J. E. Holt, (2006) "Logcrypt: forward security and public verification for secure audit logs," in Proceedings of the 2006 Australasian workshops on Grid computing and e-researchVolume 54,2006,pp.203-211.

H. Tian, Z. Chen, C.-C. Chang, M. Kuribayashi, Y. Huan & Y. Cai, et al. (2016), "Enabling public auditability for operation behaviors in cloud storage," Soft Computing, pp. 1-13,.

Y. Mansouri, A. N. Toosi, & R. Buyya, (2017) "Data storage management in cloud environments: Taxonomy, survey, and future directions," ACM Computing Surveys (CSUR), vol. 50, p. 91.

Z. Xia, Y. Zhu, X. Sun, Z. Qin, & K. Ren, (2018) "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Transactions on Cloud Computing, pp. 276-286.

Khan, A. Gani, A. W. A. Wahab, M. Shiraz, & I. Ahmad. (2016). Network forensics: Review, taxonomy, and open challenges. (in press).

Thorpe, I. Ray, T. Grandison, & A. Barbir. 2011a. The virtual machine log auditor. In Proceeding of the IEEE 1st International Workshop on Security and Forensics in Communication Systems. 1–7.

Thorpe, I. Ray, I. Ray, & T. Grandison. 2011d. A formal temporal log data model for the global synchronized virtual machine environment. Int. J. Inform. Assur. Secur. 6, 2 (2011), 398–406.

Aniruddha S. Rumale & Dinesh N. Chaudhari (2017) Cloud computing: Software as a service 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT).

Gurudatt Kulkarni, Prasad Khatawkar & Jayant Gambhir 2011 Cloud Computing-Platform as Service December 2011 Volume-1 International Journal of Engineering and Advanced Technology (IJEAT).

Pragati Chavan, Pradeep Patil,Gurudatt Kulkarni, Ramesh Sutar & Shrikant Belsare (2013), IaaS Cloud Security, 2013 International Conference on Machine Intelligence and Research Advancement.

Xiao-Gao Yu & Wei-Xing Li (2008), A new network storage architecture based on NAS and SAN, 10th International Conference on Control, Automation, Robotics and Vision

Jianqing Zhang, Nikita Borisov & William Yurcik (2006),Outsourcing Security Analysis with anonymized Logs,2006 Securecomm and Workshops

Sitaram Kowtha , Laura A. Nolan & Rosemary A. Daley (2012), Cyber security operations center characterization model and analysis, IEEE Conference on Technologies for Homeland Security (HST)

Marcello Cinque ; Domenico Cotroneo & Antonio Pecchia (2018), Challenges and Directions in Security Information and Event Management (SIEM), 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)

Mandar Sahasrabudhe , Meenakshi Panwar & Sagar Chaudhari (2013), Application performance monitoring and prediction, 2013 IEEE International Conference on Signal Processing, Computing and Control (ISPCC)

***