# EFFECTIVE MANAGEMENT OF PROOF OF LOGS

Ujwal Pandita[1], Henna Katy, Kalpana and Deepti Sonawane

[1] *Student, IT, DYPIET, Maharashtra, India*
[2] *Student, IT, DYPIET, Maharashtra, India*
[3] *Student, IT, DYPIET, Maharashtra, India*
[4] *Student, IT, DYPIET, Maharashtra, India*

**ABSTRACT**

*With the origin of cloud computing, the intruders have likewise brought their bar up in the shadow of cyber crime .Lack of security is the only hurdle in wide adoption of cloud computing. However, the regular monitoring of the logs is the most crucial part in finding the attack and building the defense against Cloud. Our design focuses on accurate time synchronization, evidence segregation without breaching the confidentiality of other users, and helps in information analysis and evidence reporting which are required for management of logs. This project will develop and enhance forensic technique for collecting logs in the emerging paradigm of cloud technology. The framework will primarily focus on obtaining accurate logs & analyzing for auditing the system.*

**Keyword: - :** *Digital Forensics, Cloud Forensics , Past of proof log , Accumulator etc.*

## 1 Introduction

Cloud computing has open new era of computing for business, IT organizations and distributed computing by offering unlimited infrastructure resource with efficient service called pay-as-you-go computing. Pay as you go service offers a low cost computing way of technology , in which consumer pays only for hour it consumes .Although cloud computing is attractive and cost efficient and high performance way of computing ,but still it suffers from many security issues [1],[2],[3] with reference to computer forensics. Due to availability of cloud technology at very low cost, this factor have attracted the malicious individuals to launch attacks from machines inside a cloud [4] or use cloud to store contraband documents. One of the new technique that attacker had identified is, Distributed Denial of Service (DDoS) attack, in which attackers are now placing a new Linux DDoS Trojan called Backdoor.Linux.Mayday.g in compromised Amazon EC2 virtual machines (VMs) and launching attacks from those VMs.

For reporting these types of attacks there is a need to execute digital forensics procedures in the cloud to determine the traces of an incident.this leads for the development of special branch of digital forensics called cloud forensics.Logs of cloud clients can expose the moves made by a client utilizing cloud infrastructure. Thus, logs are vital confirmation to indict a suspect. Be that as it may, gathering logs from the cloud infrastructure is to a great degree troublesome in light of the fact that cloud clients or examiners have next to no influence over the framework. At present, there is no chance to get for agents to gather logs from an ended VM; they have to rely on upon the Cloud Service Providers (CSP) to gather logs from the cloud. Be that as it may, investigators need to trust the CSPs

aimlessly, as they can't confirm whether the CSPs are giving substantial logs or not. While the need of logs is unquestionable in legal examinations, the reliability of this proof will stay faulty in the event that we don't take legitimate measures to secure them. An attacker can attempt to have a botnet server, spam email server, or phishing sites in cloud VMs furthermore, he can remove the traces of his malicious work by altering the logs.Also,investigator can tamper the logs before presenting into the court.

To solve the difficulties talked about in the above situation, we proposed a system called Effective management of proof of logs . Since information living in the VM are unstable (can't be managed without power),our system gathers logs from the VM and manages collected logs in effected way. While saving, it encodes private information and keeps up a hash-affix of the logs to secure the unique arrangement of logs. Our system generate the proofs of past logs (PPL) and makes the proofs available.once the PPL is made available, then CSP can not alter the published PPL.hence with the help of hash-chain and PPL, our system provides provides forward security of the logs of all past proofs.Introducing the proof technique will empower investigators to gather dependable logs of cloud-based malignant exercises and introduce those to the court specialist. The security properties guaranteed by proof system can help CSPs to build up trust with the cloud clients. Hence secure proof system enabled for all users, can prevent a malicious user from launching malicious activities from clouds.In this section we are going to present an overview of forensics with respect to proof of logs and discuss the challenges related to management of logs in cloud forensics.

## 2 Background and challenges

### 2.1 Digital forensics

Digital forensics is the process of "the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data".
Cloud crime scene investigation include all the steps of digital forensics as shown in fig1 in the cloud environment along with investigating file system, process, cash, and registry history.
All the steps of digital forensics that are mentioned in fig. vary according to the service and deployment model of cloud computing.

### 2.2Importance of logs

Logs are one of the most important factor of any analytical data in a cloud-based service framework . Logging is considered an essential means of security control for investigators. Logging helps in identifying, answering operational issues, incidents,violations, and fraudulent activities [Kent and Souppaya 2014]. Log file helps in recording various entries of an event in an IT system or network. Log file provides significant information related to a particular event at the time the log file is generated.It helps forensic investigators to identify malicious behavior of an external agent.The process of recording log files is known as logging[Chuvakin *et al.* 2013].It helps in finding all previous events occurring in the system and network during a specified time span. For instance, a network administrator can find out about the network bandwidth usage in a time interval by analyzing the network logs in a given system.An application developers can make use of application logs to identify and fix bugs inside a program code.Logging is necessary for service owner/operators to understand the status of each of the component in an infrastructure for fault monitoring to assess feature usage, and to monitor business processes.Application developers, require access to historic information for debugging(troubleshooting) and forensic investigations.

Logs helps investigators to identify the various sources of information generated
from the system at different time intervals. Many logs generated for security reasons stop future intrusions by detecting them through the various patterns and occurrences observed. Logs are most importantly log file data used for security purposes because of increased attacks on the system and network [Zuk 2011]. The logs used to record attackers activities at the time of the attack.Log file data helps the system and network administrators to investigate attacks by analyzing [Mao *et al.* 2014].lncase of large organizations, there is a issue of scarcity of resources because of different types of log files created on different devices.Hence there is a need of effective management of logs.Inorder to overcome the log management problem, organizations have started to move towards cloud

computing by using cloud logging services. The log file contains the sequential steps performed during an execution along a specified timeline. A log file is composed of log entries and each log entry contains useful information associated with events occurred in the system, network, virtual machine, or application. A log file entries differ with its types and requirements involved in particular system.

### 2.3 Cloud Forensics

Cloud forensics is an application of digital forensics in cloud computing that consists mixture of traditional computer forensics, small-scale digital device forensics, and network forensics.

As cloud computing is based on examination of network forensics i.e handling of forensics investigation while accessing network in both private and public cloud ,Ruan al. define cloud forensics as a subset of network forensics[5].
Steps for digital forensics differe based on Deployment model of cloud computing according to various services provided by cloud such as Saas(software as a service),Pass(platform as service),Iass(infrastructure as servie).

### 2.4 Challenges

Reduced Level of Control in Clouds: In conventional forensic investigation, investigators have full control over evidences . Unfortunately, we broadly rely on upon CSPs to obtain logs from clouds. Accessibility of the logs shifts relying upon the service models. Cloud clients have the most astounding control in IaaS and minimum control in SaaS. This physical detachment of the proof and absence of control over the system make confirm obtaining testing in cloud forensics. In SaaS, clients don't get any log of their system, unless the CSP gives the logs. In PaaS, it is just conceivable to get the application logs from clients.

Availability of Logs: Logs created in various layers of cloud systems are required to be open to various partners of the system. For instance, system executives require significant logs to investigate the system; developers require their obliged logs to fix the bugs of an application; investigators require logs, which can help in their investigation.

The absence of a Standard format of Logs: To analyse logs most adequately, it will be important to have a standard format of the logs. Shockingly, till now, there is no standard format of logs for cloud infrastructures. Logs are accessible in heterogeneous formats – from various layers of a cloud to various service providers.

## 3 Proposed System

Firstly we will define the vital terms of our proposed system next we define the attacker's capability for attacking on logs,and the security properties that a service should provide.

### 3.1 Definition of terms

Log: various forms of logs can be generated in th cloud for a VM,it could be network log, process log ,operating system log etc.

Proof of Past Logs (PPL): integrity of logs is ensured with the concept called PPL.

CSP: CSP(cloud service provider) is the owner of cloud infrastructure, who is responsible for generating PPL.

User: user is a customer who utilizes services from CSP.
Investigator: in case of any malicious incident fornsics expert(investigator)collects all the necessary logs from system.

Intruder: indruder is a malicious person who wants to reveal users activity from stored logs.

**3.2 Architecture:**

**3.2.1 Notations:**

- Encrypted function encrypts a message M using public key Pk.
- The Signature message function generates signature of message M using the secret key Sk.
- We assume that Law Enforcement Agencies and Cloud service provider have set up their secret keys and public keys.
- There are two secret key of the Cloud Service Provider..
- Law Enforcement Agencies uses two secret key.
- There are two public key..
- Network operation is denoted by using time of network operation.
- Encryption of log entry is denoted by Encrypted Log Entry.
- All the log entry is is put together to form log chain..
- Log Chain of the previous entry of the persistent storage is also maintained..
- Database log entry stands for entry in log database.
- Accumalator entry of each day is recorded..
- Proof generation time, and the signature over (accumalator entry,proof generation time) using secret key of the Cloud service provider..
- Secret key of cloud service provider is also maintained.
- Log Chains are maintained as log chain0,log chain1,…log chain n.

Snort: Snort's is a open source network-based intrusion detection system (NIDS).It has the ability to perform real-time traffic analysis and packet logging on Internet Protocol(IP).Snort in network detection mode will monitor network traffic and manages network logs.

Parser: Parser module collects different types of logs from Snort. After acquiring logs, parser then parses collected logs and generates a Log Entry for network logs. Parser uses the generated entry and sends it to logger module.

Logger: Logger module encrypts some data of LE to ensure privacy of user and it generates encrypted log entry. After encrypting logger module creates log chain(LC).Log chain is created to preserve the order of all log entries. Logger module then creates entry for log storage(DB).It then communicates with proof accumulator inorder to retrieve latest accumulator entry. After this logger module creates membership information of the proof accumulator storage. Then logger updates last retrieve accumulator entry with the help of membership information. After completion of all this steps logger then sends this updated entry to proof accumulator storage to store proof of logs. Each day logger does the same process and retrieves last accumulator entry for each static Upland using this accumulator entry logger then generates PPL(Proof of Past log).PPL in all consists of proof generation time, Signature of (accumulator entry, proof generation time) using secret key of cloud provider.

Accumulator**:** A Bloom Filter is a space productive probabilistic information structure which is used to represent a set and perform membership queries , i.e. to query whether an element is a member of the set or not.

Bloom filter is responsible for storing the logs for a perticulr day. logger module retrives latest bloom filter AE from the proof storage which is nothing but the bit positions for the previous inserted logs of the day.The acquired K-bit position from database entry are hashed by K different hash functions. Logger sends this information to the proof storage for each day.

## 4.Architecture Explanation:

**4.1 Process Flow Of Retrieving Log and Storing the PPL.**

In this system we are using snort as a source for network.

(1) Parser module first communicates with Snort and collects different type of logs.After acquiring logs from snort parser then parses collected logs and generates log entry in the form :

Log Entry is generted from source IP address ,destination IP address,TL,Port number,userID.

Where,

TL is time of network operation

(2)Parser then sends Log Entry to Logger module for further processing.

(3)Logger module then encrypts some confidential information of Log Entry using public key of Law Enforcement Agencies and generates Encrypted Log Entry as :

Encrypted Log Entry is generated from encryption of source IP address,port number,userID by using is public key of Law Enforcement Agency and destination IP address,TL.

(4)After generating encrypted log entry,logger module then generates log chain to preserve correct order of log entries as:

Log chain is generated by hashing of encrypted log entry and previous log chain.

where previous log chain is the Log Chain of the previous entry of the persistent storage.

(5)After this logger module then prepares entry for log database,which we denote as Database Log Entry.Database Log Entry consists of Encrypted Log Entry and Log Chain.

(6)Logger module then communicates with Proof accumulator storage and performs three steps: (i)First it retrieves latest accumulator entry.

(ii)Second, logger module generates proof of Database Log Entry i.e. it creates membership information of Database Log Entry for accumulator.

(iii)Third, finally logger module sends updated accumulator entry to accumulator storage to store proof of logs.

(7)At the end of each day, the logger retrieves the last accumulator entry of each static IP, which we denote as last accumulator entry of day.

(8)Using last accumulator entry of day. ,logger module generates proof of past log as:

Proof of past logs contains last accumalator entry,proof generation time, signature over (accumalator entry,proof generation time) using secret key of the CSP.
(9)After computing Proof of Past Log ,logger publishes them on web.Proof of past logs is then made available to protect it from manipulation by provider after publishing.

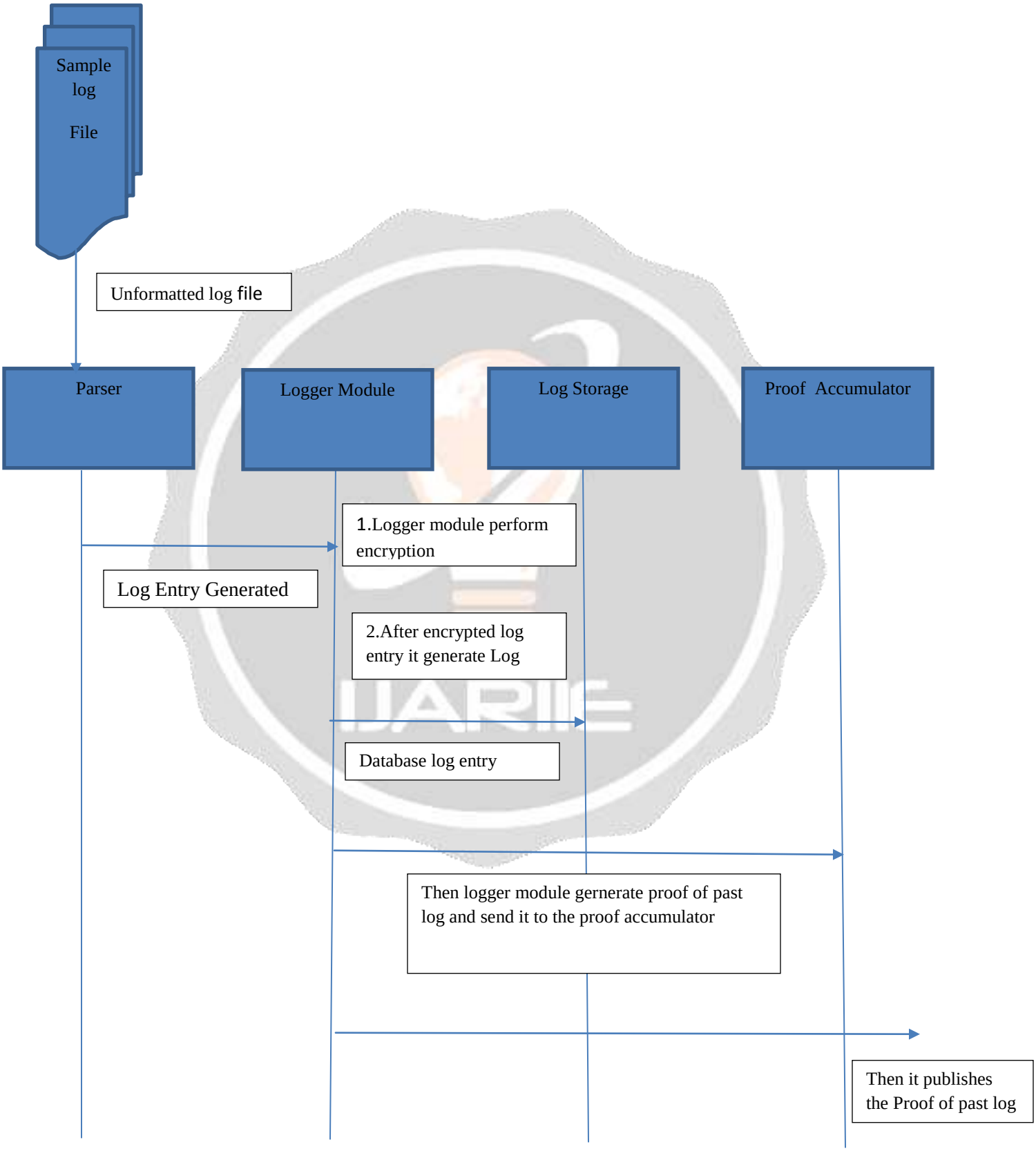
Sample log File
Unformatted log file
Parser
Logger Module
Log Storage
Proof Accumulator
1.Logger module perform encryption
Log Entry Generated
2.After encrypted log entry it generate Log
Database log entry
Then logger module gernerate proof of past log and send it to the proof accumulator
Then it publishes the Proof of past log

**Fig.1**: Process Flow Of proof of logs

## 5. CONCLUSIONS

Chain of custody is a concept which is used to record an event without loosing an information due to modification, deletion, and insertion. With the help of Chain of custody we can relate one event with another by connecting each other for extracting useful information. Different attributes of an event can be easily co related including verifiable evidence, log locations, log storage positions, log access methods, and collecting process of logs that explain and verify each step.this helps in collecting correct log files an presenting this evidence to the court. In general it is very difficult to perform all the steps of log forensics due to resource in-accessibilities, geographical diversification, virtualization, multiple layer architecture, and millions of users. As logs are generated with in CSP's platform logs are restricted from third party investigators because of there own corporative security logs and procedures. One of the challengesfor an investigator is to verify steps against the culprit in the court.a question can be arised against provider from the investigator that whether provider provides trustworthy log evidence to the court.hence our designed system will help in verifying the log evidence to the concept called chain of custody.the chain of custody gives us an important future directions for cloud log forensics due to its significance in terms of verifiability, understandability, and dependability of the whole process.Hence our proposed log management will help in identify violations and vulnerabilities created by the intruders internally or externally in an organization.

## 6. REFERENCES

[1]. M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro,"A security analysis of amazon's elastic compute cloud service," in Symposium on Applied Computing. ACM, 2012, pp. 1427–1434.
[2]. S. Subashini and V. Kavitha, "A survey on security issues in servicedelivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[3]. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
[4].The Register, "Amazon cloud hosts nasty banking trojan," http://goo.gl/ xGNkNO, 2011, [Accessed March 20, 2015].
[5].K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in Advances in digital forensics VII. Springer, 2011, pp. 35–46.