Development of Highly Secured Cloud Rendered Log Management System

Rajebhosale Sagar S.
PG Scholar,
Dept. of Computer Engineering,
SRES's College of Engineering, Kopargaon, M.S.

Pawar Anil B.
Asst. Professor,
Dept. of Computer Engineering,
SRES's College of Engineering, Kopargaon, M.S.

ABSTRACT

A log is a collection of record of events that occurs within an organization containing systems and network. These logs are very important for any organization, because log file will able to record all user activities. As this log files plays vital role and also it contains sensitive information , it should be maintained highly secure. So, management and securely maintenance of log records are very tedious task. However, deploying such a system for high security and privacy of log records is an overhead for an organization and also it requires additional cost. Many techniques have been design so far for security of log records. The alternative solution is to maintaining log records over a cloud database. Log files over cloud environment leads to challenges about privacy, confidentiality and integrity of log files. In this paper, we propose highly secured cloud rendered log management and also use of some cryptographic algorithms for dealing the issues to access a cloud based data storage. To the best of knowledge, this is the strong work to provide a complete solution to the cloud based secure log management problem.

General Terms:

Security, Cloud Computing

Keywords:

Confidentiality, Privacy, Integrity, Cryptographic algorithms

1. INTRODUCTION

A Log file is to record the elaborated information of each event of a system, network or application running in associate organization [1]. Log files are extremely helpful to search out any operational issues shortly they have occurred and additionally able to helpful data to resolve such issues. Log files are useful in distinguishing the protection incidents, erroneous activities, and policy violations. Logs contains of sensitive information of an activities in organization, therefore there have to be some protection from malicious provoker. Since log files contain record of most system events as well as user activities, they become a vital target for malicious attackers[1]. Associate provoker, breaking into a system, usually would strive to not leave traces of his or her activities behind. Consequently, the primary issue provoker or invader usually will is to break log files or interrupt the work services.

1.1 Log Generation and Maintenance

There are some ancient protocols supported syslog to generating logs. Some security extensions projected like reliable delivery of syslog [2], forward integrity for audit logs [3], syslog-ng [4], and syslog-sign [4], provides either partial protection, or don't shield the log records from malicious attacks. On alternative aspect the count, size, and format of security logs have augmented quickly, that desires of security log management? The method for generating, transmittal, storing, analyzing, and eliminating security log information. Organizations facing a serious drawback with log management are to effectively equalisation a restricted amount of log management resources with a continual offer of log information[1]. For any organization log generation and maintenance are often difficult by many factors, as well as a high range of log sources; inconsistent log content, formats, and timestamps among sources; and more and more massive volumes of log information. Log management additionally must to deliver the goods some properties like confidentiality, integrity, and availability of logs. Deploying secure work information to fulfill all the above challenges cloud storage is best economical different.

The remainder of paper is organized as follows. Section II explains existing protocol and its related properties.In Section III, present the proposed system model of secure logging as protocol. Section IV describes about Mathematical modelling. Section V describes experimental results and concludes paper in section VI.

2. RELATED WORK

Many approaches are projected for storing log information. Most of these protocols supported a protocol referred to as syslog. Syslog protocol transfers the log information to syslog server by using UDP(User Datagram Protocol). Hence in syslog the delivery of log messages isn't reliable. And additionally it doesn't shield the log information from end-point attacks[2]. Syslog - ng uses TCP(Transmission Control Protocol) for reliable log record delivery and uses SSL (Secure Socket Layer) to supply confidentiality and integrity throughout transit. but it doesn't shield log record modifications at end-points[4].

Syslog - sign which provides integrity to log message and detect missing message using signature block and certificate block but this protocol has various privacy and confidentiality

Table 1. Secure logging protocol and their Security requirements

Protocol	Authentication	Confidentiality	Integrity	Rel. Delivery
Syslog	No	No	No	No
Syslog ng	No	Yes	Yes	Yes
Syslog Sign	Yes	No	Yes	Yes
Rel. Syslog	No	Yes	Yes	Yes

issues. Syslog - sign do not provide privacy to log records during transmission and end points[4]. Syslog - pseudo protocol uses pseudonymizer filter to substitute pseudonyms for specific fields in the log record. however it doesn't guarantee correctness of log records. Once log records are substituted by some values they cannot be retrieve back[5]. Reliable - syslog protocol provides trivial mapping backward compatibility. however it does not defend the log information from privacy and confidentiality breaches.Table 1 indicates the protocol and their satisfied security requirements[6].

3. PROPOSED SYSTEM MODEL

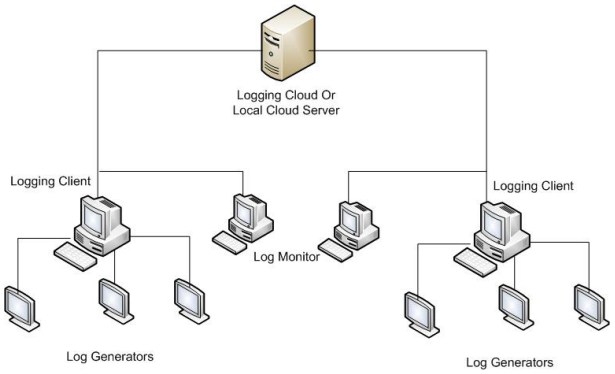

Fig. 1. System Architecture.

The complete system architecture is shown in above figure. Major components of the projected system.

Log Generator:Log generators are computing devices which generates log file. Log generators are the main target of attacker. So, Logs of these host not stored locally. for security purpose, it is pushed to logging client.

Logging Client: The logging client is receives groups of log records generated by log generators. Logging Client prepares the log data using cryptographic algorithms so that it can be securely store to the cloud.

Logging Cloud or Local Cloud Server: For maintaining log records over long term, Logging Cloud or Local Cloud Server is used. It can delete log records only after the authenticate request from logging client.

Log Monitor: Log Monitors are simply hosts that are used to monitor and review log data. They can analyse log records based on log records retrieved by authenticate request of log retrieval. Log Monitor and Logging Client may be the same host.

3.1 Module Description

(1) Module 1: Log File Preparation for Secure Storage
  (a) Log Aggregation and Encryption Module
  (b) Compute MAC and aggregated MAC Module
(2) Module 2: Secret Sharing Module
(3) Module 3: Upload, Retrieval and Deletion of Log Data
  (a) UploadTag generation and storage Module
  (b) DeleteTag generation Module
  (c) Log Retrieval Module

Module 1: Log File Preparation for Secure Storage: In this module, Log files are aggregated from different log generators. It can directly upload to cloud, but here problem of cloud provider. Cloud provider can be honest but if curios then major security problem will occur. For security from cloud provider, log records will upload to local cloud in extremely secured manner. Log files from log generators are aggregated in some batches and then encryption is done by using blowfish algorithm. After encryption, MAC will be generated from batch of encrypted log files[7]. After MAC generation, aggregated MAC will generate for log term storage at local cloud server or logging cloud. Log aggregation, encryption, MAC generation and aggregated MAC generation is done by logging client.

Module 2: Secret Sharing Module: We don't have confidence one trustworthy entity to store and manage keys and all log data[8]. So, In this scenario, To distribute the keys across several hosts, proactive secret sharing algorithm will used[9].

(1) No single entity holds the whole secret S;
(2) Any subgroup of entities of size threshold T will conjointly recreate or recover the secret S;
(3) No subgroup of entities of size Q ¡ T will re-create or recover the secret S.

Module 3: Upload, Retrieval and Deletion of Log Data:Local cloud server or Logging cloud can only accept the request of upload, retrieve and delete from authenticated and authorized clients. To uniquely identifies the log records, log records have primary key. Upload_tag can work as primary key of log records. Log records is stored at local cloud server indexed by upload_tag. To retrieve log records, an uploaded log batch of log records will used. To delete the log records, logging cloud throws the challenge for requester proves authorization by presenting a delete_tag. The log delete operation can be requested only by authorized entities. Evidence of possession of the Delete tag proves the necessary authorization. If delete_tag matches then log records will permanently delete.

4. MATHEMATICAL MODEL

When solving problems have to decide the difficulty level of problem. There are three types of classes provided for that. These are as follows:

(1) P Class: Informally the class P is the class of decision problems solvable by some algorithm within a number of steps bounded by some fixed polynomial in the length of the input. Turing was not concerned with the efficiency of his machines, but rather his concern was whether they can simulate arbitrary algorithms given sufficient time.
(2) NP-hard Class: A problem is NP-hard if solving it in polynomial time would make it possible to solve all problems in class NP in polynomial time. Some NP-hard problems are also in NP (these are called "NP-complete"), some are not.

(3) NP-Complete Class: A decision problem L is NP-complete if it is in the set of NP problems so that any given solution to the decision problem can be verified in polynomial time, and also in the set of NP-hard problems so that any NP problem can be converted into L by a transformation of the inputs in polynomial time.

Summary: From all the above aspects, This proposed model is of P Class because:

(1) Problem can be solved in polynomial time.
(2) This system always produces strong results.

Let S be the set of Inputs, Functions and Outputs S = {I,F,O} where I represents input i.e. log file and encryption keys which is input to log files, F represents the set of functions that are performed on the input. O is the Set of output.

Inputs:
I1= Log File
I2=Encryption Keys

Functions:
F1= Log File Preparation for Secure Storage
F2= Secret Sharing Module
F3= Upload, Retrieval and Deletion of Log Data

Output:
O1= Retrieve Secured File

Sets:
I = {I1, I2}
F= {F1, F2, F3}
O={O1}

Input is mapped to output which is shown in the following Venn diagram: State Diagram showing Input and output after each

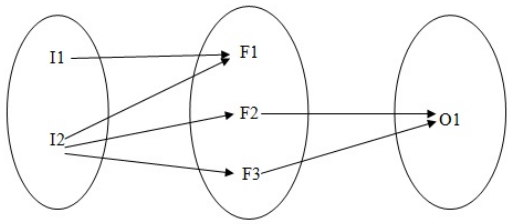

Fig. 2. Venn Diagram

Process.
Where,

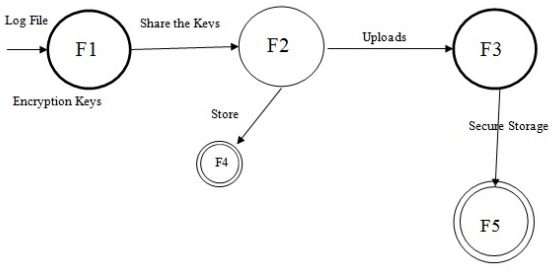

Fig. 3. Process State Diagram

F1= Log File Preparation for Secure Storage
F2= Secret Sharing Module
F2= Upload, Retrieval and Deletion of Log Data
F4= Success of Secret Share
F5= Secure Storage

As can see from the diagram there are three sets; one of the set is of input i.e. Log file and Encryption Keys having n tuples. Similarly for number of operations can provide secure storage to log file. So for a normal flow the time complexity of the Encryption algorithm is O(n), while same complexity for the Hash Function become O(n+m). So time complexity for overall system become O(n) ignoring m.

5. EXPERIMENTAL RESULTS

The proposed model is under development phase. Some part of projected system is working very accurate and The initial results of projected system is as follows.

5.1 Step 1. Project Management Console

Figure 4 shows the home page of our system. This page contains ”Load Log File” button for loading the log file. Log file automatically loading from predefined location and then it will open as input file.

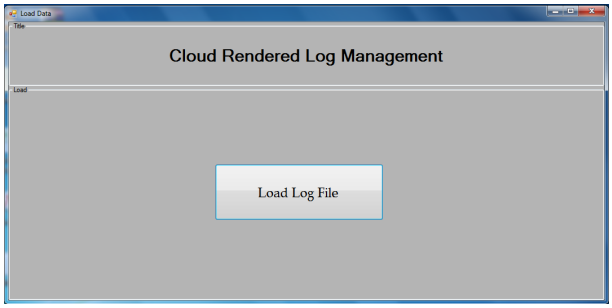

Fig. 4. Project Management Console

5.2 Input File

Figure 5 shows the input file in notepad. After loading log file, this input file will be open. For opening the log file system should ask for proper application to open specific file and after selecting it i.e. Notepad, System should open Log file which contains all the details about events and activities performed by user on system.

Fig. 5. Input file

5.3 Step 2. Show in Tabular Form

Figure 6 shows the page which contains "Show in Tabular Form" button. After clicking on this button, loaded input file will be save and convert to tabular form and shows on next form which contains Sr. No, Description, Title, Visit Count, Date and Time.

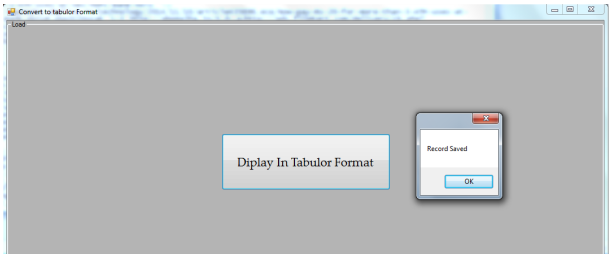

Fig. 6. Show in Tabular Form

5.4 Step 3. Encrypt log files

Figure 7 shows the form which contains log file in tabular form and it is ready for encryption.Tabular form contains Sr. No, Description, Title, Visit Count, Date and Time. After clicking on "Encrypt Files", files will be encrypted using Blowfish algorithm. After encryption, output file will be open on next form.

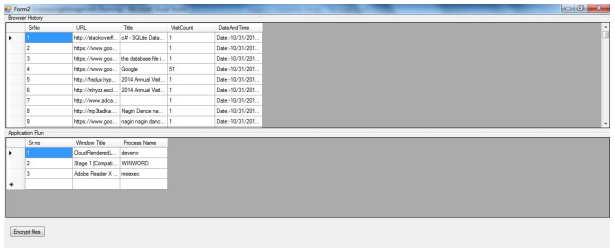

Fig. 7. Do Encryption

5.5 Step 4. Encryption Done

In Figure 8, Log file is encrypted by Blowfish Algorithm and open partially in non readable format. On this form, encrypted contains of file is partially open. After clicking on "View" button, Actual output file will be open.

Fig. 8. Encryption Done

5.6 Output File

Figure 9, Shows the output file which is in encrypted form. So, It is in non readable form. Blowfish algorithm uses 16 rounds. So, Encrypted file will be more secure and then save it locally.

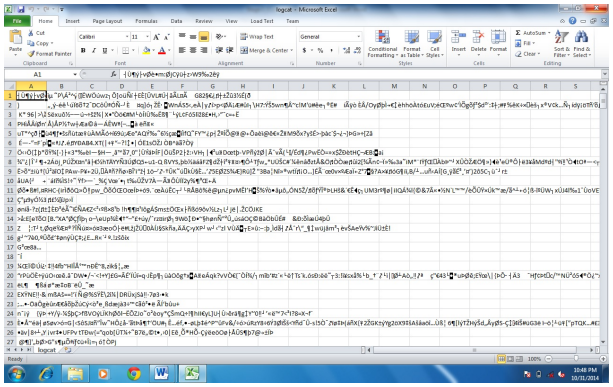

Fig. 9. Output File

6. CONCLUSION AND FUTURE SCOPE

In this project, a complete system is proposed to firmly delegate log records to a cloud. It examines existing protocols and system with their problems in numerous situations and provides complete extremely secured cloud rendered log management service. It is summarize that encryption techniques used affects the overall performance of system. Then projected a comprehensive scheme that addresses all security issues like confidentiality, privacy and integrity not simply throughout log generation phase, however conjointly throughout all alternative stages in log management process. From initial results, It is proven that log records are very secured due to encryption technique used in this project. Future work of this project will be implementation of advanced cryptographic algorithms which able to give high security to log records. Simultaneously, work on automation of log aggregation and upload to cloud server. It will affects to less overhead of projected system.

7. REFERENCES

[1] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, Mariappan Rajaram "Secure Logging As a Service Delegating Log Management to the Cloud" in IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013

[2] Karen Kent ,Murugiah Souppaya "Guide to Computer Security Log Management" in NIST Special Publication 800-92

[3] C. Lonvick, The BSD *Syslog Protocol*, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

[4] D. New and M. Rose, *Reliable Delivery for Syslog*, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001

[5] U. Flegel, "Pseudonymizing unix log file, in Proc. Int. Conf. Infrastruture Security, LNCS 2437. Oct. 2002, pp. 162179

[6] M. Bellare and B. S. Yee, "Forward integrity for secure audit logs", Dept. Comput. Sci., Univ. California, San Diego, Tech. Rep., Nov. 1997.

[7] B. Schneier and J. Kelsey, "Security audit logs to support computer forensics",in ACM Trans. Inform. Syst. Security, vol. 2, no. 2, pp. 159-176, May 1999.

[8] A. Shamir, "How to share a secret", Commun. ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[9] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage", in Proc. 15th Ann. Int. Cryptology Conf., Aug. 1995, pp. 339-352.