A SURVEY ON SECURED LOGGING IN THE CLOUD

Prasad P Kharade[1], S.B.Natikar[2]

[1]ME Student, Computer Engineering, VACOE, Maharashtra, India
[2]Asst .Professor, Computer Engineering, VACOE, Maharashtra, India

Abstract

Log is a group of different types of actions that take place in organization. Logs are often compromised by an attacker so providing security to the log record is challenging task. Log record generally contains some sensitive information so confidentiality and integrity are important as the privacy is concerned. So there is need to protect the log records for the proper functioning of any organization. It is observed that over extended period of time introducing the secured logging techniques involves great capital that finds every organization irresistible. Appointing the logs record to the cloud environment saves the cost In this paper we are suggesting the homo morphic encryption scheme that provides a strong security.

Keywords: *cloud computing, Logging, Security.*

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

1. INTRODUCTION

A log is a collection of events that take place in any organization and all activities are recorded in a log file. Log records are helpful to track all the user actions. Logging is essential because log record can be used to rectify the troubles and to improve the system's performance. log records are the main target of attacker because attacker don't want to leave any footprint of any action performed by him at the time of attack. In this way first target of attacker is to have access to the log files therefore after having access to log file the first thing that attacker want to do is to damage the files and threaten to the confidentiality and second thing is that to discontinue the logging service to confused the loggers. Furthermore there are chances of outsourcing the personal information to others in this way violating the security. One example is that when user wrongly put his password in the username filed at that time when he logged into system then logging program take password as username in this way breaches the security. From above scenario it is mandatory that logging should be done in secure manner and log files are sufficiently protected for long amount of time.

2. DESIRABLE PROPERTIES TO SECURE LOGGING

1. Correctness: Log record is important because it shows the true history of the system so that collected log record should be correct. It should be same when it was generated.

2. Verifiability: It must be able to check that all the entries in the log record are available or not and it must be ensured that data in log record have not been altered.

3. Confidentiality: Log records should not be easily searchable to collect the personal information of others. Access should be provided to only legitimate users.

4. Privacy: While in transit log records should not be track able to unauthorized persons.

5. Tamper Resistance: A log should be provided security in such a way that only log generators are allowed to introduce valid entries.

3. LITERATURE SURVEY

In this section we are going to review different types of secure logging techniques along with their major disadvantages. Different techniques used for secure logging are shown below.

Table 1secured Logging Method Review

Sr.No	Scientist's Name	Proposed Models	disadvantages
1	C Lonvick,Aug2001	Syslog Protocol	Uses UDP protocol so unreliable delivery and it can't protect log records in transit
2	Balabit,2011	Syslog-ng	It can't protect against log data modification when it stored in system.
3	J. Kelsey & J. Callas, May 2010	Syslog-sign	It doesn't provides data confidentiality and privacy during transit of data.
4	U. Flegel, Oct 2002	Syslog-pseudo	This protocol doesn't ensure

			exactness of logs.
5	D. New & M. Rose, Nov 2001	Reliable-syslog	Not prevent against confidentiality and privacy of data.
6	M. Bellare and Yee, Nov 1997	Forward Integrity	This protocol requires online trusted servers.
7	D. Ma and Tsudik, March 2009	Forward secure sequential authentication	Competent method but requires more capital.
8	Indrajit Ray & K. Belyaev, June 2013	Secure Logging As A Service-Delegating Log Management to the Cloud	Most competent And secured method but loosely coupled architecture.

3.1 DISCUSSION ON SURVEY PAPERS

3.1 The BSD Syslog Protocol

D. New and M. Rose declared in their work as: The BSD Syslog Protocol[1][2] defines a number of service associated options and also relate to inseminating event messages. This message also describes the two mappings of the syslog protocol to TCP connections, both which are helpful for transmitting trustworthy delivery of event messages. This administers a trivial mapping maximizing backward compatibility and also helps in supplying a more entire mapping. Both provides a degree of sturdiness and security in message delivery that is engaged to the usual UDP-based syslog protocol, by providing encryption and authentication over a connection-oriented protocol.

3.2 Forward Integrity for Secure Audit Logs

M. Bellare and B. S. Yee[3] explaining as: Applications incorporate more secure audit logs (e.g., syslogd data) for intrusion exposure or accountability, communications security, and authenticating incomplete results of computation for mobile agents. Computer audit logs including descriptions of notable events which crashes of system programs, system resource consumption, failed login attempts, etc. Many of these events are serious for investigating analysis after a break-in. The rst aim of an experienced attacker will be the audit log system: the attacker desires to remove traces of the compromise, to avoid detection as well as to maintain the method of attack undisclosed so that the security gap broken will not be detected by the system administrator. To construct the audit log secure, we must avoid the attacker from modifying the audit log data.

3.3 Logcrypt: Forward Security and Public Verification for Secure Audit Logs

J. E. Holt[9] predictable as: The famous application Tripwire manages cryptographic fingerprints of all files on a computer granting the administrators to identify when attackers compromise the system and modify the essential system files. But Tripwire is incompatible for system logs and other files that alters often, since the fingerprints generates affect to files in their intactness. A number of peoples have projected cryptographic techniques which permit each new log entry to be fingerprinted, blocking attackers from discarding proof of their attacks from system logs.

3.4 Secure Audit Logs to Support Computer Forensics

B. Schneier and J. Kelsey[8] discussed on the following: In many real-world applications, sensitive data are put in logs which are fewer on an un trusted machine. When an incident takes place as an attacker controls this machine, it is assured that the attacker will achieve tiny or no information from the log less and to bound his ability to damage the log files. Here the projected system shows a computationally inexpensive method for making all log entries generated earlier to the logging machine's compromise unfeasible for the attacker to read and also unfeasible to unnoticeably change or destroy. A computer that uses logs of different kinds of network activity wishes to have log entries of an attack undeletable and not alterable, even in the occasion that an attacker takes over the logging machine over the network. An intrusion-detection system that logs the starting access and exit of people into a secured region desires to oppose attempts to scrub out or alter logs, even after the machine on which the logging takes place has been taken over by an attacker.

3.5 A New Approach to Secure Logging

D. Ma and G. Tsudik[6] stated as :The necessity for secure logging is well-understood by the security professionals, counting both researchers and practitioners. The capability to professionally validate all log entries is more essential to any purpose handling secure logging techniques. In this paper, we start by investigating state-of-the-art in secure logging and recognize some troubles inborn to systems based on trusted third-party servers. They suggest a very dissimilar approach to secure logging based upon newly developed Forward-Secure Sequential Aggregate authentication techniques.

3.6 On the Security of Public Key Protocols

D. Dolev and A. Yao[10] explained as: newly the use of public key encryption was to offer a secure network communication which has established a significant attention. Such public key systems are frequently useful in providing against the passive eavesdroppers, who regularly try to strike the lines and try to decode the message. It has been

pointed out, that an inappropriate designed procedure could be susceptible to an active behavior like that, one who may imitate another user or change the message being transmitted. numerous models have been prepared in which the security of protocols are discussed accurately. Algorithms and characterizations are used in finding protocol security in these models which have been given. The use of public key encryption was to offer a secure network communication which has established substantial attention.

4. PROPOSED WORK

The increasing popularity of cloud-based data and mobile devices has led to the appearance of a number of latest information services to meet people's needs. At the same time, there is an increasing attentiveness of the problem of personal information becoming public and of the require to be proficient to use personal data while keeping it private. In this paper we are introducing the concept of homo morphic encryption. Homo morphic encryption means it is a form of encryption which allows particular types of computations to be takes place on cipher text and produce an encrypted result which, when decrypted, matches the result of operations carried out on the plaintext in this way security achieved is more.

Encryption is an helpful way to defend data, although in most encryption methods, data needs to be temporarily decrypted in order to perform calculations such as totals. This is problematic because the data becomes exposed the moment it is decrypted. Homo morphic encryption, however, allows for calculations to be performed on data in an encrypted manner, making it a talented technique for delivering new cloud services.

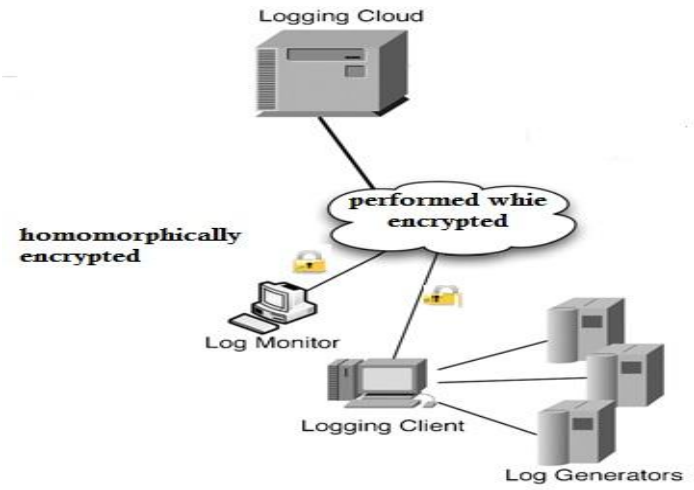

Fig 1. System Architecture

5. CONCLUSIONS

In this project, a comprehensive system to securely contract out log records to a cloud service provider. It analyzed presented results and recognized troubles in the present operating system based logging services such as syslog and practical difficulties in some of the existing secure logging methods and discover the challenges for a secure cloud based log management service.

Homo morphic implementation of log management system to carry out the implementation of encrypted query operating on encrypted data. We discussed a simple homo morphic encryption scheme as a orientation model. The basic homo morphic scheme will not get a efficient processing of queries over encrypted log records and also have drawbacks. In Future to remove drawback there is need to developed sophisticated homo morphic encryption method.

REFERENCES

[1]. C. Lonvick, The BSD Syslog Protocol, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.
[2]. D. New and M. Rose, Reliable Delivery for Syslog, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.
[3]. M. Bell are and B. S. Yee, "Forward integrity for secure audit logs," Dept. Computer. Sci., Univ. California, San Diego, Tech. Rep., Nov. 1997.
[4]. Bala Bit IT Security (2011, Sep.). Syslog-ng—Multiplatform Syslog Server and Logging Daemon [Online]. Available: http://www.balabit. Com /network-security / syslog-ng
[5]. J. Kelsey, J. Callas, and A. Clemm, Signed Syslog Messages, Request for Comment RFC 5848, Internet Engineering Task Force, Network Working Group, May 2010.
[6]. D. Ma and G. Tsudik, "A new approach to secure logging," ACM Trans .Storage, vol. 5, no. 1, pp. 2:1–2:21, Mar. 2009.
[7]. U. Flegel, "Pseudonymizing unix log file," in Proc. Int. Conf. Infrastructure Security, LNCS 2437. Oct. 2002, pp. 162–179.
[8]. B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," ACM Trans. Inform. Syst. Security, vol. 2, no. 2, pp. 159–176, May 1999.
[9]. J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in Proc. 4th Australasian Inform. Security Workshop, 2006,pp. 203–211.
[10]. D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inform. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[11]. K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92
[Online].Available:http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf