Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Enhanced secure log record management system in Cloud

Banumathi.D
PG Scholar, Department of CSE,
Sri Shakthi Institute of Engineering & Technology,
Anna University, Chennai

Dr. Kannammal K E
Professor, Department of CSE,
Sri Shakthi Institute of Engineering & Technology
Anna University, Chennai

Abstract -- A log is the record of events occurring within an organization that containing systems and networks. Log records are mainly used for many purposes like to evaluate the system performance, to identify the malicious attack, with troubleshooting problems and any policy violations. As this log file plays an important role and also it contains sensitive information, it ought to be maintained very securely. The integrity of the log file and that the logging process needs to be ensured at all time. So, management and securely maintenance of log records are terribly tedious task. The capital expenses will be very high to maintain log data for many organizations over a long period. Another solution is to maintain log records over a cloud database. Log files with sensitive information over a cloud environment will lead to challenges about confidentiality and privacy. So we propose an effective, secure cloud-based log management and also the use of homomorphism encryption as a solution for dealing the issues to access a cloud based data storage and also it greatly reduces the communication overhead between a large monitor and logging cloud.

Keywords -- cloud computing, log record management, integrity, security, confidentiality, homomorphic encryption

I. INTRODUCTION

A Log file is to record the detailed information of every event of a system or application running in an organization. Logging is important because log data can be used for many purposes like to identify malicious attack, to evaluate system performance, to identify violation of policy, and to troubleshoot problems. Securely maintaining log record is very important since log data records events such as user activities which become main target for attackers. An attacker, who breaking into a system, generally would not leave traces of his or her activities behind. So the attacker will try to damage log records first. Furthermore, the sensitive information contained in log files often directly contributes to confidentiality breaches. Example is that when user mistakenly enters his password in the username field at that time when he logged into system, then logging program take password as username in this way breaches the privacy. In the above observations, it is very important that logging process should be provided in a secure manner and that the log records are protected for a predetermined amount of time.

There is various traditional protocol available for logging which are mainly based on syslog [7] have not been designed with such security features. Hence security extensions protocol such as syslog-ng [1], syslog-sign [6], Syslog-pseudo [4], reliable syslog [8] and forward integrity for audit logs [2] have been proposed. But these protocols do not protect the log records from end point attacks. Besides, log management requires storage and processing ability. The log service must be able to store data in an organized manner and provide a fast and useful retrieval facility. These records should be able to be accessed by outside auditors also. Deploying a secure logging infrastructure to meet all these challenges entails significant infrastructural support and capital expenses that many organizations may find overwhelming. Cloud computing offers a better long-term storage and maintenance of organization's log record with low cost opportunity. Organizations can outsource the long-term storage requirements of log files to the cloud. Pushing log records to the cloud, introduces a new challenge in storing and maintaining log records. Since the cloud provider who providing a single service into many organizations would be benefit from economies of scale.

In this paper, we address integrity and security challenges involved in storing and maintaining log records in cloud servers. We propose not only cryptographic algorithm to address confidentiality and security problems but also propose a cloud-based homomorphic encryption method which reduces the communication overhead in cloud environment. Our proposal is to encrypt data before sending it to the cloud provider, but to execute the calculations the data should be decrypted every time we need to process it. Until now it was not to encrypt data and to trust a third party to keep them safe. So to allow the Cloud provider to perform the operations on encrypted data without decrypting them requires using the Homomorphic Encryption.

II. RELATED WORK

A number of approaches have been proposed for logging information in computing systems. Most of these protocols supported a protocol referred to as syslog. Syslog protocol transfers the log data to syslog server by using UDP (User Datagram Protocol).Thus, there is no reliable delivery of log messages. And furthermore it doesn't defend the log information from end-point attacks.

Syslog-ng [8] is a replacement that is backward compatible with syslog. Syslog-ng uses TCP(Transmission Control Protocol) for reliable log record delivery and uses SSL (Secure Socket Layer) to supply integrity and confidentiality throughout transit. However, syslog-ng does not protect against log data modifications when it resides at an end-point.

Syslog - sign which provides integrity to log message, replay resistance, message sequencing, and detection of missing messages by using two additional messages using signature block and certificate block but this protocol does not provide confidentiality or privacy during the transmission of data or at the end points.

Syslog - pseudo protocol uses the pseudonymizer filters to substitute pseudonyms for specific fields in the log record. Thus, strictly speaking, this protocol does not ensure correctness of logs. Once log records are substituted by some values they cannot be retrieving back.

Reliable-syslog [6] aims to implement reliable delivery of syslog messages. It is built on top of the blocks extensible exchange protocol (BEEP) which runs over TCP to provide the required reliable delivery service. But it does not protect the log data from privacy and confidentiality breaches.

Schneierand Kelsey proposed a logging scheme for cloud that relays on forward integrity and assures it. Forward integrity of log data used to protect the log data from insertion, deletion and modification of log data. But it does not address the confidentiality and privacy problems with log file storage and retrieval.

Table 1 indicates the protocol and their satisfied security requirements

Table 1. Secure logging protocol and their Security requirements

Protocol Proposed Models	**Scientist Name**	**Security Requirements**			
		Confidentiality	**Integrity**	**Reliable Delivery**	**Authentication**
Syslog	C.Lonvick, Aug 2001	no	no	no	no
Syslog-ng	Balabit, 2011	yes	yes	yes	no
Syslog-sign	J. Kelsey & J.Callas, May2010	no	yes	no	yes
Reliable-syslog	D. New &M. Rose, Nov 2001	yes	yes	yes	yes
Secure Logging As A Service-	Indrajit Ray & K.Belyaev, June 2013	yes	yes	yes	yes

In the existing work, all vehicles relied on a Trusted Authority (TA) for controlling the overall network which leads to the need of a centralized authority. It is infeasible for any attacker to compromise. Thus, creates a burden to message authentication scheme and overload to Trusted Authority. Since TA acts as administrator that maintains message authentication and management of network, TA load increases due to large number of received messages.

Secure logging as a service which was proposed by Ray and Belyaev uses aggregated MAC (Message authentication code) [5].secure logging as a service consists of log generators, logging client and logging cloud. The log generators are computer device used to generate the log data and it is stored temporarily then moved to logging client. The logging client is a collector that receives groups of log records from log generator and uploaded in batches to logging cloud.

The logging cloud provides long term storage and maintenance service to log data received from different logging clients. The logging cloud is maintained by cloud service provider. Only those organizations that have subscribed to the logging cloud's services can upload data to the cloud. Even though secure logging as a service satisfies most of the security requirements. The encryption technique used here affects overall performance of the system.

III. PROPOSED SYSTEM

Homomorphic encryption scheme is used to reduce the communication overhead, without compromising privacy and security of log data. Homomorphic Encryption systems are used to perform various operations on the encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. The logging client can encrypt the log data x and send encryption Enc(x) to the logging cloud. The logging cloud can take the ciphertext Enc(x) and evaluate a function f obtaining result Enc (f(x)). The logging client can decrypt this result but the logging cloud never learns anything about the data that computed on.

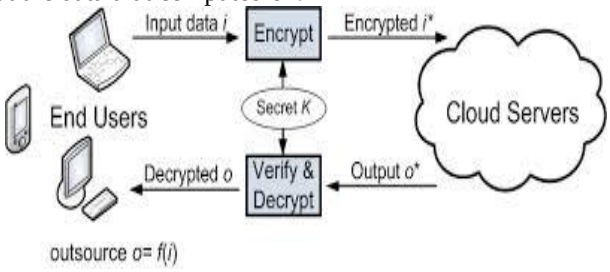

Fig 1 Homomorphic encryption process

Fig 1 explains about the homomorphic encryption. A homomorphic (public-key) encryption scheme HE = (Gen, Enc, Dec, Eval) is a quadruple of probabilistic polynomial-time (PPT) algorithms as follows.

• **Key generation**: The algorithm **(pk, sk) ←Gen *(1^k)*** takes a unary representation of the security parameter and outputs a public encryption key pk**,** and a secret decryption key ***sk.***

• **Encryption**. The algorithm ***c*←Enc*(pk,μ)*** takes the public key pk and a single bit message μ ∈ {0, 1} and outputs a ciphertext c.

• **Decryption.** The algorithm: ***μ**←Dec*(sk,c)*** takes the secret key sk and a ciphertext c and outputs a message μ ∈ {0, 1}.

• **Homomorphic evaluation.** The algorithm ***c*←Eval(pk,*f*,c_1,...,c_l)** takes the evaluation key pk, a function f: {0, 1}^{l} → {0, 1} and a set of l ciphertexts c1, . , c l, and outputs a ciphertext c.

.

$$P_r\left\{\mu^*=f(c_1,\ldots,c_2)\;\middle|\;\begin{array}{c}(pk,sk)\leftarrow Gen\,(1^{\lambda})\\ c_1\leftarrow Enc(pk,\mu_1),\ c_2\leftarrow Enc(pk,\mu_2),\ldots,\ c_l\leftarrow Enc(pk,\mu_l)\\ c\leftarrow Eval(pk,f,c_1\ldots c_l)\\ \mu^*\leftarrow Dec\,(sk,c)\end{array}\right\}=1\text{-}negl(\lambda)$$

If c is the class of all function, then we call it as fully-homomorphic encryption. Evaluation is public process the adversary can perform the homomorphic evaluations themselves without the help of logging client which created the log data. Thus with the help of the above mention equation overhead is reduced. Below. Fig 2. explains that the homomorphic performance is better than RSA approach.

Fig 2. Performance evaluation between RSA and Homomorphic system

IV. CONCLUSION

Logging plays a very important role in the proper operation of an organization's information processing system. Sometimes the log record contains sensitive information that should be maintained very securely. However, maintaining logs securely over long periods of time is difficult and expensive in terms of the resources needed. Hence, we designed a protocol which simultaneously provides the needed security and privacy features. This protocol reduces the communication overhead to a significant level and low cost for maintaining the log record.

REFERENCES

[1] BalaBit IT Security (2011, Sep.). *Syslog-ng - Multiplatform Syslog Server and Logging Daemon* http://www.balabit.com/networksecurity/syslog-ng

[2] Bellare.M and B. S. Yee, "*Forward integrity for secure audit logs* " Nov. 1997.

[3] Eckert.C and A. Pircher, "Internet anonymity: Problems and solutions," pp. 35–50. In Proc. Int. Conf. Inform. Security, 2001.

[4] Flegel.U, "*Pseudonymizing Unix log file*", Oct. 2002,. In Proc. Int. Conf. Infrastruture Security, LNCS 2437. Oct. 2002,.

[5] Indrajit Ray, kirill Belyeav, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram, *"Secure logging as a Service – Delegating Log Management to the Cloud "*.

[6] Kelsey.J, J. Callas, and A. Clemm, "*Signed Syslog Messages*", May 2010. RFC 5848,
[7] Lonvick.C, The BSD Syslog Protocol, Internet Engineering Task Force,Request for Comment RFC 3164,Network Working Group, Aug. 2001.
[8] New.D and M. Rose, Reliable Delivery for Syslog, Internet Engineering Task Force, Network Working Group, Nov. 2001. RFC 3195
[9] Rafael Accorsi, "*Safekeeping Digital Evidence - State of art and challenge*".
[10] Vinod Vaikuntanathan "*Homomorphic and General encryption Madars Virza 6.892 Computing on Encrypted Data* September 09, 2013

