ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Cloud-based Secure Log Management using Homomorphic Encryption to reduce Communication Overhead

Deepalakshmi.A[1], Mohanraj.T[2]

PG scholar, Department of CSE, Karpagam University, Coimbatore, Tamilnadu, India[1]

Assistant professor, Department of CSE, Karpagam University, Coimbatore, Tamilnadu, India[2]

**ABSTRACT-** Log record contains much useful information including user activity and used for many purpose like to evaluate system performance, to identify violation of policy, to identify malicious attack and to troubleshoot problems. It may also contain highly sensitive information. So it is important that any organization should ensure integrity, security and confidentiality of their log files. But deploying secure infrastructure for log record is very expensive. Hence in this paper, we delegating log record management to cloud to reduce the cost and simultaneously identify security challenges in cloud-based log management. We also try to reduce the overhead of communication in cloud environment using homomorphic encryption scheme.

**KEYWORDS-** cloud computing, log record management, integrity, security, confidentiality, homomorphic algorithm

## I. INTRODUCTION

Securely maintaining log record is very important since log data records events such as user activities which become main target for attackers. A malicious attackers who try to break system, would not leave trace of their activities behind. So the attacker will try to damage log records first and foremost. Further, the sensitive information in log files contributes to confidentiality and privacy breaches. There is various traditional protocol available for logging which are mainly based on syslog [1]. But main drawbacks of syslog based protocols are they lack in security features. Hence security extensions protocol such as syslog-ng [2], syslog-sign [3], Syslog-pseudo [4], reliable syslog [5] and forward integrity for audit logs [6] have been proposed. But these protocols provide either partial protection or do not protect from end point attacks. They also need large storage and processing capabilities. It is also important to provide quick and useful retrieval facility of stored data. These records should be able to be accessed by outside auditors also. Deploying a secure logging infrastructure which meets all the above mentioned challenges involves large capital expenses and significant infrastructural support which the organization may find intense. Instead we are pushing logging files to cloud.

Cloud computing offers a better long-term storage and maintenance of organization's log record with low cost opportunity. Since the cloud provider who store and maintain the log record, providing single service to many organizations that it will benefit from economics of scale. However pushing log data to cloud may introduces security and confidentiality challenges. The curious cloud provider may try to link log record related activities to their sources and try to get confidential information from log records.

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. We also use anonymizing protocol [7] to avoid correlating and linking of log records by the cloud provider with its respective log record generator and requesters.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The remainder of our paper is organized as follows. Section II explains existing protocol and its related properties. In Section III, we present the case study of secure logging as a service protocol. Section IV describes about homomorphic encryption scheme and we conclude our paper in section V.

## II. EXISTING PROTOCOLS

Many approaches have been proposed for storing log data. Most of these are based on a network logging protocol known as syslog. Syslog protocol transfers the log data to syslog server by using UDP(User Datagram Protocol). Hence in syslog the delivery of log messages is not reliable. And also it does not protect the log data from end-point attacks. Syslog-ng uses TCP(Transmission Control Protocol) for reliable log record delivery and uses SSL (Secure Socket Layer) to provide confidentiality and integrity during transit. However it does not protect log data modifications at end-points.

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 issues. Syslog-pseudo protocol uses pseudonymizer filter to substitute pseudonyms for specific fields in the log record. But it does not ensure correctness of log records. Reliable-syslog protocol provides trivial mapping backward compatibility. But it does not protect the log data from privacy and confidentiality breaches.

Table 1 indicates the protocol and their satisfied security requirements as per Safekeeping digital evidence [8]

TABLE 1
Secure logging protocol and their Security requirements

| Protocol | Security Requirements | | | |
|---|---|---|---|---|
| | Confidentiality | Authentication | Integrity | Reliable Delivery |
| **Syslog** | no | no | no | no |
| **Syslog-ng** | yes | no | yes | yes |
| **Syslog-sign** | no | yes | yes | no |
| **Reliable Syslog** | yes | yes | yes | yes |
| **Secure logging as service** | yes | yes | yes | yes |

Forward-integrity of log data used to protect the log data from insertion, deletion and modification of log data. But it does not provide privacy and suffers from truncation attack. Secure logging as a service [9] which was proposed by Ray and Belyaev uses aggregated MAC (Message authentication code).

The system architecture of 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. The log file generated are temporarily stored and then pushed to the logging client. The logging client collects the log record and uploaded in batches to logging cloud. The logging cloud receives log record from different logging client from different organizations.

The logging cloud is maintained by cloud service provider. Only authorized and subscribed organization can upload, store or delete data from logging cloud. Log monitor is used to review the log data and to generate queries to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

retrieve log data. This protocol ensures security, integrity and confidentiality features of log data not only during generation phase of log record but also during transmission phase. The secure logging as a service enables the integrity of log data by using Forward-Integrity protocol and ensures authentication by using aggregated MAC. It also ensures confidentiality using RSA (Rivest, Shamir and Adleman) encryption schemes. It also use anonymous upload, deletion and rotation of log file by using the k-times anonymous authorization protocol [10] for authentication of logging client. In addition, the secure logging as a service satisfies the following property.

a. Correctness
b. Verifiability
c. Tamper Resistance
d. Privacy

## III. CASE STUDY

Even though secure logging as a service satisfies most of the needed security requirements, the encryption technique used here affects the overall performance of the protocol. We designed a set of simulations that allows us to analyze the effectiveness of encryption setting in our prototype. We designed test scenarios to understand the overhead that arise during log record generation process. We kept batch size of encrypted log record as 10, 20, 30 and 40. For each and every log batch, we analyzed and measured 3 different log file preparation settings. First, we measured the total time taken to fill up the log batch with log records without any security protocol which results in best achievable performance. Next, we measured an overhead for filling up log batch with partial security related log preparation which includes unencrypted log record and aggregated MAC function. Finally we measured an overhead with encrypted log records and aggregated MAC functions. That is with full security preparation. The results are shown in Fig.3(a). X-axis represent batch size and Y-axis represents overhead in milliseconds. The overhead is about twice in adopting complete security preparation compared to no security.

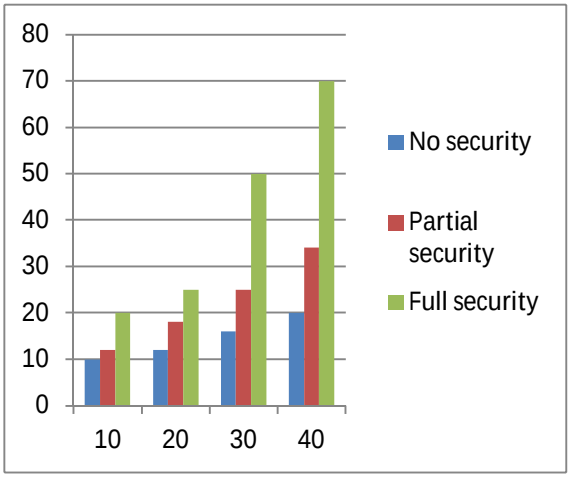


Fig 3(a) Batch Creation overhead.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## IV. HOMOMORPHIC ENCRYPTION

In order to reduce communication overhead, without compromising privacy and security of log data we performing homomorphic encryption scheme[11] instead of general encryption. Homomorphic encryption permits to compute on encrypted data. 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.

Assume that encryption scheme is c-homomorphic, where c is the class of function supported. If c is the class of all function, then we call it as fully-homomorphic encryption.

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

If c is the class of all function, then we call it as fully-homomorphic encryption. Eval 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.

## V. CONCLUSION

Log record contains many useful information. Thus it is important to securely maintain the log record for proper operation of an organization's information process management system. However, securely maintaining log record over extended period of time is expensive. Hence, we designed a protocol which simultaneously provides the needed security and privacy features. At the same time, it reduces the communication overhead to a significant level and promises a low cost opportunity for maintaining log records.

## REFERENCES

[1]C. Lonvick, The BSD Syslog Protocol, Internet Engineering Task Force,Request for Comment RFC 3164,Network Working Group, Aug. 2001.
[2]BalaBit IT Security (2011, Sep.). Syslog-ng - Multiplatform Syslog Server and Logging Daemon.http://www.balabit.com/networksecurity/syslog-ng
[3]J. Kelsey, J. Callas, and A. Clemm, "Signed Syslog Messages", May 2010. RFC 5848,
[4]U. Flegel, "Pseudonymizing Unix log file", Oct. 2002,. In Proc. Int. Conf. Infrastruture Security, LNCS 2437. Oct. 2002,.
[5]D. New and M. Rose, Reliable Delivery for Syslog, Internet Engineering Task Force, Network Working Group, Nov. 2001. RFC 3195
[6]M. Bellare and B. S. Yee, "Forward integrity for secure audit logs Nov. 1997.
[7]C. Eckert and A. Pircher, "Internet anonymity: Problems and solutions," pp. 35–50. In Proc. Int. Conf. Inform. Security, 2001. [8]Rafael Accorsi, "Safekeeping Digital Evidence - State of art and challenge".
[9]Indrajit Ray, kirill Belyeav, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram, "Secure logging as a Service – Delegating Log Management to the Cloud ".
[10]I. Teranishi, J. Furukawa, K. Sako, "k-times anonymous authentication..2004, pp. 308–322.in Proc. 10th Int. Conf. Theor. Appl. Cryptology Inform. Security.
[11]Vinod Vaikuntanathan "Homomorphic and General encryption Madars Virza 6.892 Computing on Encrypted Data September 09, 2013.