International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Design of Secure Log Management Over Cloud

Harshal N. Kolhe[1], Imran R. Shaikh[2]

[1]Department of Computer Engineering, S.N.D.College of Engineering, Babhulgaon. Dist- Nashik, Maharashtra, India

[2]Professor, Department of Computer Engineering, S.N.D. College of Engineering, Babhulgaon. Dist-Nashik, Maharashtra, India

Abstract: ***A Log is consists of much helpful data regarding activities or events of systems and networks and these data having number of attributes and own syntax. These logs are made-up of events which has been done by users on systems or in networks. These information is very expensive for organizations. These logs are used for finding problems, to optimize performance, to record all events, and to investigate malicious activity in systems or networks. So, protection from attackers is required. Hence organization should maintained integrity, confidentiality, security of logs. The capital expenses will be very less to maintain logs for organizations for longer period. Hence in this paper, we propose more effective secure cloud based log management to decrease cost and provide security of logs from attackers. By using encryption and MAC provide secured log.***

Keywords: Cloud computing, privacy, Integrity, security, log record management

1. Introduction

A Log information is the records the information of all events or activities on a system or application or on network running in any organization. Log files are very important to find problems immediately. They have occurrences and able to solve problems. Log files are used to identify the security incidents, fraudulent activities, and policy violations. Logs consists of expensive and important information for organization so there should be some protection from third party attacker.

1.1 Log Generation and Maintenance

The log generation is depends on protocols on syslog. We have to achieve securities of logs likes provide partially protections, syslog-sign, syslog-ng, integrity of audit logs, delivery of syslogs and many more from attackers.

Now-a-days size, format of security log are increased faster. These logs require number of steps to computer secure log management. Steps are generations, storage, analyzing, transmission, displaying of secure log data.

For any type of organization have log generation and maintenance is more complicated by number of factors, like lot of log resources, improper log contents, lack of proper format, and timestamps of sources, and large volumes of log data. Log management require maintenance also, this maintenance means to achieve properties for e.g. confidentiality, integrity, and availability of logs. To Designing secure logging information for all the above challenges cloud management is best way for any organization.

1.2 Delegating Logs to Cloud storage

The cloud storage is best medium to storage purposely and having access from any where. The cloud storage have to minimum resources from end users. In cloud storage any type of data is delivered as a service (Xaas) and there are three main service model :

1) **Software as a Service (SaaS)** - This Software as a Service is to provide or deliver softwares over internet. SaaS consist of running the software on the provider's cloud infrastructure. The software delivery is to a single or multiple clients as per demand through a thin client (e.g. browser) .
2) **Platform as a Service (PaaS)** - This Platform as a Service provides the flexibility for a client to building, developing, testing and deploying applications on provider's platform. PaaS hoster provides the infrastructure besides PaaS. The provider provides the platform and development tools to the end PaaS user.
3) **Infrastructure as a Service (IaaS)** -This Infrastructure as a Service provides access to resources as on demand such as networking related works, servers and storage for organization, can be accessed with a service API.

The ownership over the infrastructure of cloud computing is depends on following four deployment models and this raises security issues.

A. **The Public Cloud** – It is basic view of cloud computing. This Public cloud generally owned by large organization, to make its infrastructure for providing availability to the general public over the Internet by a multitenant model on self-service basis. This Public cloud is cost effective cloud for saving, security, privacy issues from physical/ actual location of the infrastructure provides.
B. **The Private Cloud** – This private Cloud infrastructure is used by a single tenant environment, and which is to be manage by the single tenant organization or by third party within or outside the tenant premises. This cloud having more cost than the public cloud model.
C. **The Community Cloud** – This Community Cloud model infrastructure used or shared by multiple organizations of a specific community, which is to be managed by any one of the organizations or a third party.
D. **The Hybrid Cloud** – This Hybrid Cloud model is a combination of any two or all of the three models discussed above. However user can select the models based on organization's requirements but the major security issues raises in cloud computing are availability of data, data secure, third party control, Privacy and legal issue based on the model.

1.3 Secure logging and It's challenges :

The above discussed issues over a cloud environment have to provide a secured logging as a services, there are some properties to achieve are as below:

a) **Availability** – Availability property of a cloud management describes that the logs over cloud storage must be available any time as per required. This availability is a high prior for cloud database users.
b) **Verifiability:** Verifiability with respect to Cloud management property is to verify each and every entry in the log is present and does not modified from attacker. Each and every entry in logs must be verified its authenticity independent of others, and there must be all entries have linked together in such a way that to determine whether any entries are missing or not by using this linked entries..
c) **Privacy**: On Cloud, Log records would be distributed globally which may raises issue of data exposure and privacy of information over a Cloud.
d) **Confidentiality**: Log records should not be easily searched to get sensitive information called as Confidentiality. Only Legitimate search access to users such as auditors or system administrators should be allowed. No one have privileges to prevent an attacker who has logging system from accessing sensitive information that the system would put information in future log entries, aim of this to protect the pre-compromised log records from confidentiality breaches.

To achieve all these above challenges a secure way log generation for e.g. extracts, transforms, and encryption must be required.

2. Literature Survey

This section describes some techniques for Secure Logging with disadvantages as shown in Table 1.

C. Lonvick, D.Ma and Indrajit Ray and co-authors introduced the major techniques and models used for secure logging. The different authors introduced different techniques, but these are often so inaccurately in practice it is not possible to verify performance.

Table 1: Various techniques for Secure Logging with disadvantages

Name of Researcher	*Month and Year*	*Proposed Technique*	*Disadvantages*
M. Bellare & B.S.Yee	Nov 1997	Forward integrity of log information	Requires guaranteed server to maintain secret keys, and it may be attacked by unauthenticated user.
C. Lonvick	Aug 2001	Syslog	Uses UDP protocol. UDP Protocol is not providing reliable delivery of log message.
D.New & M.Rose	Nov 2001	Reliable Syslog	Doesn't prevent against confidentiality breaches.
U.Flegel	Oct 2002	Syslog-pseudo	Not ensure about correctness of logs.
J.E.Holt	2006	Logcrypt	Truncation Attack possible.
D.Ma & G. Tusdik	March 2009	Forward Secure sequential aggregate authentication	Efficient but very costly method
J.Kelsey & J.Callas	May 2010	Syslog-sign	Does not provide privacy or confidentiality during transmission of data or at end.
Balabit IT Security	Sept 2011	Syslog-ng	Does not protect against log data modification.
Indrajit Ray & K. Belyaev	June 2013	Secure Logging As A Service-Delegating Log Management to the Cloud	Most efficient and secured technique but loosely coupled architecture.

3. Proposed Work

The most contributions are the design for the various parts of the system and develop encrypted protocols to maintain integrity and confidentiality problems during storing, maintaining, and retrieving log records at the honest however curious cloud provider and in transit. One most disadvantage of existing system is that it cannot show the confidentiality and privacy with log file storage and retrieval. The client uploads information in batches wherever every batch is delimited by a start-of-log record and an end-of log record. The cloud provider can get log records from its authenticated clients. Thus, throughout upload logging client must authenticate to cloud to prove that the client had obtained previous authorization from the logging cloud to use the latter's services. However, it cannot wish the identity of the logging client to be connected to any of its transactions include the authentication method. For this purpose develop four protocols for retrieval, deletion, upload of log knowledge.

3.1 Upload-Tag Generation

An uploaded log batch of log records should be stored with index key. Index key is most important to provide guarantee that key value can't be suggested to the logging client or the logging monitor to seek the data. So, the log data is to be store at the cloud by generator upload tag. This upload tag has been created by the logging client in co-operation with the log monitor. It is generated by publicly available data. To Retrieved log details from the cloud by the logging monitor can send a request of retrieve to the logging cloud using upload tag. The upload tag is not sent in an encrypted message. Any attacker can try to use the upload-tag to retrieve the log data. The log data must be deciphered if and only if the corresponding decryption key is available.

3.2 Upload logs data

The entity that requires to that upload the log data sends a request message. In the request message consists of the upload-tag of related to the desired log data. By using the

communication channel the logging monitor can send log data to the logging cloud. In the upload message none value use individually or in a group can be tied to the logging client. The logging cloud and logging monitor send pre-defined formatted message to the logging cloud in order to the upload or retrieve any piece of information.

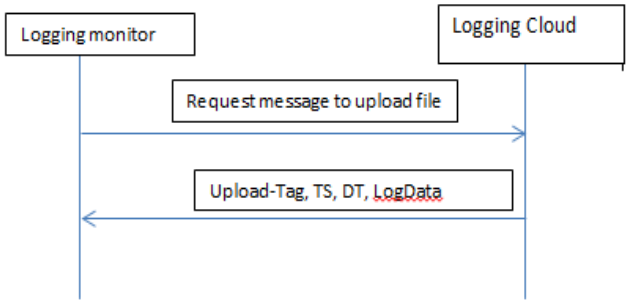

Figure 1: Protocol for Upload Log

3.3 Retrieve Log Data

This protocol is use to download log data from cloud, and send retrieve request with the upload-tag corresponding to the desired log data. The logging cloud can get the data from its storage location and sends that data over the channel to the requester. The cloud provider does not require to authenticate the requester of logging client. This is require for quality of the log batches has been encrypted, the retrieved data is useful only to those who have the valid decryption keys.

Figure 2: Protocol for retrieve Log

3.4 Delete Logs

The requester sends an delete message to the logging cloud to delete log data. The cloud gives the response to requester as a challenges to the requester. The authorization proves to delete by presenting a correct delete tag.

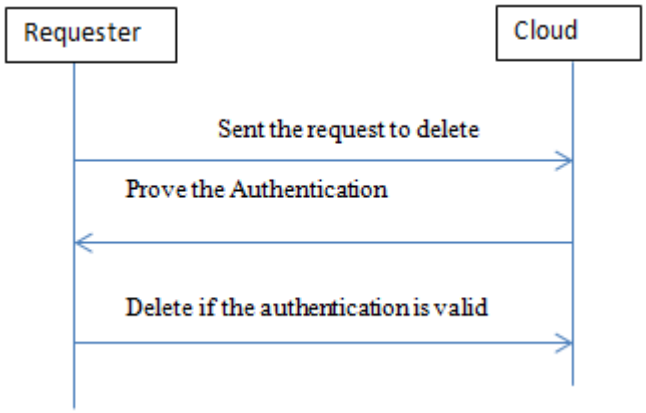

Figure 3: Protocol for Delete Log

4. System Architecture

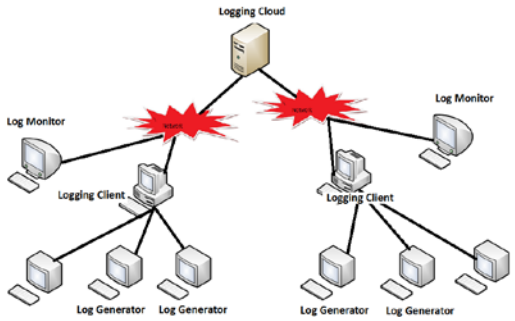

Figure System Architecture

The Architecture of the secure cloud log management system is shown in above Fig. There are four important parts in this system.

1) Log Generators
Log Generators are computing devices that are use to generate log information. Each and every organization that adopts the cloud-based log management services to log generates. Every generator is capable of logging. The log files generated by these hosts aren't hold on local machine except temporary until they're pushed to the logged client.

2) Logging client or Logging Relay:
The logging client is act as collector that receives group of log records generated by one or a lot of log generators, and prepares the log information in order to that it may be pushed to the cloud for future storage. The log information is transferred from the generators to the client in batches, either on a schedule, or as and once required depends on the quantity of log information waiting to be transfer. The logging client combines security protection on batches of accumulated log information and pushes every batch to the logged cloud. Once the logging client pushes log information to the cloud it acts as a logging relay. The term logging client and logging relay use to interchangeably. The logging client or logging relay may be enforced as group of collaborating hosts. For simplicity, we tend to assume that there's one logging client.

3) Logging Cloud
The logging cloud provides future storage and maintenance service to log information received from completely different logging clients to different organization. The number of logging cloud is maintained by a cloud service provider. Those organizations that have signed to the cloud's services will transfer information to the cloud. The cloud, as per demands from a company can delete log information and perform log rotation. Before the cloud can delete or rotate log information it require a proofs from the requester that the latter is allowed to form such demands. The logging clients generates such proofs. However, the proof may be given by the logging client to any entity that it needs to authorize.

4) Log Monitor
These are hosts that can be used to monitor and review log information. They'll generate queries to retrieve log information from the cloud. These monitors can perform additional analysis as per demands. They'll additionally raise

the log cloud to delete log information for good, or rotate logs.

We assume that the organization maintains the log generators and also the logging client. The log monitor may be maintained by organization or may be a separate entity. The logging client also can play the role of a log monitor. We tend to develop our model that the log monitor could be a separate entity that's trust by the logging client. The logging client and log monitor operate freely of every other, they'll communicate in asynchronous manner. This implies that if a logging client needs to send some information to the log monitor (vice versa), the sender can't expect the receiver to be on-line to receive the info. As a result the sender has got to publish the info in some location and also the receiver wants retrieve the info from there once required. The logging cloud facilitates this communication by receiving and servcing applicable requests. The logging client and also the log monitor communicates with the external world, over associate an unencrypted network that gives full-duplex communication. Our proof-of thought example gets this service from the network. Attacks on the Tor network that breach anonymity of communication parties, are well studied and solutions planned. Protect the communication channel is on the far side the scope of this paper.

5. Conclusion

In this paper we've got reviewed some existing techniques for secure logging system. For every technique, we've got provided detail explanation with the new contributions and limitations. From this analysis, variety of short and limitations were highlighted of those techniques. Further study of development of efficient technique, use cloud architecture for secured log with encrypted log records. And to construct architecture that reduces cost and overhead to secure log records of an organization.

References

[1] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, DieudonneMulamba, MariappanRajaram "Secure Logging As a Service—Delegating Log Management to the Cloud" IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013
[2] U.S. Department of Health and Human Services. (2011, Sep.). HIPAA—General Information [Online]. Available: https://www.cms.gov/hipaageninfo
[3] PCI Security Standards Council. (2006, Sep.) Payment Card Industry (PCI) Data Security Standard—Security Audit Procedures Version 1.1 [Online]. Available: https://www.pcisecuritystandards.org/pdfs/ pci−audit−procedures−v1-1.pdf
[4] Sarbanes-Oxley Act 2002. (2002, Sep.). A Guide to the Sarbanes-Oxley Act [Online]. Available: http://www.soxlaw.com/
[5] C. Lonvick, The BSD Syslog Protocol, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.
[6] D. New and M. Rose, Reliable Delivery for Syslog, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.
[7] M. Bellare and B. S. Yee, "Forward integrity for secure audit logs," Dept. Comput. Sci., Univ. California, San Diego, Tech. Rep., Nov. 1997.
[8] BalaBit IT Security (2011, Sep.). Syslog-ng—Multiplatform Syslog Server and Logging Daemon [Online]. Available: http://www.balabit.com/network-security/syslog-ng
[9] J. Kelsey, J. Callas, and A. Clemm, Signed Syslog Messages, Request for Comment RFC 5848, Internet Engineering Task Force, Network Working Group, May 2010.
[10] 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.
[11] U. Flegel, "Pseudonymizing unix log file," in Proc. Int. Conf. Infrastruture Security, LNCS 2437. Oct. 2002, pp. 162–179.
[12] C. Eckert and A. Pircher, "Internet anonymity: Problems and solutions," in Proc. 16th IFIP TC-11 Int. Conf. Inform. Security, 2001, pp. 35–50 .
[13] M. Rose, The Blocks Extensible Exchange Protocol Core, Request for Comment RFC 3080, Internet Engineering Task Force, Network Working Group, Mar. 2001.
[14] 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.
[15] J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in Proc. 4th Australasian Inform. Security Workshop, 2006, pp. 203–211.
[16] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgeneration onion router," in Proc. 12th Ann. USENIX Security Symp., Aug. 2004, pp. 21–21.
[17] The Tor Project, Inc. (2011, Sep.) Tor: Anonymity Online [Online]. Available: http://www.torproject.org
[18] 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.
[19] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[20] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. Nat. Comput. Conf., Jun. 1979, p. 313.
[21] R. Ostrovsky and M. Yung, "How to withstand mobile virus attack," in Proc. 10th Ann. ACM Symp. Principles Distributed Comput., Aug.1991, pp. 51–59.
[22] 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.
[23] I. Teranishi, J. Furukawa, and K. Sako, "k-times anonymous authentication (extended abstract)," in Proc. 10th Int. Conf. Theor. Appl. Cryptology Inform. Security, LNCS 3329. 2004, pp. 308–322.
[24] D. L. Wells, J. A. Blakeley, and C. W. Thompson, "Architecture of an open object-oriented database management system," IEEE Comput., vol. 25, no. 10, pp. 74–82, Oct. 1992.
[25] K. Nørv°ag, O. Sandst°a, and K. Bratbergsengen, "Concurrency control in distributed object oriented database systems," in Proc. 1st East-Eur. Symp. Adv. Databases Inform. Syst., Sep. 1997, pp. 32–32.

[26] R. Droms, Dynamic Host Configuration Protocol, Request for Comment RFC 2131, Internet Engineering Task Force, Network Working Group, Mar. 1991.
[27] Project: AN.ON—Anonymity Online. (2012, Mar.). JAP Anonymity and Privacy [Online]. Available: http://anon.inf.tu-dresden.de/index−en.html
[28] Ultrareach Internet Corporation. (2012, Mar.). Ultrasurf—Privacy, Security, Freedom [Online]. Available: http://ultrasurf.us/index.html
[29] Global Internet Freedom Consortium. (2012, Mar.). FreeGate [Online]. Available: http://www.internetfreedom.org/FreeGate
[30] 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