

Construction on Log Management to Public Cloud

Sohail Nawaz Parvez¹, Meghraj Dilip Borole², Sangeeta Nageshwarrao Varsala³, Abhilasha Namdeo Mahale⁴, Prof. B.A.Abhale⁵

¹²³⁴student, Dept. of Information Technology Engineering, SNDCOE, Maharashtra, INDIA

⁵Professor, Dept. of Information Technology Engineering, SNDCOE, Maharashtra, INDIA

Abstract- A Log records are important info that is said to activities of systems, applications or networks and these log records having varied fields and their syntax. really logs are mechanically generated on activities that are done and doing by user on system, or on any Applications like Google Chrome or in networks. These logs are pricey and want to any organization for future references like to spot or finding any issues, to record all events, to search out performance, and to analyze malicious activities in systems or networks or in application. So, protection of logs from attackers is needed. Hence organization ought to maintain integrity, confidentiality, and security of logs. the value to keep up logs for organizations for extended amount is incredibly less. Hence, we have a tendency to developed secure log management over cloud to decrease value in addition as offer security of log from attackers. to attain this, we've got done this with the assistance of Blowfish algorithm to cipher log records then SHA-1 is employed to produce confidentiality whereas transmittal and at finish purpose security purpose we have a tendency to used Shamir's Secret sharing algorithm.

Keywords—privacy, encryption, security, cloud computing, log record management, integrity, secret sharing.

Introduction

A Log is that the recording the data of activities on systems or applications like Google chrome or on networks running in any organization. Log files

are terribly helpful to seek out drawback. Log records are use to unravel issues like to spot the deceitful works, security incident, and any policy violations. Log consists of expensive, useful, and really vital info for any organization thus that's why we've to supply protection from third party assaulter.

Generation and Maintenance of Log

The generation of log is depends on activities done on any application like we've used History of Google chrome may be a log file to system. These log having range of steps to figure secured log management. Steps are generation of log, storage of log, analyzing of log, transmission, displaying of secure log information. For any style of organization needed log generation and maintenance. however it's a lot of difficult by some factors like lack of log resources, improper logs content, lack of correct format, and timestamp of every sources, and enormous or serious volumes of log information. Log management consist maintenance section, this maintenance means that to realize properties for instance confidentiality, integrity, and handiness of logs. To planning secure work info for all the higher than challenges

cloud management is best approach for any organizations.

Logs storage to Cloud

The storage on cloud is that the best medium for storage designedly and user will access from anyplace. The storage on cloud needed minimum resources to finish users. In storage on cloud, any style of information is delivered acts as a service i.e. XaaS and there are some main services models :

Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)

The homeowners of the infrastructure of cloud computing is depends on following four readying models and this raises security problems.

A. Public Cloud: This Public cloud is value effective cloud for saving, security, privacy problems from physical/ actual location of the infrastructure provides.

B. Private Cloud: Private Cloud infrastructure is employed by one tenant atmosphere, and that is to manage by the only organization or by third party among or outside the premises

C. The Community Cloud: Community Cloud model infrastructure used or shared by multiple organizations of a particular community, that is to be managed by anybody of the organizations or a 3rd party.

D. The Hybrid Cloud: Hybrid Cloud model is combination of any 2 or all of the 3 models mentioned higher than.

Secured Log and challenge of Secured Log :

The higher than mentioned problems over a cloud surroundings got to give a secured work as a services, there square measure some properties to attain square measure as below:

Availability: convenience of cloud management is that the logs over cloud storage should be out there at any time as per demand.

Verifiability: Verifiability with relevance Cloud management property is employed to verify every and each entry within the log is gift and didn't modify from offender.

Privacy: On Cloud storage, Log records would be distributed globally which can raise issue of the information exposure and privacy of data over a Cloud.

Confidentiality: Log records shouldn't be simply searched to urge sensitive info referred to as Confidentiality. solely Legitimate search access to users like auditors or system directors ought to be allowed solely

To achieve these all higher than challenges a secure approach log generation for instance extracts, transforms, and cryptography should be needed.

LITERATURE SURVEY

Some techniques associated with work with disadvantages square measure as shown in Table one.

Table 1: Various techniques for Secure Logging with disadvantages

Researcher & Year	Technique	Drawback
M. Bellare, B.S.Yee. Nov- 1997	Forward integrity of log.	Requires guaranteed server to maintain secret keys
C. Lonvick Aug- 2001	Syslog	Uses UDP protocol Unreliable delivery of log message.
D.New, M.Rose Nov- 2001	Reliable Syslog	Does not prevent against confidentiality.
U.Flegel Oct- 2002	Syslog-pseudo	Does not ensure about correctness of logs.
J.E.Holt 2006	Logcrypt	Truncation Attack can be done.
D.Ma, G. Tusdik March- 2009	Forward Secure sequential aggregate authentication	Efficient but more costly
J.Kelsey, J.Callas May- 2010	Syslog-sign	Does not provide privacy or confidential during transmission
Balabit IT Security Sept- 2011	Syslog-ng	Does not protect against log data alteration.
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.

SYSTEM ARCHITECTURE

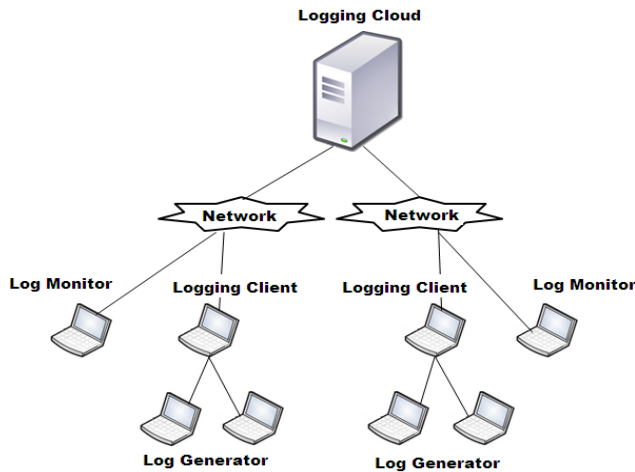


Figure 1: System Architecture

The design of the secure log management over Cloud system is shown in Fig. There square measure four vital components during this system.

1) **Log Generators:** Log Generators square measure computing devices that square measure wont to generate log data of associate degree Application like Google Chrome. each generator is capable of work. The log files generated by these hosts don't seem to be hold on native machine except temporary till they are pushed to the logged shopper.

2) **Logging Client:** The Client is act as collector that receives cluster of log records generated by one or variety of log generators, and prepares the log data so as to it it should be pushed to the cloud for future storage. The log data is transferred from the generator to the shopper in batches, either on a

schedule, and once needed depends on the amount of log data waiting to be transfer. The client combines security protection on batches of accumulated log data and pushes each batch to the logged cloud. Once the work shopper pushes log data to the cloud it acts as a work relay. The term work shopper and work relay use to interchangeably. The Client could also be implemented as cluster of collaborating hosts. For simplicity, we have a tendency to tend to assume that there is one client & Client is capable to perform secret writing of Log and generate code to produce security of Logs throughout transmission also as at the top additionally by victimization Shamir's secrete Sharing formula.

3) **Logging Cloud:** The Logging provides future storage and maintenance service to log data received from utterly totally different work shoppers to different organization. the amount of work cloud is maintained by a cloud service supplier. Those organizations that have signed to the cloud's services can transfer data to the cloud. The cloud, as per demands from an organization will delete log data and perform log rotation. Before the cloud will delete or rotate log data it needed proof from the requester that the latter is allowed to create such demands. The work shoppers generate such proof. However, the proof could also be given by the work shopper to any entity that it has to authorize. once work cloud is logged, Logs encrypted also as shared is to be hold on on cloud.

4) **Log Monitor:** Log monitor square measure hosts that may be wont to monitor and review log data. they will generate queries to retrieve log data from the cloud. These monitors will perform further analysis as per demands. They will in addition raise the log cloud to delete log data permanently, or rotate logs. we have a tendency to assume that the organization maintains the log generators and additionally the work shopper. The log monitor could also be maintained by organization or could also be a separate entity. The work shopper can also play the role of a log monitor. we have a tendency to tend to develop our model that the log monitor can be a separate entity that is trust by the work shopper. The work shopper and log monitor operate freely of each alternative, they will communicate in asynchronous manner. this means that if a work shopper has to send some data to the log monitor (vice versa), the sender can't expect the receiver to be on-line to receive the data. The work cloud facilitates this communication by receiving and sexual union applicable requests.

These square measure main components of our system. largely we have a tendency to use the Log generators of lower configurations. Client and Log monitor is one and same system. And work Cloud is use as non-public cloud to storage purpose.

The most contributions square measure the look of the varied components of the system and developed encrypted protocols to keep up

confidentiality and integrity issues throughout maintaining, storing, and retrieving log records at the honest but curious cloud supplier and in transit. Disadvantage of existing system is that it can't show the privacy and confidentiality with log file storage and retrieval. The shopper uploads the knowledge in batches and each batch is delimited by begin of log record and finish of log record. The cloud supplier gets log records from its documented shoppers. The throughout transfer work shopper should certify to cloud to prove the shopper had obtained previous authorization from the work cloud to use the services. However, it can't want the identity of the work shopper to be connected to any of its transactions embrace the authentication methodology. For this purpose we have a tendency to develop four protocols for transfer, retrieval, deletion of log knowledge on cloud with secure manner that steps square measure as follows.

Upload log Generation

We have uploaded log records from shoppers. The log of Google Chrome is generated from variety of shoppers. So, the log knowledge may be store at the cloud once transfer. This transfer is completed by the work shopper. To Retrieved log details from the cloud by the work monitor will send asking of retrieve to the work cloud. Any assailant will attempt to use the transfer knowledge to retrieve the log knowledge. The log knowledge should be deciphered if and

providing the corresponding secret writing key's out there.

Retrieve Log knowledge

This Retrieve Log knowledge is use to transfer or retrieve log knowledge from cloud. The work cloud will retrieve information from its storage location and sends that data over the channel to the requester. The cloud supplier doesn't need authenticating the requester of work shopper. this can be needed for quality of the log batches has been write in coded; the retrieved knowledge is beneficial solely to people who have the valid secret writing keys to encrypt logs.

Delete Logs

The requester sends delete message to the work cloud to delete log knowledge. The cloud provides the response to requester as challenges to the requester. The authorization proves to delete by presenting an accurate delete tag.

ALGORITHM

1. Blowfish Algorithm for Encryption of Log record:

1. Blowfish Algorithm:

1. Divide input x into two 32-bit halves: x_L , x_R .

2. Then, for $i = 1$ to 16:

$$x_L = x_L \text{ XOR } P_i$$

$$x_R = F(x_L) \text{ XOR } x_R$$

Swap x_L and x_R

3. After the sixteenth round, swap x_L and x_R again to undo the last swap.

4. Then, $x_R = x_R \text{ XOR } P_{17}$ and $x_L = x_L \text{ XOR } P_{18}$.

5. Finally, recombine x_L and x_R to get the ciphertext.

2. SHA-1 is used for MAC

SHA1 stands for Secure Hashing Algorithm. It is the improvement upon the original SHA0. SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications. SHA1 outputs a 160bit digest of any sized file or input. It uses a 512 bit block size and has a maximum message size of $2^{64}-1$ bits:

SHA1 Algorithm Description:

1. Padding

(a) Pad the message with a single one followed by zeroes until the final block has

448 bits.

(b) Append the size of the original message as an unsigned 64 bit integer.

2. Initialize the 5 hash blocks (h0,h1,h2,h3,h4) to the specific constants defined in the SHA1 standard.

3. Hash (for each 512 bit Block)

(a) Allocate an 80 word array for the message schedule

i. Set the _rst 16 words to be the 512 bit block split into 16 words.

ii. The rest of the words are generated using the following algorithm.

Word[i-3] XOR word[i-8] XOR word[i-14] XOR word[i-16] then rotated 1 bit to the left.

(b) Loop 80 times doing the following.

i. Calculate SHAfunction() and the constant K (these are based on the current round number.

ii. e=d

iii. d=c

iv. c=b (rotated left 30)

v. b=a

vi. a = a (rotated left 5) + SHAfunction() + e + k + word[i]

I Add a,b,c,d and e to the hash output.

4. Output the concatenation (h0,h1,h2,h3,h4) which is the message digest.

3. Shamir's Secret Sharing algorithm for Sharing:

It divides knowledge D into n items in such the simplest way that D is definitely reconstruct from any k items, however even complete information of k - one items reveals completely no info regarding D. this method allows the development of sturdy key management schemes or cryptological schemes that may operate firmly and dependably even once misfortunes destroy 0.5 the items and security breaches expose virtually one amongst the remaining items. we tend to generalize the matter to 1 within which the key is a few knowledge D (e.g., the safe combination) and within which non-mechanical solutions (which manipulate this data) also are allowed.

Our goal is to divide D into n items D1, ..., Dn in such the simplest way that:

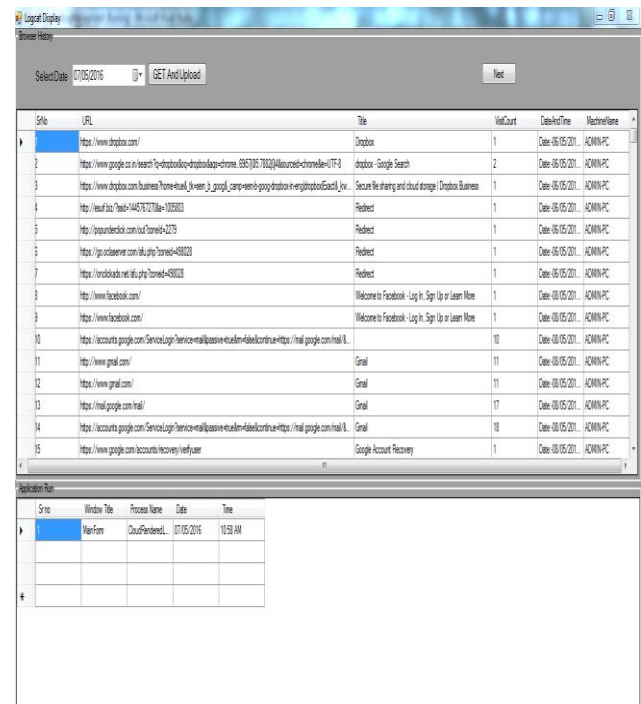
(1) information of any k or a lot of Di items makes D simply computable;

(2) information of any k - one or fewer Di items leaves D fully undetermined (in the sense that every one its potential values area unit equally likely). Such a theme is termed a (k, n) threshold theme. economical threshold schemes may be terribly useful within the management of cryptological keys.

Result: The Performance is required to find out the quality of Construction of Log Management to Public Cloud with another existing log management system. When we measured to Construction of Log management to Public Cloud

with security, we have provided system which having more security of the logs.

We have constructed this system with 3 algorithms to improve previous systems. First Blowfish algorithm is used because this is more secured and required less space than other algorithms. Secure Hash Algorithm 1 is chosen because outputs a 160 bit digest of any size file. It uses a 512 bit block size and has a maximum message size of 264-1bits. And lastly, we used Shamir's secret Sharing algorithm to protect against attackers at the end side of storage . With the help of these three algorithms we have constructed this system. In this system, log file is history file of google chrome as a input. These history files are logs of different systems of users. Then we have encrypted that records by using blowfish algorithm and generate MAC for sender as well as for receiver to provide security during transmission using SHA algo. For more security, we have again encrypte that MAC and log record. At the end, we had stored the information on cloud with secret sharing in number of parts. When records are stored on cloud that is in encrypted format and when we want retrieve records then decryption is required. According to the above parameters , our system is more secured, and required less time as well as takes less space to manage Logs over Cloud.



SNo	URL	Title	VisitCount	Date	MachineName
1	https://www.dropbox.com/	Dropbox	1	Date: 16/05/2011	ADMINPC
2	https://www.google.co.in/search?q=dropbox&dropbox=chrome:5957397702&hlsource=chrome&itf=9	dropbox - Google Search	2	Date: 16/05/2011	ADMINPC
3	https://www.dropbox.com/business/home?view=9&view=2_group&camp=seem-b-population&e=engine&open=Google	Secure file sharing and cloud storage Dropbox Business	1	Date: 16/05/2011	ADMINPC
4	http://search.twitter.com/search?q=dropbox&lang=en	Feedlist	1	Date: 16/05/2011	ADMINPC
5	http://www.underlock.com/out/turned+4275	Feedlist	1	Date: 16/05/2011	ADMINPC
6	https://go.scoopster.com/64.php?turned+49323	Feedlist	1	Date: 16/05/2011	ADMINPC
7	https://viralchicken.net/64.php?turned+49323	Feedlist	1	Date: 16/05/2011	ADMINPC
8	https://www.facebook.com/	Welcome to Facebook · Log In, Sign Up or Learn More	1	Date: 16/05/2011	ADMINPC
9	https://www.facebook.com/	Welcome to Facebook · Log In, Sign Up or Learn More	1	Date: 16/05/2011	ADMINPC
10	https://accounts.google.com/ServiceLogin?service=mail&passive=true&dm=facebook&continue=https://mail.google.com/mail/&		10	Date: 16/05/2011	ADMINPC
11	http://www.gmail.com/	Gmail	11	Date: 16/05/2011	ADMINPC
12	https://www.gmail.com/	Gmail	11	Date: 16/05/2011	ADMINPC
13	https://mail.google.com/mail/	Gmail	17	Date: 16/05/2011	ADMINPC
14	https://accounts.google.com/ServiceLogin?service=mail&passive=true&dm=facebook&continue=https://mail.google.com/mail/&		18	Date: 16/05/2011	ADMINPC
15	https://www.google.com/accounts/Recovery/verifyuser	Google Account Recovery	1	Date: 16/05/2011	ADMINPC

SNo	Window Title	Process Name	Date	Time
1	MainForm	CloudPentestL...	07/05/2016	10:58 AM

fig: Generation of logs file

Conclusion

Log records area unit important to any organization. Log is that the activities or event that area unit done by user. This logs area unit most significant to assaulter. This logs keep secured is extremely vital to organization. And organization needs to stay records for extended time with less value. we've got achieved this with the assistance of some algorithmic rules like Blowfish cryptography algorithm to cipher logs then SHA-1 for Message Authentication Code to supply confidentiality whereas sending knowledge from sender to receiver and the other way around. Finally, Shamir's Secrete Sharing algorithmic rule

is employed to stay encrypted logs on numerous location.

REFERENCES

- [1] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, Mariappan Rajaram "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. Infrastructure Security, LNCS 2437. Oct. 2002, pp. 162–179.
- [12] M. Rose, The Blocks Extensible Exchange Protocol Core, Request for Comment RFC 3080, Internet Engineering Task Force, Network Working Group, Mar. 2001.
- [13] 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
- [14] J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in Proc. 4th Australasian Inform. Security Workshop, 2006, pp. 203–211.

- [15] 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.
- [16] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
- [17] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Comput. Conf.*, Jun. 1979, p. 313.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] K. Nørveg, O. Sandst^oa, 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.
- [22] R. Droms, *Dynamic Host Configuration Protocol, Request for Comment RFC 2131*, Internet Engineering Task Force, Network Working Group, Mar. 1991.
- [23] 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>