Cloud information accountability using cloud log security protocols

A.PUNITHA ANGEL MARY[1], P.MALARKODI[1]

Abstract

Log records are the vital source of information, which stores data about user activities and events in the network of an organization. As increasing number of organizations moves their operations over cloud, sensitive log data should be ensured for security, data integrity, data redundancy, and confidentiality. Cloud, being a public space and vulnerable to hackers and intruders through its accessibility via internet, hence tracking, recording, monitoring and storing log records securely in cloud is unambiguously needed. Log data are generated and maintained by both Cloud Service provider (CSP) and Cloud users in cloud "as a service" models. This papers implements and analyses cloud based log management framework, which is used for generating, storing, and optimizing data storage in cloud. The log data are stored and monitored frequently and audited in regular intervals. This assures for the security and intrusion free computing over cloud. An alert will be thrown for occurrences of any unusual activities.

Keywords: cloud security, logging, and cloud based log management framework.

I. INTRODUCTION

Log data is a record of events and user activities that occurs in an organization network. Log data can be used to track and monitor any unusual activities, troubleshoot errors, enhance system's performance, detect occurrence of policy violations, and to record user activities and events. Log files contains vital information about the organization it might me the target for intruders and attackers. An attacker while intruding into our system will try not leaving any traces of attacks or his activities in the network. The attacker tries to get any confidential or useful information from the log record. The attacker could intrude the log data that is being transmitted to the cloud, intercept it and replay it to the cloud. Conventional security protocols such as syslog and the likes are not designed with such security measures.

A.Punitha Angel Mary & P.Malarkodi M.E – Pervasive Computing Technologies, Kings College Of Engineering, Tamilnadu, India.

II. SYSTEM ARCHITECTURE

The system architecture represents the operations and collaborations of the each entity. Cloud is the public space where several tenants use the same resources for their computing and storage operations. The data owner and cloud user interacts with the cloud and performs their tasks over it. Then their activities are recorded and encrypted, uploaded as jar files to the cloud space. The data owner is provided with the log data through emails in the push mode and they can view log data using pull mode.

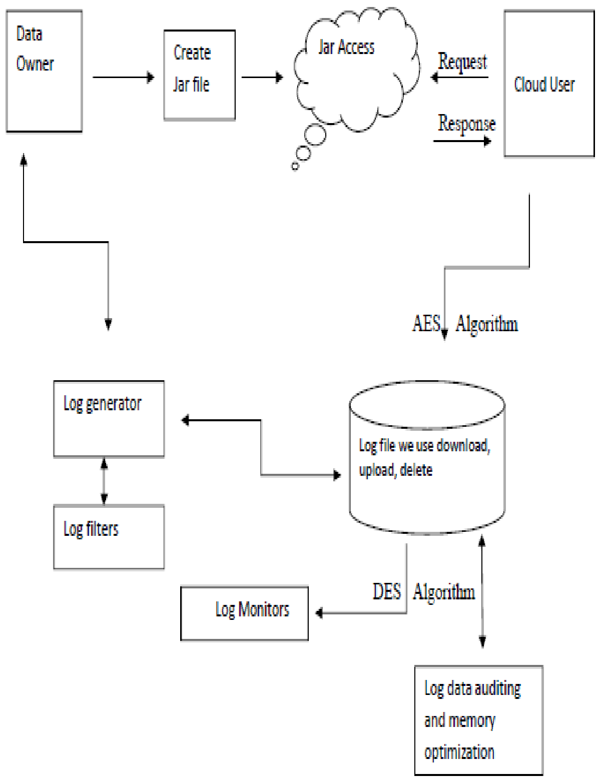

Fig – 1: system architecture

The system contains a log generator which monitors user activity and generate logs based on the prescribed format. The generated logs are converted to JAR files and then encrypted using AES algorithm. The encrypted logs are transferred to the database. The user can view any logs modify and delete on a later time to audit it.

A. Log Generators

These are the computing devices that generate log data. Each organization that adopts the cloud-based log management service has a number of log generators. Each of these generators is up to with logging capability. The log files generated by these hosts are not stored locally except temporarily till such time as they are pushed to the logging client.
Log generators are deployed with log filters, which are used to filter and remove unwanted log data before transmitting it to cloud.

B. LOGGING CLIENT OR LOGGING RELAY

The logging client is a collector that receives groups of log records generated by one or more log generators, and prepares the log data so that it can be pushed to the cloud for long term storage. The log data is transferred from the generators to the client in batches, either on a schedule, or as and when needed depending on the amount of log data waiting to be transferred. The logging client incorporates security protection on batches of accumulated log data and pushes each batch to the logging cloud. When the logging client pushes log data to the cloud it acts as a logging relay. We use the terms logging client and logging relay interchangeably. The logging client or relay can be implemented as a group of collaborating hosts. For simplicity however, we assume that there is a single logging client.

C. LOGGING CLOUD

The logging cloud provides long term storage and maintenance service to log data received from different logging clients belonging to different organizations. The logging cloud is maintained by a cloud service provider. Only those organizations that have subscribed to the logging cloud's services can upload data to the cloud. The cloud, on request from an organization can also delete log data and perform log rotation. Before the logging cloud will delete or rotate log data it needs a proof from the requester that the latter is authorized to make such a request. The logging client generates such a proof. However, the proof can be given by the logging client to any entity that it wants to authorize.

D. LOG MONITOR

These are hosts that are used to monitor and review log data. They can generate queries to retrieve log data from the cloud. Based on the log data retrieved, these monitors will perform further analysis as needed. They can also ask the log cloud to delete log data permanently, or rotate logs.

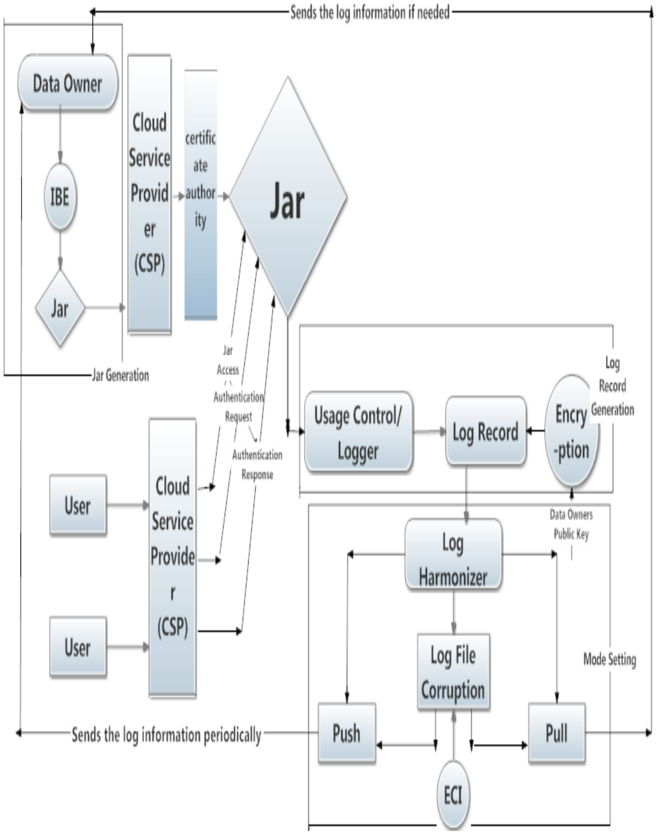

Fig – 2: data flow diagram

E. DOLEV- YAO ATTACKER MODEL

We assume the Dolev- Yao attacker model to study and analyze our threats that may be encountered In a cloud scenario.

1) The attacker can intercept any message sent over the Internet.

2) The attacker can synthesize, replicate, and replay messages in his possession.

3) The attacker can be a legitimate participant of the network or can try to impersonate legitimate hosts.

F. SELECTIVE LOG MAINTENANCE

The cloud users may not need to store all activities in the logs. The proposed system provides filters to some activities in the cloud storage spaces.

The log information before being uploaded to the cloud it is being allowed through a filter which in turn filters the unwanted log data. The filtered data is encrypted and uploaded from the database to the cloud.

G. MEMORY OPTIMIZATION IN DATABASES

Logs are stored, monitored and deleted after a prescribed time interval. To keep hold of logs related to extremely significant documents that has to be recorded for a prolonged or indefinite time, memory optimization technique is implemented. The log data are retrieved and audited, while auditing being completed log data are forwarded through a filtering component which deletes all data other than that are marked vital.

This process can be automated by marking into the related log data as the document is vital and all activities performed over the document are kept in database indefinitely.

III. ADVANCED ENCRYPTION STANDARD (AES)

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

IV. STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

Steganographic messages are often first encrypted by some traditional means, and then a covertext is modified in some way to contain the encrypted message, resulting in stegotext. For example, the letter size, spacing, typeface, or other characteristics of a covertext can be manipulated to carry the hidden message; only the recipient (who must know the technique used) can recover the message and then decrypt it

V. IMPLEMENTATION

The project is deployed in a prototype model, in which we used apache tomcat server to act as a virtual machine in our system. The data owner stores their data in cloud space in JAR format and it contains the information about the services provided by the owner. The user can access through their services and each event occurring in the system is recorded as logs. The logs may contain the data such as username, login, signup, sign out, download, upload, view, delete etc. each log entry contains details about username, file name, data and time, location, and their action. The logs are stored temporarily in a database and after auditing important log records are stored in the permanent database indefinitely.

VI. CONCLUSION AND FUTURE WORK

The project implemented deployed and analyzed the cloud log framework and automated selective log maintenance and memory optimizations. The future work involves analyzing its performance and efficiency in a realtime cloud environment and upgrading it to a product.

VII. REFERENCES

1. Secure Logging As a Service—Delegating Log Management to the Cloud, Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013
2. PROVENANCE MANAGEMENT IN CURATED DATABASES Peter Buneman, Adriane P. Chapman, James Cheney
3. BalaBit IT Security (2011, Sep.). Syslog-ng—Multiplatform Syslog Server and Logging Daemon [Online]. Available: http://www.balabit.com/network-security/syslog-ng.
4. K. Kent and M. Souppaya. (1992). Guide to Computer Security LogManagement, NIST Special Publication 800-92 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

5. D. New and M. Rose, Reliable Delivery for Syslog, Request for CommentRFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.
6. IDENTITY-BASED ENCRYPTION FROM THE WEIL PAIRING Dan Boneh, and Matt Franklin
7. R. Accorsi, “On the relationship of privacy and secure remote logging in dynamic systems,” in IFIP Security and Privacy in Dynamic Environments,S. Fischer-H¨ubner et al., Eds., 2006, vol. 201, pp. 329–339.
8. A Survey on Delegating Log Management to The Cloud, Sinu P S, M.Ananthi, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February-2014.
9. Internet Anonymity: Problems and Solutions, Claudia Eckert, Alexander Pircher, Springer.
10. E. Kenneally, “Digital logs – Proof matters,” Digital Investigation, vol. 1, no. 2, pp. 94–101, 2004.
11. J. Clark and J. Jacob, “A survey of authentication protocol literature,” 1997, available at http://www.cs.york.ac.uk/jac/papers/drareview.ps.gz
12. How to withstand mobile virus attacks Rafail Ostrovsky, Moti Yung., Proc. 10th ACM conference on principles of distributed systems, aug 1991
13. M. Alles, A. Kogan, and M. Vasarhelyi, “Black box logging and tertiary monitoring of continuous assurance systems,” Inf. Sys. Cont., 2003.
14. Log Data as Digital Evidence:What Secure Logging Protocols Have to Offer?, Rafael Accorsi, ieee explore, COMPSAC – 2009.
15. D. Ma and G. Tsudik, “A new approach to secure logging,” ACM TOS,vol. 5, no. 1, pp. 1–21, 2009.
16. How to Share a Secret, Adi Shamir. Communications of the ACM November 1979 Volume 22 Number 11
17. Hide and seek: an introduction to steganography - Niels proves, and peter honeyman, IEEE security and privacy, 2003.
18. Forward integrity for secure log audits, Mihir Bellare, Bennet.s. Lee.
19. Amazon Web Services Overview of Security Processes, amazon white paper, http://aws.amazon.com/security
20. The Dolev-Yao Intruder is the Most Powerful Attacker, Iliano Cervesat.
21. Security Analysis in the Migration to Cloud Environments, David G. Rosado, Rafael Gómez, Daniel Mellado and Eduardo Fernández-Medina, Future Internet 2012.

A.PUNITHA ANGEL MARY, and P.MALARKODI, are pursuing their Masters in Pervasive Computing Technologies in Kings College of Engineering Affiliated to Anna University. Area of interests includes Cloud Computing, Cloud Security, pervasive computing, and Networking.