Delegating Log Management to the Cloud by Secure Logging as a Service

[1]Priyadharshini.T.R - Final Year IT [2]Senbagavalli.M-Associate Professor/IT
[3]Saravana kumar.R -Associate Professor/IT
[123]Jayam College of Engineering and Technology, Dharmapuri, TamilNadu, India.

Abstract

Managing the Log Records is highly tedious and confidential in any organization. Even though Log Records contain Log Files, it should be protected from third party hackers. Since, Log Files contains privacy details and sensitive information. Delegating log management is cost saving measure.. In order to overcome from hackers we introduce a secure algorithm known as Advance Encryption Standard (AES). It provide secret key to both Client and Data Owners. It provides high Bandwidth & low level Inactivity. It's the cheapest method where an attacker cannot read or modify/destroy the data's. We can implement AES Algorithm for various Security Issues.

I. INTRODUCTION

A. Log Management

A LOG is a record of Events occurring within an organization's system or network. Logging is important because Log Data can be used to troubleshoot the problems. Log Records play a significant role in Digital Forensic Analysis of system. Log Service must be able to store data in an organized manner for Fast Retrieval of data. Cloud Computing-Low cost to store and manage Log Records in some orders[1]. Our main objective in this paper is to prove secure framework for data sharing in cloud computing environment. This project is based on security issues involved in log management for secure logging.

B.Cloud Computing

Cloud computing is an computing concept in which large number of computers are connected through a communication medium ie.network.Cloud computing services are Software As A Service (SaaS)-it is also called as cloud – based application. Servers are connected to users via. Internet and web browsers. Platform As A Service (PaaS)-open source software platform where cost and complexity of buying hardware and software is free.

Infrastructure As A Service(IaaS)- it provides hardware,network,,storage and data centre space.

II. KEY CONCEPTS: A VIEW

A. Servlets

Java Servlets are programs that run on a Web or Application server and act as a middle layer between a request coming from a Web browser or other HTTP client and databases or applications on the HTTP server and Servlets are platform-independent.

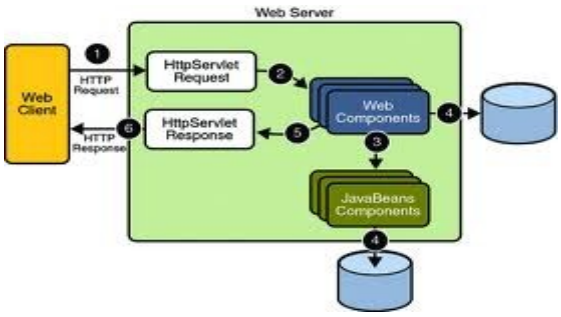

Fig 1. Servlet Architecture

B. JSP (JAVA SERVER PAGES)

Java Server Pages (JSP) technology provides a fast way to create dynamic web content. which helps developers insert java code in HTML pages by making use of special JSP tags, most of which start with <% and end with %>. JSP are platform-independent.JSP files are stored at server.JSP is an server side programming language.

ISSN: 2278 – 1323

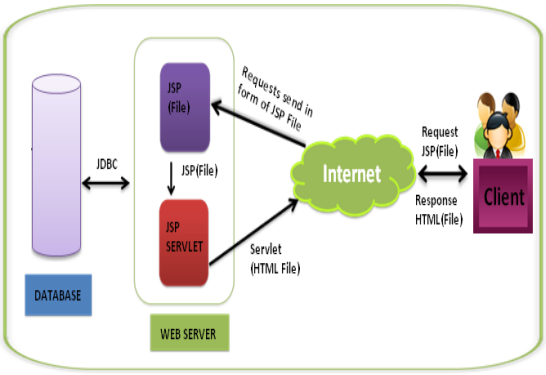

Fig. 2 JSP ARCHITECTURE

III. Existing System

Data handling in the cloud goes through a complex and dynamic hierarchical service chain. This does not exist in conventional environments. Ordinary web framework Uses web services for request and responses. The syslog protocol used UDP to transfer log information to the log server[3]. Thus, there is no reliable delivery of log messages, more over syslog doesn't protect Log Records during transit or at the end -points.

LIMITATIONS

- No security for user's data. No authentication or security provided
- Cost of implementation is high.
- Not suitable for small and medium level storage users.

IV. PROPOSED SYSTEM

We provide a solution for Storing and Maintaining Log Records in a Server Operating In a cloud based environment. We use Cryptographic Protocols for Integrity and Confidentiality Issues[2].We address security and integrity issues not only just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage, and retrieval.

Advantages

- It is suitable for large and limited number of storages.
- Protects from birthday attacks, JVM attacks and meet-in-the-middle attack.

V. LOG MANAGEMENT SYSTEM ARCHITECTURE

The overall architecture of cloud management is shown below. Log Clients consists of Log Generators which generates Log Records over the network. Log Monitors merge with network cloud to provide security.

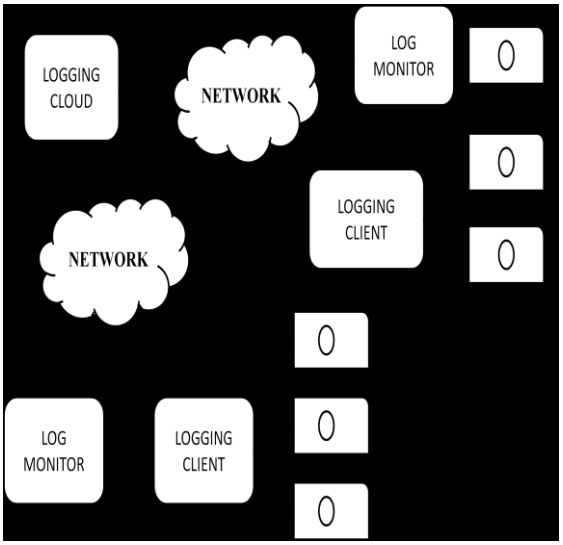

Fig 3. Log Management System Architecture

VI. MODULES

Modules Description

There are five different types of modules in this paper, that are listed in the following,

- Log Generators
- Logging Client or Logging Relay
- Logging Cloud
- Log Monitor

a) Log Generators

These are the computing devices that generate log data. Each organization hat 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.

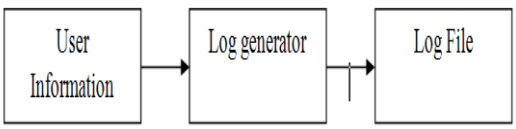

Fig 4. Log Generator

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. The log data is transferred from the generators to the client in batches, either on a schedule or amount of log data waiting to be

ISSN: 2278 – 1323

transferred. The logging client or relay can be implemented as a group of collaborating hosts.

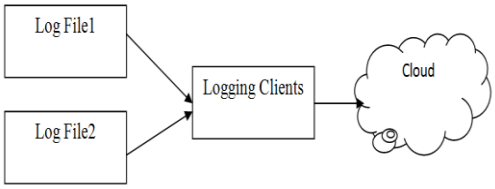

Fig 5. Logging Relay

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. Only those organizations that have subscribed to the logging cloud's services can upload data to the cloud**.**

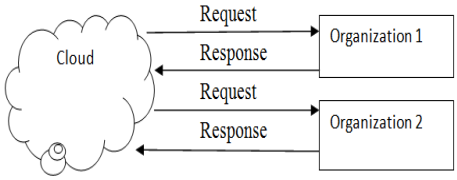

Fig 6 Logging Cloud

d) Log Monitor

These are hosts that are used to monitor and review log data. They can also ask the log cloud to delete log data permanently, or rotate logs[1]. 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.

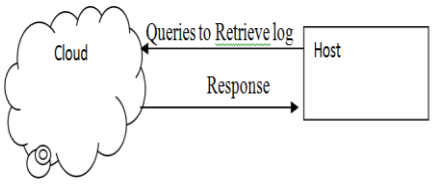

Fig 7 Log Monitor

VII. AES (Advanced Encryption Standard) ALGORITHM

Advance Encryption Standard is a symmetric 128-bit block data encryption technique. It works at multiple networks layers. It has fixed block size of 128-bits and a key size of 128,192 or 256-bits. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years[5].It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

a) ALGORITHM EXPLANATION:

AES is based on a design principle known as a Substitution permutation network. 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)[5]. Most AES calculations are done in a special finite field.

b) *APPLICATIONS OF AES*

The applications of Advance Encryption Standard are:

- Digital Cinema Projection System.
- Low Power Implementation for Bluetooth.
- Digital Cryptography

VIII. EXPERIMENTAL RESULTS

a) VIEW FILE

Clients can view the datas and informations of the Data Owners here.They can download the images once if the Data owners have given authentication to access it.

ISSN: 2278 – 1323

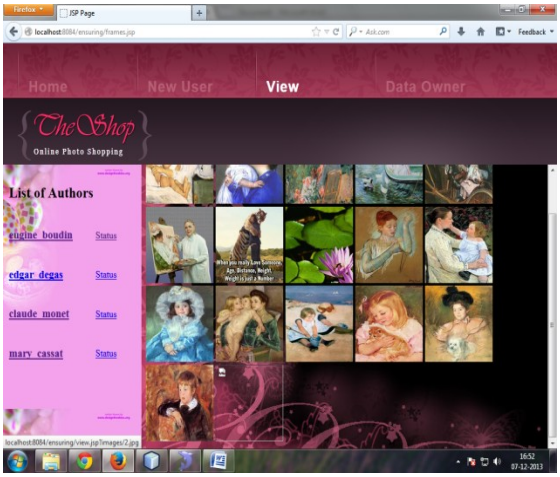

Fig 8. View File

b) SECURE CALCULATION

In order to provide security to images data owners provide a secure mathematical equation to solve and then download the images. This setup is for secure downloading.

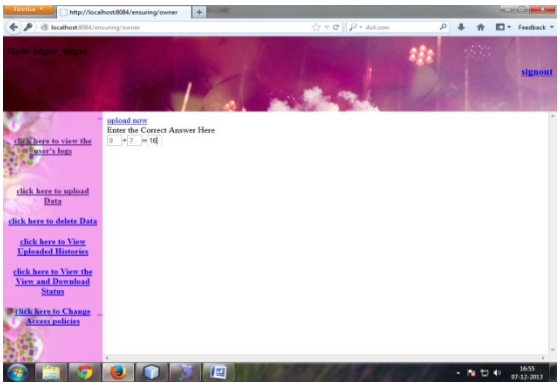

Fig 9. Secure Calculation

c) VIEW DOWNLOAD STATUS

Data owners can view there download status and uploaded histories in this setup.

Fig 10. View Download Status

IX.CONCLUSION

In our paper, we discussed the various security Issues by means of Advance Encryption Standard Algorithm. We choose AES Algorithm since the block size is fixed to 128-bit.It is the cheapest method and the attackers can hack data in three steps--First Attackers can interrupt messages over network. Second Attackers can replicate and replay messages. Third Attackers can justify the participant of the network. We have also provided solution for storing and maintaining log records in cloud-based environment. We have used cryptographic protocols for confidentiality issues. We provide security all the four stages of present system modules

X. FUTURE WORK

In future work, the present system module Log Client implementation is refined to replace the current log process. We have planned to investigate practical Homomorphism Encryption Schemes that allows encryption of Log Records with privacy and confidentiality.

HOMOMORPHIC ENCRYPTION

It is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

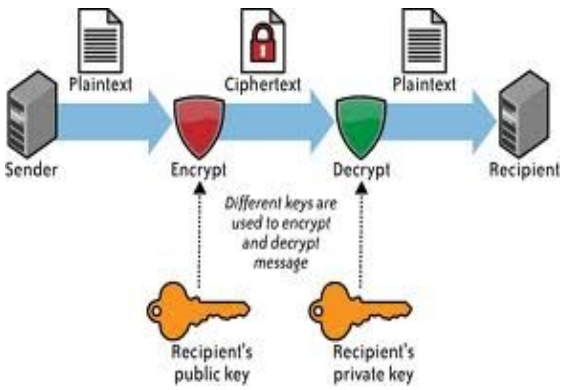

Fig 11. Homomorphism Encryption

ISSN: 2278 – 1323

XI. BIBLIOGRAPHY

[1] **K**. Kent and M. Souppaya (1992),"Guide to Computer Security Log Management" NIST Special Publication 800-92 [Online]. "http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf"

[2] U.S. Department of Health and Human Services.(2011,Sep.)"HIPAA—General Information [Online]".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].

[4] Sarbanes-Oxley Act 2002. (2002, Sep.).'' A Guide to the Sarbanes-Oxley Act [Online]''. Available: http://www.soxlaw.com/

[5] D. New and M. Rose, "Reliable Delivery for Syslog, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001''.

[6] 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.

[7] A. Shamir, "How to share a secret," Communication. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[8] G. R. Blakley, "Safeguarding cryptographic keys, "in Proc. Nat. Computer.Conf., Jun. 1979, p. 313.

[9] R. Ostrovsky and M. Yung, "How to withstand mobile virus attack,"
in Proc. 10th Ann. ACM Symp. Principles Distributed Computer., Aug. 1991, pp. 51–59.

[10] 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.

AUTHORS REFERENCES

Priyadharshini.T.R

B.Tech-IT Final Year

Jayam College of Engineering And Technology, Dharmapuri.

M.Senbagavalli Associate Professor/IT

B.Tech-IT

Sona College Of Engineering And Technology, Salem.

M.E-CSE

Jayam College of Engineering And Technology, Dharmapuri.

Currently pursuing Ph.D in Anna University Chennai.

R.Saravana Kumar

Associate Professor/IT

B.E-CSE

Bharathiryar University

M.E-CSE

Anna University Chennai

Currently working as an Assistant professor at the CSE Department

Jayam college of Engineering and Technology, Dharmapuri.

ISSN: 2278 – 1323