IJDCST @ Feb-March, 2014, Issue- V-2, I-2, SW-15
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

A New approach to secure logging-In cloud with the use of Cryptography Techniques

[1]V.Prathyusha[2]Dr.N. Chandra Sekhar Reddy[3]P.Ila Chandana kumari

[1]M.tech(CSE) prathyu.vissa@gmail.com Institute of Aeronautical Engineering,HYD-500043,AP,India.

[2]Professor, CSE Dept naguchinni@gmail.com Institute of Aeronautical Engineering,HYD-500043,AP,India.

[3]Associate Professor, MTech (CSE) ilachandana@gmail.com Institute of Aeronautical Engineering,HYD-500043,AP,India.

ABSTRACT: Securely maintaining log records over extended periods of it slow is unbelievably necessary to the correct functioning of any organization. Integrity of the log files that of the work process ought to be compelled to be ensured in any respect times. In addition, as log files often contain sensitive data, confidentiality and privacy of log records are equally necessary. However, deploying a secure work infrastructure involves substantial capital expenses that many organizations might notice overwhelming. Reputation log management to the cloud looks to be a viable worth saving measure. Throughout this paper, we've got an inclination to determine the challenges for a secure cloud-based log management service and propose a framework for doing constant.

Keywords: log records, sensitive data integrity

INTRODUCTION:

ALOG may be a record of events occurring within an organization's system or network. Work is very important because log information are often wont to troubleshoot issues, fine tune system performance, determine policy violations, investigate malicious activities, and even record user activities. Log records play a significant role in digital forensic analysis of systems. laws like HIPAA, Payment Card Industry information Security normal, or Sarbanes-Oxley often need forensically sound preservation of data. To befits these regulations, proof made in a court of law, as well as log records, should be unbiased, non tampered with, and complete before they'll be used. Since log files contain record of most system events as well as user activities, they become a very important target for malicious attackers. AN aggressor, breaking into a system, typically would attempt to not leave traces of his or her activities behind. Consequently, the primary issue AN aggressor usually will is to damage log files or interrupt the work services. Moreover, the sensitive info contained in log files usually directly contributes to confidentiality breaches. AN example of this is once logs contain information dealings information. Frequently, log info will be useful to AN aggressor in gaining unauthorized access to system. One example of this can be the case when a user erroneously enters her parole within the usernamefield where as work into a system. Work programs can store the parole because the user-id to record the data that a user has didn't log in. Last, however not least, info in log file can even be wont to cause privacy breaches for users in the system since the log file contains record of all events in the system. In lightweight of the higher than observations, it's vital that logging be provided in an exceedingly secure manner which the log records square measure adequately protected for a planned quantity of time (maybe even indefinitely). Ancient work protocols that square measure supported syslog haven't been designed with such safety features in mind. Security extensions that have been projected,

like reliable delivery of syslog forward integrity for audit logs often offer either partial protection, or don't defend the log records from finish purpose attacks. Additionally, log management requires substantial storage and process capabilities. The log service should be able to store information in associate degree organized manner and provide a quick and helpful retrieval facility. Last, but not least, log records might typically got to be created accessible to outside auditors World Health Organization aren't associated with the organization.

Deploying a secure work infrastructure to fulfill of these challenges entails important infrastructural support and capital expenses that a lot of organizations might notice over whelming. The rising paradigm of cloud computing guarantees allow value chance for organizations to store and manage log records in an exceedingly correct manner. Organizations will source the semipermanent storage necessities of log files to the cloud.The challenges of storing and maintaining the log recordsbecome a priority of the cloud supplier. Since the cloudprovider is providing one service to several organizationsthat it'll take pleasure in social science of scale. Pushing logrecords to the cloud, however, introduces abrand new challengein storing and maintaining log records. The cloud supplier can be honest however curious. This implies that it will strive notonly to urge direction directly from log records,but additionally link log record connected activities to their sources. Noexisting protocol addresses all the challenges that arise oncelog storage and maintenance is pushed to the cloud.

LITERATURE SURVEY:

1)Reliable Delivery and Filtering for Syslog

The Reliable Delivery and Filtering for Syslog feature allows a device to be customized for receipt of syslog messages. This feature provides reliable and secure delivery for syslog messages using Blocks Extensible Exchange Protocol (BEEP). Additionally, it allows multiple sessions to a single logging host, independent of the underlying transport method, and provides a filtering mechanism called a message discriminator. This module describes the functions of the Reliable Delivery and Filtering for Syslog feature and how to configure them in a network.

2) Guide to Computer Security Log Management

It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization. The publication presents log management technologies from a high-level viewpoint, and it is not a step-by-step guideto implementing or using log management technologies.

3)Explorative Visualization of Log Data to support Forensic Analysis and Signature Development

In this paper, we propose an approach for log resp. audit data representation, which aims at simplifying the analysis process for the security officer. For this purpose audit data and existing relations between audit events are represented graphically in a three dimensional space. We describe a general approach for analyzing and exploring audit or log data in the context of this presentation paradigm. Further, we introduce our tool, which implements this approach

and demonstrate the strengths and benefits of this presentation and exploration form.

4)On the Security of Public Key Protocols

The Use of public key encryption to provide secure network communication has received considerable attention.Such public key systems are usually very effective against a "passive" eavesdropper, namely, one who merely taps the communication line and tries to decipher the intercepted message. However, as pointed out in Needham and Schroeder an improperly designed protocol could be vulnerable to an "active" saboteur, one who may impersonate another user and may alter or replay the message. As a protocol might be compromised in a complex way, informalarguments that assert the security for a protocol are prone to errors

5)Architecture of an Open Object-Oriented Database Management System

An open, incrementally extensible object oriented database management system lets developers tailor database functionality for applications. It can also serve as a platform for research. This article describes the architecture of the Open OODB system. First wediscuss its requirements, then its computational model.Which builds databasefunctionality as an extensible collection of transparent extensions to existingprogramming languages. We also describe how Open OODB's *system architecture*is decomposed into a kernel *meta-architecture* and a collection of modules implementing specific behavioral extensions.Finally, we discuss risks of the approachand report on the project's status.

6)Concurrency Control in Distributed Object-Oriented Database Systems

In this paper we have given results from simulations with two different scheduler strategies. Further work for the DBsim simulator includes extensions that could make it more suitable for simulation of algorithms for object-oriented databases. Obviously, much more can be done with both the simulation model and the simulator. This includes adding new schedulers to the system, e.g., other versions of the two-phase locking scheduler, like wound-wait and wait-die. In a real system, replication is used for increased reliability and performance. This could also be integrated into this framework.

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.

LIMITATIONS:

- No security for user's data. No authentication or security provided
- High resource costs needed for the implementation.
- Not suitable for small and medium level storage users.

PROPOSED SYSTEM:

In this paper, we propose a comprehensive solution for storing and maintaining log records in a server operating in a cloud-based environment. 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. The major contributions of this paper are as follows. We propose architecture for the various components of the system and develop cryptographic protocols to address integrity and confidentiality issues with

storing, maintaining, and querying log records at the honest but curious cloud provider and in transit.

ADVANTAGES

- One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication.
- Providing defences against man in middle attack, dictionary attack, Disassembling Attack, Compromised JVM Attack
- It's Suitable for limited and large number of storages.

CONCLUSION:

We proposed a complete system to securely outsource log records to a cloud provider. We reviewed existing solutions and identified problems in the current operating system based logging services such as syslog and practical difficulties in some of the existing secure logging Techniques. In this work, find out the challenges for a secure cloud based log management service. The attackers use below three steps to hack. First, the attacker can intercept any message sent over the Internet. Second, the attacker can synthesize, replicate, and replay messages in his possession. And Last The attacker can be a legitimate participant of the network or can try to impersonate legitimate hosts. We implement how to store secure log file in cloud and that file we can change read, write, delete, upload and download. We can implement AES algorithm that uses for log monitor and log generator. We then proposed a comprehensive scheme that addresses security and integrity issues not just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage and retrieval. One of the unique challenges is the problem of log privacy that arises when we outsourced log management to the cloud. Log information in this case should not be casually linkable or traceable to their sources during storage, retrieval and deletion. We provided anonymous upload, retrieve and delete protocols on log records in the cloud using the Tor network. The protocols that we developed for this purpose have potential for usage in many different areas including anonymous publish-subscribe.

REFERENCES:

[1] 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

[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 Version1.1* [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-OxleyAct* [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 CommentRFC 3195, Internet Engineering Task Force, Network WorkingGroup, 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.