iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Secure Data Sharing in an E-Commerce Site on a Cloud Based Environment

S. Lovely Jacinth Kirthana[1], P. Durga Devi[2]
[1]M.E-CSE, Assistant Professor, [2]NPR College of Engineering and Technology

Abstract- ***Cloud computing provides services like infrastructure, software, applications and platform from a distant data centre to the client. Cloud computing has the advantage of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Privacy is always a concern in cloud computing because the service provider can access the data that is on the cloud at any time. Many cryptographic techniques are used to preserve data integrity from unauthorized users. The authenticity of the data in a insecure channel can be prevented using the cryptographic techniques and log generation scheme. This proposed system along with dynamic operation and public verifiability prevents adversary attack that takes place during the data sharing. This proposed system discusses the security issues involved in log management for a Secure Logging as a service and presents a design and implementation of a prototype delegating secure log manager. Main goal of a log manager in the third party auditor is to provide high bandwidth and low level inactivity. The sensitive information are kept in log files in cloud provider .The event that an attacker captures this server this system is likely to guarantee that the adversary will gain little or no information from the log files and to limit his ability to corrupt the log file. This system has implemented how to store secure log file in cloud and that file can be performed dynamic operation by the authorized users.***

Keywords: ***Elgamal Algorithm; Third-party Auditor (TPA); Log Generation; Log manager; Dynamic Operation.***

I. INTRODUCTION

This system provides a secure data sharing in an E-commerce website which is cloud based. It proposes a comprehensive solution for storing and maintaining log records in a server operating in a cloud-based environment, and 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. The proposed architecture develop a cryptographic algorithm to address integrity and confidentiality issues with storing, maintaining, and querying log records at the honest but curious cloud provider and in transit. Many security schemes like dynamic key generations and jar files are used to prevent unauthorized users from accessing the data shared in E-Commerce site.

II. RELATED WORK

A. Reliable Delivery and Filter 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.

B. 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 guide to implementing or using log management technologies.

C. Explorative Visualization of Log Data to support Forensic Analysis and Signature Development

In this paper, the system 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, the tool introduced, implements this approach and demonstrate the strengths and benefits of this presentation and exploration form.

D. 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, informal arguments that assert the security for a protocol are prone to errors.

E. 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 it discuss its requirements, then its computational model. which builds database functionality as an extensible collection of transparent extensions to existing programming languages. It describe how Open OODB's *system architecture* is decomposed into a kernel *meta-architecture* and a collection of modules implementing specific behavioral extensions. Finally, it discuss risks of the approach and report on the project's status.

F. Concurrency Control in Distributed Object-Oriented Database Systems

In this paper has 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.

III. IMPLEMENTATION

The sellers register and share their products in an e-commerce website in which the server is a cloud based environment. 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. 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.The security modeling provides secure data sharing from attackers,elgamal algorithm which has a better key length than RSA is used so as to generate dynamic keys for OTP.CAPTCHA scheme is used so as to avoid slowing the website usage.The images stored by the sellers cannot be downloaded since right click option is disabled.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. ARCHITECTURE

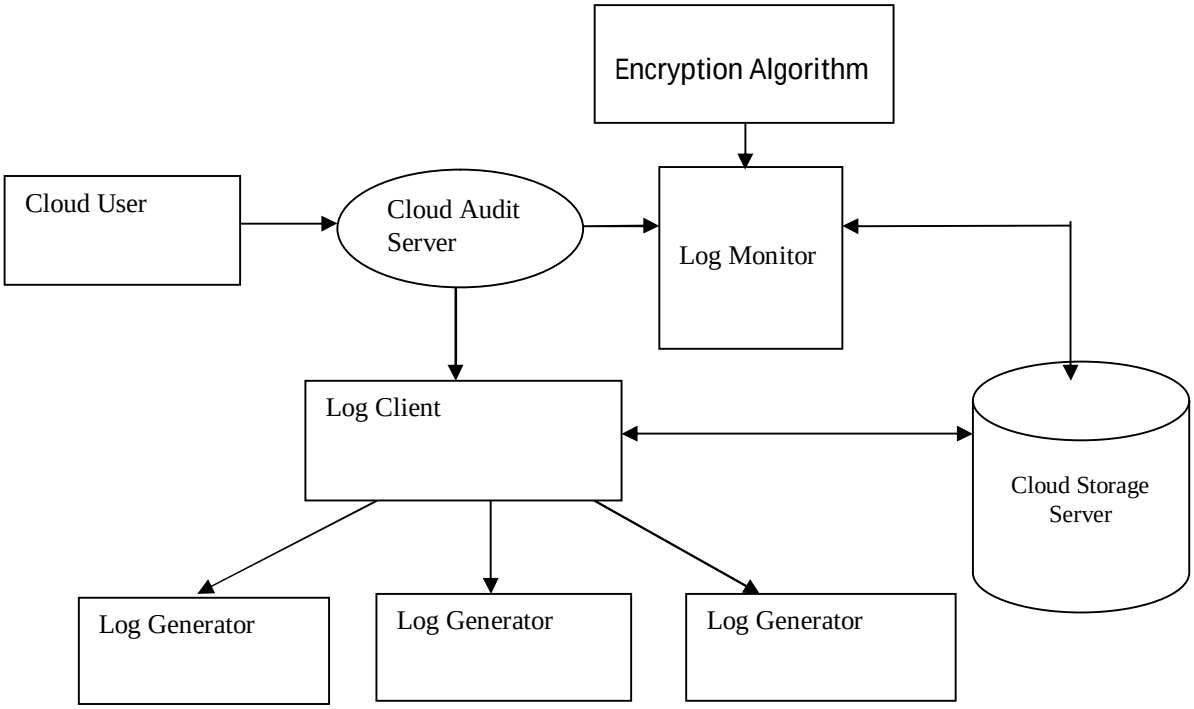


Fig. 1. Architecture of proposed system

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. MODULES

A. Cloud Users

The Cloud users are the one who totally depends on cloud providers which stores and maintains their data. Cloud users are the sellers in an E-commerce site they login and store their data in the cloud storage server.The cloud users can also be the buyers they can register and buy the products. The audit server generates 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 sellers or cloud users can perform dynamic operation for their products in the e-commerce site.

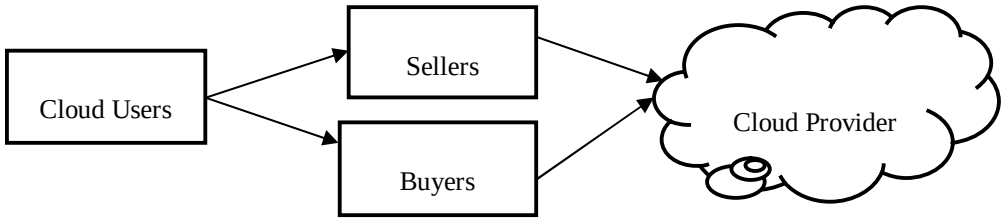


Fig. 2. Cloud Users.

B. Cloud Audit Server

The cloud audit server has the logging client which is a collector that receives groups of log records generated by one or more log generators, and prepares the data so that it can be pushed to the cloud for long term storage. The 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 data waiting to be transferred. The logging client incorporates security protection on batches of accumulated data and pushes each batch to the cloud. When the logging client pushes log data to the cloud it acts as a logging relay. The terms logging client and logging relay are used interchangeably. For simplicity however, assume that there is a single logging client.The Sellers when needed to upload data to share in the e-commerce site receives a dynamic key which are generated using the Elgamal algorithm and the sellers enters the key in the cloud provider the audit server decrypts and uploads the product.Still to prevent hackers to make any middle man attack the captcha scheme is used by the auditor.

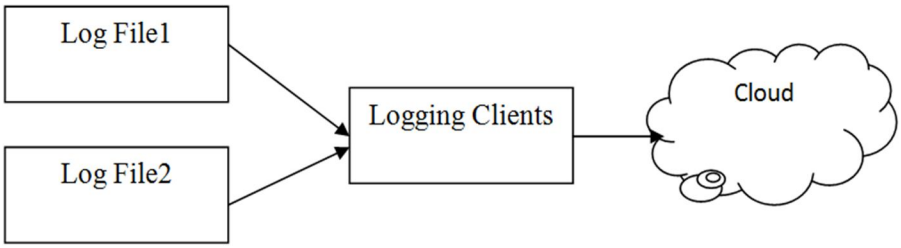


Fig. 3. Cloud Audit Server

C. Cloud Storage Server

The cloud storage server (CSS) provides long term storage and maintenance service to log data received from different logging clients belonging to different organizations. The CSS is maintained by a cloud service provider. Only those organizations that have subscribed to the 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.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

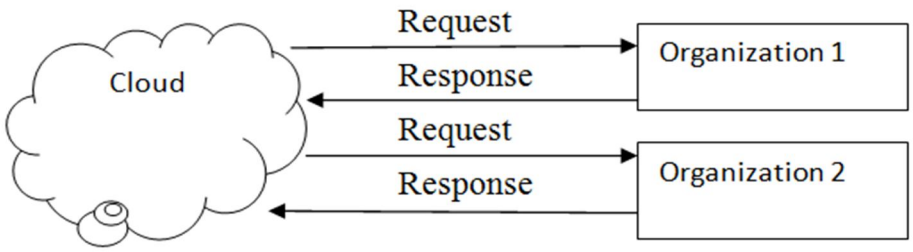


Fig. 4. Cloud Storage Server.

D. Security Model

This model provides the complete security in order to prevent the adversary attacks when data are shared by the sellers in E-commerce site. only registered users can upload their products unauthorized users are prevented in accessing the products by using one time password which are being generated using the Elgamal algorithm. Not all the users could download the pictures of the products, right click option is disabled for those who are not registered users, the buyers can be public or private users and download options are available only for private cloud users. The Log monitor manages the logging clients and converts the users login details and stores them as jar files in the audit server 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.

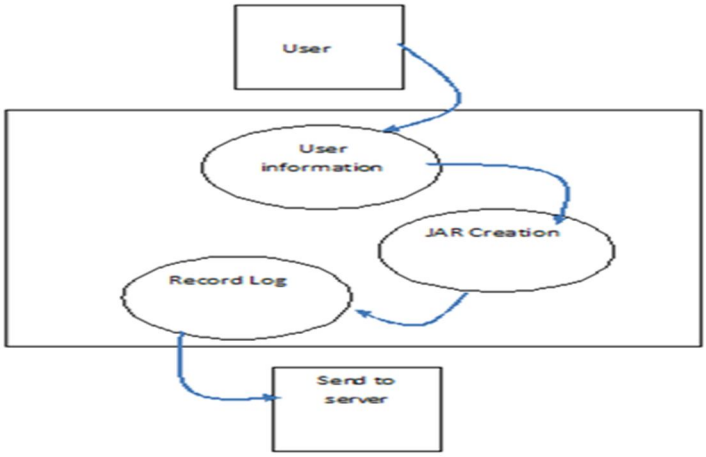


Fig. 5.Security Model

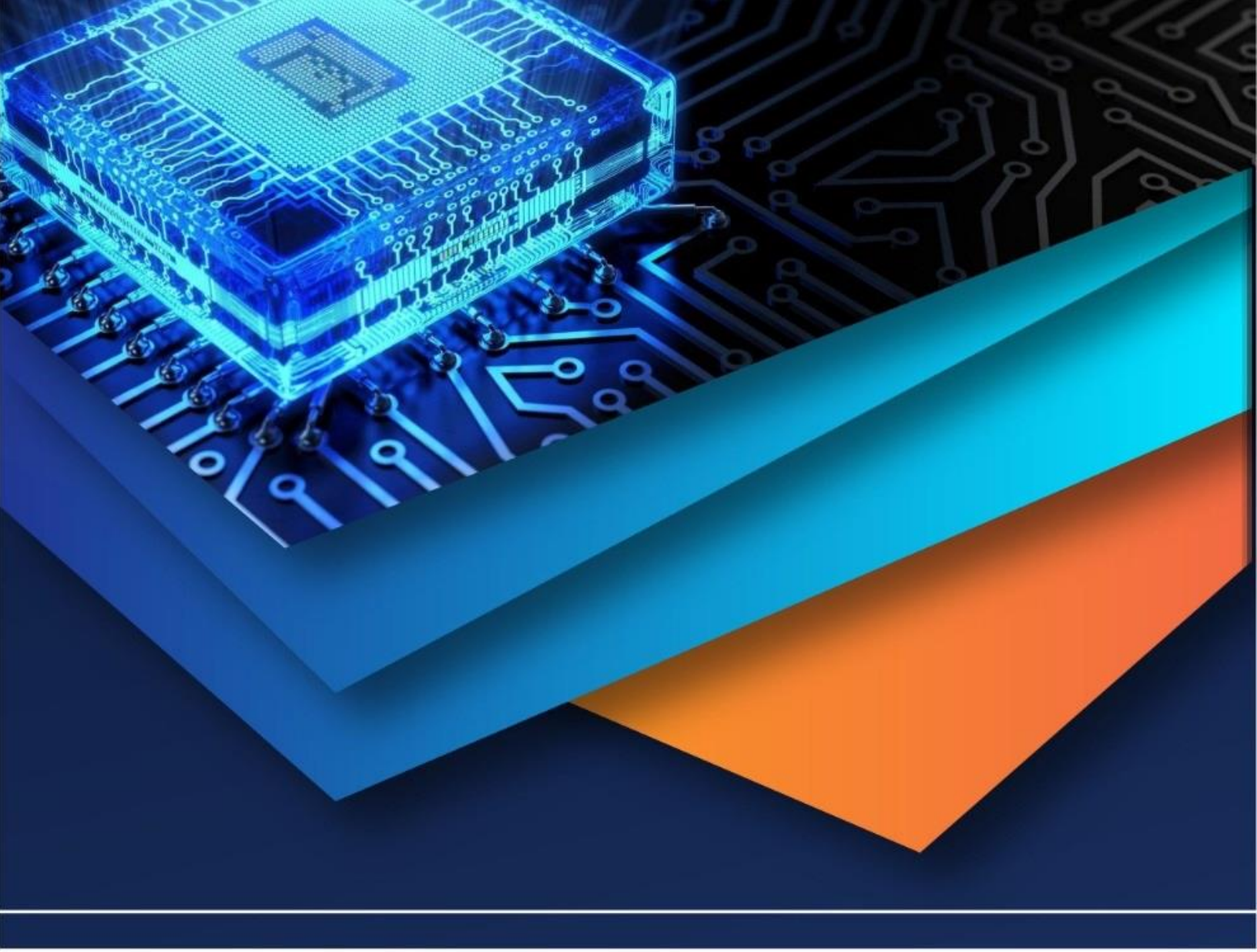
VI. CONCLUSION

This proposed system is a complete system to securely outsource log records to a cloud provider. The 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. This system helps to store secure log file in cloud and that file we can change read, write, delete, upload and download. This system has implemented Elgamal algorithm that uses for log monitor and log generator. The proposed system gives 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. It provides anonymous upload, retrieve and delete protocols on log records in the cloud using the two tier cloud network. The protocols are developed for

this purpose have potential for usage in many different areas including anonymous publish-subscribe.

REFERENCES

[1] KB. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS '13), pp. 90-99, 2013.
[2] D. Cash, A. Kupcu, and D. Wichs, "Dynamic Proofs of Retrievability via Oblivious RAM," Proc. 32nd Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 279-295, 2013.
[3] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
[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. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.
[8] K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY