ISSN:0975-9646

K.Kartheek et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 6942-6945

Secure Data Storage and Log Records Using JAR, AES

K.Kartheek[1](M.Tech), C.Narasimha[2](Ph.D)

[1]*PG Student,* [2]*Assistant Professor*
[1 2]*Department of Computer Science and Engineering,*
Madanapalle Institute of Technology and Science,JNTUA

***Abstract*— In cloud to maintain data in secured manner using java archive files (JAR) for data storage. Whenever user accesses the data no other will get the transactions those are occurring on JAR files. For JAR files providing security through manifest files for accessing permissions. Along with this to provide more security applying Advanced Encryption Standard for log record which contain events those are performed by the user. These log files plays a key role in any organization privacy, so need to get service from trusted third party cloud service provider. For data access control using authentication and efficient accountability in cloud storage one have to use Cloud Information Accountability framework. It provides distributed accountability for data sharing among users of cloud.**

***Keywords*— Data Storage, JAR files, Log Records, Advanced Encryption Standard, Cloud Computing.**

I. INTRODUCTION

Cloud is nothing but it is a storage space where we can store resources like software etc. through internet users can use these stored resources. Cloud storage will provide by the third party service provider, to keep data in secured manner must approach trusted service provider. The cloud may be public or private, in case of public clouds anybody can access the data from cloud, but in case of private clouds only the authorized persons can access cloud. The service providing also will takes place in three ways SAAS means Software As A Service, PAAS means Platform As A Service and IAAS means Infrastructure As A Service. Based on client requirement third party cloud service provider will provides any model among these. Advantages of using cloud computing are Scalability, Reliability and Efficiency.

Java archive files (JAR) files are using to store data in efficient secured manner. When user access the data from java archive file no other is able to see those transactions. Manifest files are plays a major role to provide data security in JAR files, because through attributes of manifest files can provide permissions for using JAR files data like reading, modifying etc.

JAR files maintain a broad collection of functionality, including electronic signing, control of version, package sealing, and others. Versatility for Java Archive file will get by manifest file, this manifest file contains metadata about files those are packaged in Java Archive files which is able the Java Archive File to use in many purposes.

Log records contain data about the users proceedings in network, when attacks made on network to investigate about those attacks these log files are useful because log files contains information like system IP address through which login id the attack was made etc. so log record contains very sensitive information, to protect these data we are using algorithm is Advanced Encryption Standard.

Advanced Encryption Standard accountability will provide security to the log records by generating one encrypted password which is can't able to trace by the attacker and also they can't modify the data which is present in log record. Advanced Standard Algorithm uses three types sizes of keys according to requirement, but the encryption and decryption processes are same in any type change will made in number of rounds for encryption and decryption.

Cloud Information Accountability is to maintain end to end accountability of data. Through this framework can provide distributed data sharing among the users. Cloud Information Accountability will controls the accessing of data through authentication.

II. LITERATURE REVIEW

A. Reliable Delivery and Filtering for Syslog Published: November 17, 2006

The consistent Delivery of data and Filtering for Syslog characteristic allows a mechanism to be adapted for delivery of syslog communication. This characteristic provides secure and reliable delivery by means of BEEP (Blocks Extensible Exchange Protocol) for syslog messages. BEEP is for connection-oriented application protocol, and asynchronous communications. It is proposed to grant the features that usually have been duplicated in different protocol implementations. Blocks Extensible Exchange Protocol allows the exchange of messages and typically runs on top of TCP.

By using SYSLOG future it is not sufficient for all organizations because of using BEEP protocol so in place of this future using advanced encryption standard algorithm to provide security, reliability to the data.

B. MurugiahSouppaya, Karen Kent Guide to Computer Security Log Management

Log management is useful to organizations in different ways. It is efficient way to find out the system functioning in particular period of time. By analyzing and reviewing log data more beneficial for policy violations, operational problems, security incidents, and fraudulent activity identification and for resolving problems.

Infrastructure of log management contains following three tiers:

-Log Generation
-Log analysis and storage
-Log Monitoring

All these are more useful in developing, implementing and maintaining effective log management practices architecture and to increase the performance of the system.

C. René Rietz, Michael Vogel,Sebastian Schmerl, andHartmutKönig Explorative Visualization of Log Data to support Forensic Analysis and Signature Development,Group of Computer Networks and Communication Systems

It is an approach to represent the log data, and audit data for simplifying the analyzing process for the security administrator. It is representing the relations of audit events and audit data in three dimensional manners. This approach will give more benefits to present data to organization very easy manner and time for retrieving also takes less. So it is more efficient to log data maintenance.

To represent the log data, and audit data in graphically in three dimensional spaces which support for forensic analysis and signature development.

D. ANDREW c. YAO,AND DANNY DOLEV
On the Security of Public Key Protocols

Public key encryption is to provide communication of network securely. These systems of public key are very effective.

In public key system, every user N has an encryption E function, and D decryption function,A secured public directory encompasses all the (N, E) pairs, while the decryption function D, is known only to user N.

E(M) the public directory does not reveal anything about the value M.

Thus everyone can send Na message E(M), N will be able to decode it by forming D,(E,(M)) = M, but nobody other than N will be able to find M even if E,(M) is available to them.

Instead of Public key using symmetric algorithm which is Advanced Encryption Key algorithm to provide the security to the data while data transactions and maintenance.

III. SECURED DATA AND LOG RECORDS

To provide security to the data which is stored in cloud using Java Archive files. In JAR file archiver including manifesto (mft) files. Through these manifesto files giving some attributes to give accessing permissions like read, write and modify etc. along with these providing meta information to know about the data which give clear idea about the data. And also generated log records by using log generators will store in java Archive files only which are can't access by the users only the third party cloud service provider can access them.

Log files will plays a key role in any organization privacy issues so to keep those log files in secured manner here we are using Advanced Encryption Standard algorithm which will store in encryption format even though the attacked try to modify the log files data it is not possible because along with username and password have to use this Advanced Standard Algorithm Encrypted key to access those log records.

Also using Cloud Information Accountability Framework to maintain end to end accountability of data in efficient manner. It provides distributed data sharing among the users.

The processing of encryption will takes place based on key size we are using it may be AES-128 or AES-192 or AES-256 bits. But the procedure is same in any bit size algorithm because of using iterations the change will made in number of iterations. In case of AES-128 uses 10 rounds, in AES-192 uses 12 rounds and in AES-256 uses 14 rounds. The procedure of encryption process is as shown in below

Functions to be perform while encryption

A. Primary Round

1) *Add round key*: all the bytes of state will combined with round key block by using XOR bitwise operation

B. Rounds

1) *Sub bytes*: here non linear substitution of every byte will takes place by means of lookup table.
2) Shift rows: it is an transposition in last three rows of state will shift cyclically.
3) *Mix columns*: this operation will operates on state columns by combining each coumn bytes.
4) *Add round key*

C. Last Round (no Mix columns)

1) *Sub bytes*
2) *Shift rows*
3) *Add round key*

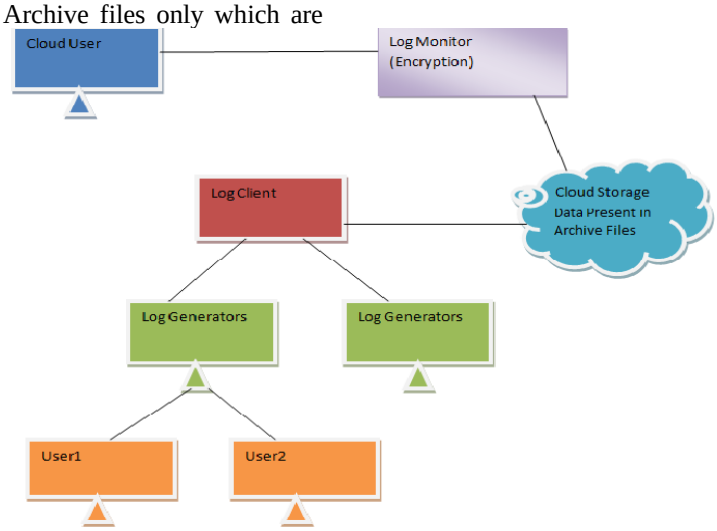

Fig. 1 Architecture for Proposed System

IV. SIMULATION RESULTS

By applying above specified mechanisms to the system obtained results are as shown in below graphs.

Here using overhead and number of messages to draw graph and showing three lines first line specifying the data without any security here overhead of system is very high. Second line specifies the data with partial security where the overhead is became low compared to data without security and the third line specifies that the overhead is very less because of using full security to the data.

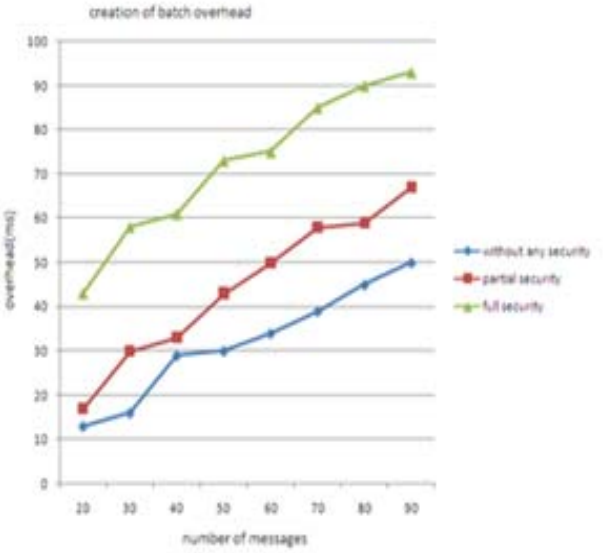

Fig. 2(a). Graph shows performance based on Security provided

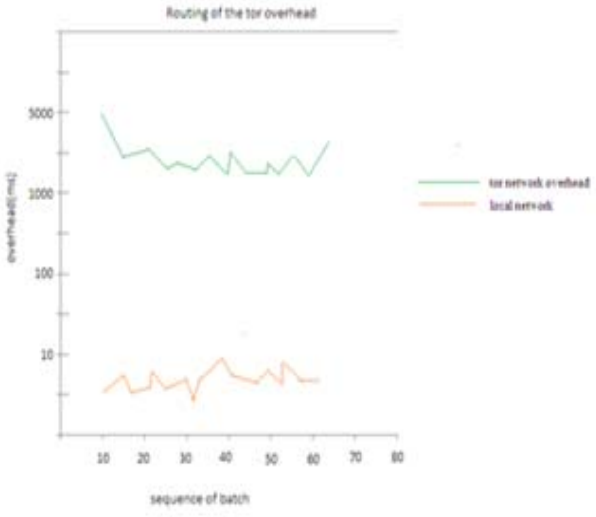

Fig. 2(b). Graph shows performance in TOR and Local networks

Where as in second graph between overhead and sequence of batch (number of files are combined into one batch). The overhead is high for the tor network like world wide web etc. but in case of local area network the overhead is low which means it is very efficient to use.

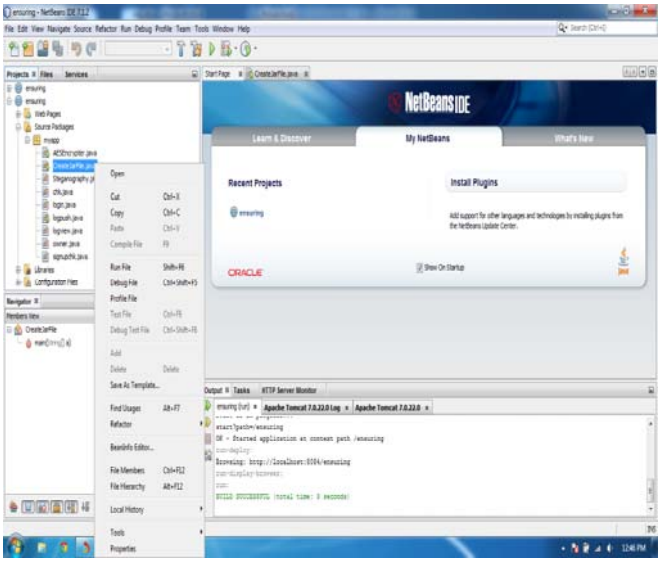

Fig. 3. Creation of JAR file to store data in Cloud

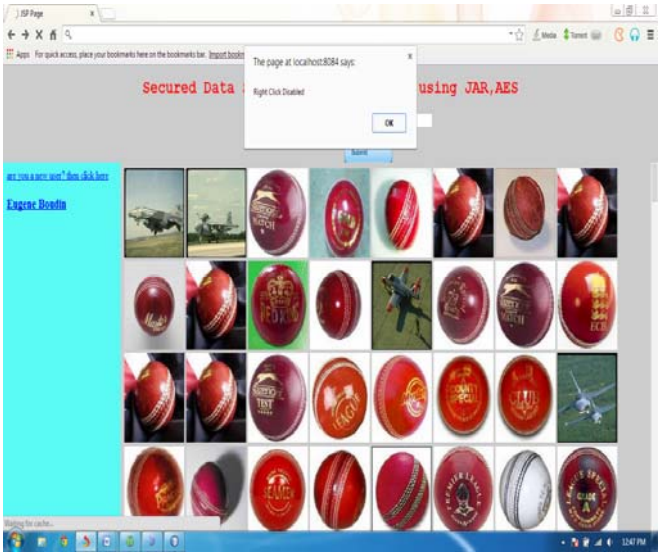

Fig. 4. Disabling Right click to avoid downloading of images directly with out authentication.

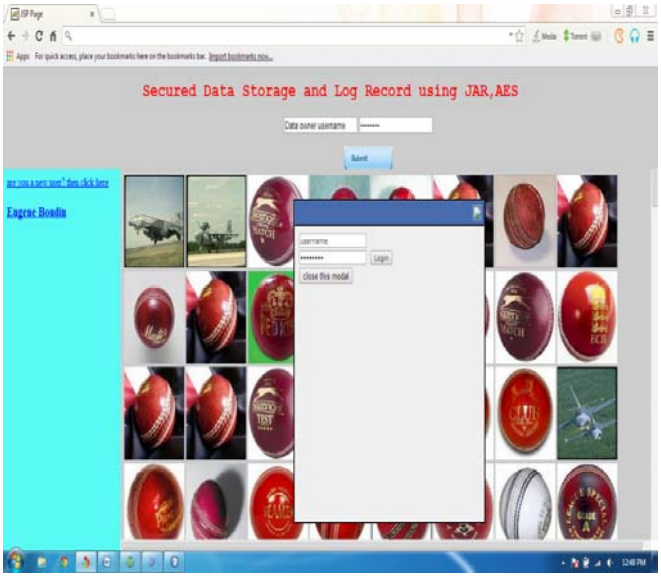

Fig. 5. Authorised login into the system to access data

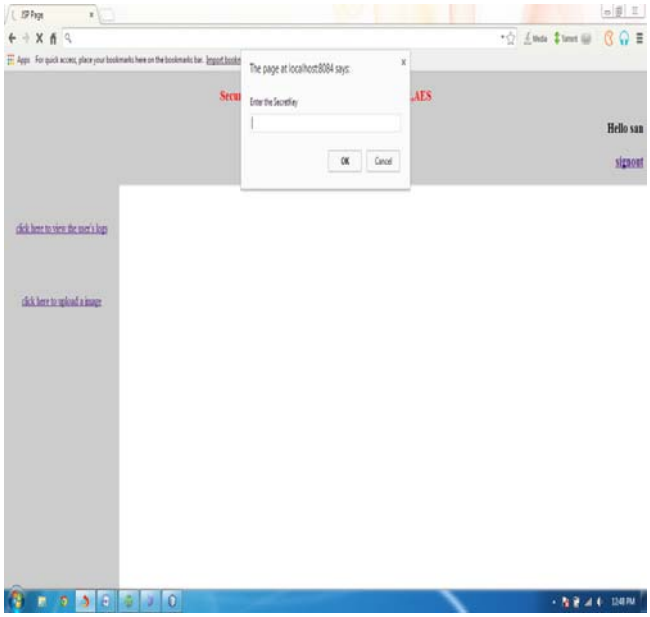

Fig. 6. Using AES secured key to access the Log data.

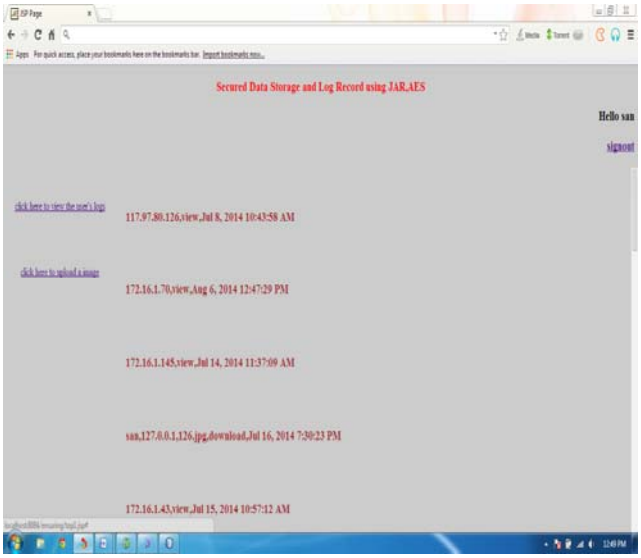

Fig. 7. Displayed Log Files to the Administrator.

CONCLUSION & FUTURE WORK

Maintaining of log files in cloud becomes burden to the cloud service provider because resource expensive will increase. Here using Archive files to store data in cloud, to secure data using authenticated login and also to provide security to the log records using Advanced Encryption Standard which tends to security to the data as well as log records. Here we tried to provide full security in all operations while sending, retrieving and storing. But need to outsource the log record maintenance for trusty third party cloud service provider only otherwise they may misuse the organization information.

In the future, possible to made changes in client logging in efficient manner, which will strongly incorporate with the operating system. In this present implementation can use log records by tag values. We can implement some more techniques which can execute queries on encrypted log records without effecting privacy.

.

REFERENCES

[1] Secure Logging As a Service—Delegating Log Management to the Cloud Indrajit Ray, Kirill Belyaev, MikhailStrizhov,Dieudonne Mulamba,and Mariappan Rajaram, VOL. 7, NO. 2, JUNE 2013

[2] Ensuring Distributed Accountability for Data Sharing in the Cloud Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and DanLin, VOL. 9, NO. 4, JULY/AUGUST 2012

[3] 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

[4] "Reliable Delivery and Filtering for Syslog" Published: November 17, 2006 Last Updated: November 14, 2008

[5] 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.

[6] 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.

[7] Sebastian Schmerl, Michael Vogel, René Rietz, and Hartmut König on "Explorative Visualization of Log Data to support Forensic Analysis and Signature Development", Computer Networks and Communication Systems Group, Brandenburg University of Technology, Cottbus, Germany