IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Efficient and Secure Cloud Log Secrecy Scheme for Cloud Forensics

Vijeth M[1*], Vikas H R[2],Vishwas B S[3],Vishwas N[4], Prasanna Kumar M [5]

[1,2,3,4,5]Department of Computer Science, East West Institute of Technology, Bengaluru, India

DOI: https://doi.org/10.26438/ijcse/v7si15.183186 | Available online at: www.ijcseonline.org

***Abstract*—**Client action logs can be a profitable wellspring of data in cloud legal examinations .thus, guaranteeing the unwavering quality and security of such logs is significant. Most existing proposition for secure logging is intended for conventional environment as opposed to the perplexing condition of the cloud. The log documents present in the log records ought to be protected from aggressors and outsider associations. Log Files contains private data about the association's action. So as to conquer the assaults from outside elements, In this paper, we propose the Efficient and secure log secrecy schemefor cloud forensics process as an elective plan for the verifying of logs in a cloud domain. In Efficient and secure log secrecy scheme for cloud forensics, logs are encrypted utilizing the individual client's public key with the goal that just the client can decrypt the substance. So as to avert unapproved change of the log, we produce proof of past log (PPL) using cryptography techniques.

***Keywords*—**Logs,Cloud,cryptography.

I. INTRODUCTION

Cloud storage, security, and privacy are fairly established research areas[1-7]. The cloud would keep track of the users for security purpose and enhanced performance. Unlike earlier server-client models, where all the data and information of business systems were within the enterprise boundaries, in case of cloud (especially public cloud), data can be saved at any remote location in the world. The major difference lies in where data resides and the optimization of resources. The user activities are stored in the cloud as logs. A log is an official record of activities happening within a system or network. Logging is important because Log Data can be used to track user activities within an organization. Log records play a vital role in generating forensic analysis report if there is any kind of security breach in an organization. Hence, Log management within an organization should be given a higher preference. Logs are very important for service providers, as they help them calculate service charges for customers. Logs also help in tracing inappropriate activities such as hacking. However, a smart hacker could tamper with the log itself, leaving no trace of his activity. The Logs can also be manipulated by cloud service providers. Hence, logs should be saved in a way that they cannot be hacked or read by anyone else but the user. The main objective of this paper is to provide a secure framework for log maintenance such that only the user can view his activities, hence preventing tampering of logs by hackers, cloud service providers

In the existing system, the logs are encrypted using the investigating agency's public key and stores the encrypted logs in a cloud server. This ensures privacy and confidentiality of the cloud user unless the particular user is subject to an investigation (e.g. via a court order). To facilitate log integrity, Existing system generates proof of past log (PPL) with the log chain and publishes it publicly after each predefined epoch. However, it is difficult to ensure or verify that the CSP is writing the correct information to the log, or that any information pertinent to the investigation is not omitted or modified. Specifically, the existing system does not provide the user with the ability to verify the accuracy of the log (since the log is encrypted with the agency's public key). Also, the files can be accessed without the owner's permission.

In order to overcome this security issue, the proposed system will encrypt the users' log activities using an encryption algorithm. The encrypted log file would be stored in the cloud, hence preventing tampering of cloud logs. The log files are encrypted using the user's private key. The encrypted file logs can only be viewed by the user with the corresponding key.

II. RELATED WORK

Dependable cloud logs assume a critical job in forensic investigation. Log securing, looking after privacy, uprightness and forward mystery, legitimacy check and openness by specialists (or another approved gathering), are a portion of the various measurements a forensic investigator and researcher should focus on.

Digital forensics for eucalyptus

F. Anwar and Z. Anwar [8] endeavoured to address a portion of these difficulties by recognizing the likelihood of Syslog or snort log to aid the discovery of cloud assaults. The authors directed that cloud forensic investigation is dependent on the logs produced by Eucalyptus, an open-source distributed computing programming. In particular, they produced their own dataset by reproducing a DDoS assault on Eucalyptus and distinguished the assaulting

machine IP address by investigating the log. Security, get to control, and confirmation of log were not considered.

Loggingsystem for cloud computing forensic environments
Patrascu and Patriciu [9] proposed a forensic module to be kept up as a major aspect of the cloud's controller module, which is intended to speak with an alternate heap of cloud resources (for example virtual file system, virtual memory, network stack, and system call interface) so as to gather and store logs. Likewise, the security of the gathered log (either in transmission or away) was not considered.

Forward integrity for secure audit logs
Bellare and Lee presented the idea of forward integrity [10] or forward secrecy as a system property to moderate an attacker's capacity to debase a logging system without discovery. Breaches incorporate addition of false logs, change or erasure of existing logs, and reordering of logs. Forward integrity is built up utilizing a cryptographically strong one-way hash function (for example HMAC) and a secret key that is generated using pseudo-random function(PRF). In other words, each successive log entry has an associated hash key that is dependent upon the previous entry.

Secure audit logs to support computer forensics
Schneier and Kelsey proposed a log the board scheme[11] dependent on forward integrity and gave a few real-world applications. Dissimilar to Bellare and Lee, the forward integrity property in the methodology of Schneier and Kelsey is guaranteed utilizing a secret key which is the underlying purpose of one-way hash chain and message authentication code.

Towards building forensics enabled cloud through secure logging-as-a-service Zawoad proposed a novel plan "SecLaaS" [12], that has taken into consideration by lot of CSPs, for example, unpredictability, breaching of cloud information, and potential malicious loggers(CSP itself). They have given a total arrangement of secure logging for all cloud exercises of VMs (or its customers)

We evaluate SecLaaS, identifying a number of weaknesses. We propose an alternative approach that incrementally builds upon SecLaaS in an attempt to respond to these identified weaknesses.

III. METHODOLOGY

Our proposed Systemwill make sure that the manipulation of the user logs do not happen,it would consist of following components

A) Preservation of Log &Its Proof: Parser collects the log from log source. When a log file changes (i.e. new lines append) it triggers the parser to check the change and to start processing a new log.Retrieving log from log source, the parser parses the log and gets the necessary information. Our goal is to keep log content secure given a parser that will provide the system a log message in string format, regardless of content. The format of the log is out of the scope of this work.

B)Accumulator Design**:** Cryptographic accumulators are space/time efficient data structures that are used to test if a value/element belong to a given set. They are the cryptographic counterpart of a data structure very popular in the field of networking: thecryptographic accumulators generate a fixed-size digest representing an arbitrarily large set of values. Interestingly, a one-way accumulator further provides a fixed-size witness for any value of the set, which can be used together with the accumulated digest to verify membership of value in the set.

C) Verification: Only a verification process thatestablishes authenticity will be able to determine the presence of log contamination. There are two types of verifications in our approach. First is verification where the user checks if the CSP is writing correct logentries or not. Second is verification by any party: user, investigator, law enforcement authority (LEA) or court of law to verify PPL to check for log modification. In both cases, the CSP can provide a small utility verification software or the user/investigator can buy it from individual software vendor (ISV) to verify.

D) Secret Key Sharing: We propose, in Efficient and Secure cloud log secrecy scheme for cloud forensics, to encrypt the log with the user's private key. In this case, we make use of AES which is a symmetric encryption technique and RSA-KEM for sharing of the key.

of 16 new bytes. It should be noted that this step is not performed in the last round.

IV. SYSTEM ARCHITECTURE

An untrustworthy cloud client can assault a system outside the cloud. They can likewise assault any application deployed in the same cloud. In, Efficient and Secure Cloud Log Secrecy Scheme for Cloud Forensics the proof of past log is published in a public domain which preserves the integrity of the logs.

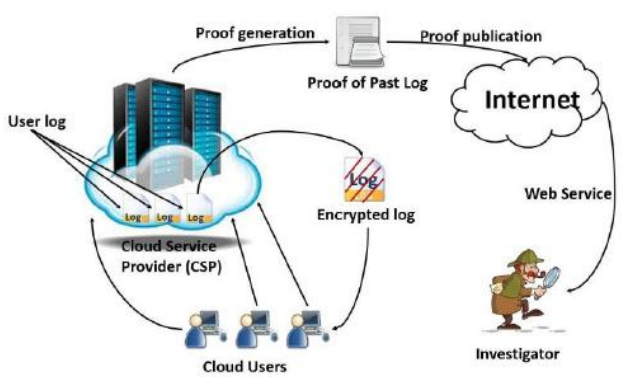

Figure 1: An Overview Architecture of Efficient and Secure cloud log Secrecy scheme for cloud forensics

The system architecture for the proposed system is as shown in Figure 1. The cloud users activities or logs will be monitored and stored in the cloud service provider(CSP) server in the encrypted format using the user's encryption key. Also, the proof of past log would be published over a public domain. During any kind of security breach, the forensic investigator will be responsible for the investigation.

V. ALGORITHM

AES(Advanced Encryption Standard):
AES is a Symmetric Encryption technique.AES is an iterative cipher. It is based on 'substitution-permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs(substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. It is as shown in figure-1

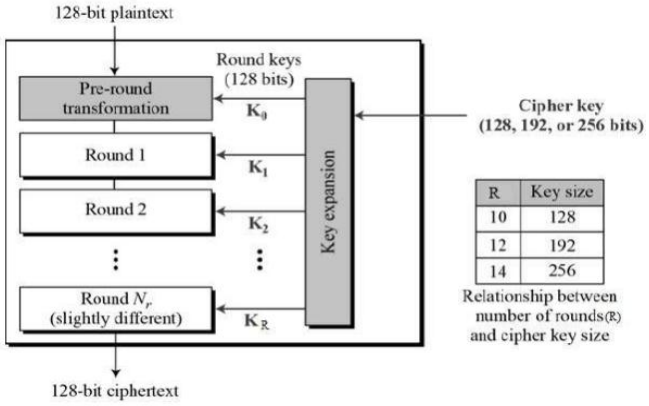

Figure-1

The encryption process in AES would consist of the following steps

Byte Substitution (SubBytes): The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.
Shiftrows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of the row. The shift is carried out as follows −

- The first row is not shifted.
- The second row is shifted one (byte) position to the left.
- The third row is shifted two positions to the left.
- The fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

RSA-KEM: Key encapsulation mechanisms are a class of encryption techniques designed to secure symmetric cryptographic key material for transmission using asymmetric algorithms.In practice, public key systems are clumsy to use in transmitting long messages. Instead, they are often used to exchange symmetric keys, which are relatively short. The symmetric key is then used to encrypt the longer message. RSA-KEM involves following steps

- Generate a random AES key using the Key Derivation Function(KDF).
- Encrypt the message(M) and AES key(Kaes) using AES encryption as shown below
  C1= Eaes(M,Kaes)
- Encrypt Kaes and Kpu using RSA as shown below
  C2= Ersa(Kaes,Kpu)
- The recipient would use decryption key Kpr to recovermessage(M) as shown below
  Kaes= Drsa(C2,Kpr),M= Daes(C1,Kaes)

VI. RESULTS AND DISCUSSION

The proposed system would make use of the AES (Asymmetric Encryption Standard) cryptography encryption technique in order to encrypt the logs of the user. The logs are encrypted by

making use of a user's secret key.By, doing this the tampering of the cloud logs by the Cloud Service Providers(CSP) can be avoided.

We obtain an encrypted file as a result of the operation which can only be decrypted using the secrete key. The logs as well as the files uploaded by the data owner are in the encrypted format.

VII. CONCLUSION AND FUTURE SCOPE

Conclusion:

In this paper, we propose a safe logging plan for distributed computing with highlights that encourage the conservation of client protection and that alleviate the harming impacts of intrigue among different gatherings. Efficient and Secure Cloud Log secrecy scheme for cloud forensics preserves the privacy of cloud usersby encrypting cloud logswith a public key of therespective user while also facilitating log retrieval in the event of an investigation. Moreover, it ensures the accountability of the cloud server by allowing the user to identify any log modification. This has the additional effect of preventing auser fromrepudiating entries in his own log once the log has had its PPL established.

Future Scope:

Normally logs are low-level data and hard for the common user to understand what exactly those logs signify. Thus, we will explore leveraging big data techniques to facilitate user retrieval and visualization of information from log data. Standardization of log format is also an associated research area. To ease searching, we kept some crucial and sensitive information in plaintext format. This makes them vulnerable . Thus, designing secure and efficiently searchable encryption would extend this work.There is also the need for an online credibility system designed to develop trust and credibility of a cloud user so that the CSP can enable stricter auditing policies for low-trust users in comparison to high-trust users. Designing and implementing a prototype of the proposed scheme in collaboration with a real-world CSP, with the aim of evaluating its utility(e.g. performance and scalability) in a real-world environment.

ACKNOWLEDGEMENT

Firstly, we express our sincere thanks to our guide Mr. Prasanna Kumar M, Assoc. Professor, Department of CSE, EWIT and Dr. Arun Biradar, Head of Department of computer science and engineering for their moral support. We express our sincere gratitude to our principal Dr. K Chennakeshavalu forhis constant support and encouragement, we also thank all the faculties of East West Institute of Technology for their co-operation and support.

REFERENCES

[1] X. Liu, R. H. Deng, K.-K. R. Choo, and J. Weng, "An efficient privacy-preserving outsourced calculation toolkit with multiple keys," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2401-2414,2016.

[2] Y. Mansouri, A. N. Toosi, and R. Buyya, "Data storage management in cloud environments: Taxonomy, survey, and future directions," ACM Computing Surveys(CSUR), vol. 50, p. 91, 2017.

[3] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes,"Future Generation Computer Systems, vol. 78, pp. 1040-1051,2018.

[4] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE TransactionsonCloudComputing,pp.276-286, 2018.

[5] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers&Security,vol.69,pp.84-96,2017.

[6] Q. Alam, S. U. Malik, A. Akhunzada, K.-K. R. Choo, S. Tabbasum, and M. Alam, "A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification,"IEEETransactionsonInformation Forensics and Security, vol. 12, pp. 1259-1268, 2017.

[7] L.Li,R.Lu,K.-K.R.Choo,A.Datta,andJ.Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 1847-1861, 2016.

[8] F.Anwar and Z.Anwar "Digital forensics for eucalyptus," in Frontiers of Information Technology (FIT), 2011, 2011, pp.110-116.

[9] A. Patrascu and V.-V. Patriciu, "Loggingsystem for cloud computing forensic environments," Journal of Control Engineering and Applied Informatics, vol. 16, pp. 80-88,2014.

[10] M. Bellare and B. Yee, "Forward integrity for secure audit logs," Technical report, Computer Science and Engineering Department, University of California at SanDiego1997.

[11] B. Schneier and J. Kelsey, "Secure audit logs to support computer forensics," ACM Transactions on Information and System Security (TISSEC), vol. 2, pp. 159-176,1999.

[12] S. Zawoad, A. K. Dutta, and R. Hasan, "Towards building forensics enabled cloud through secure logging-as-a-service," IEEE Transactions on Dependable and Secure Computing, vol. 13, pp. 148-162,2016.

Authors Profile

Mr. Vijeth M is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Cloud Computing, Big Data and cryptography .

Mr. Vikas H R is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Cloud computing and Big Data.

Mr. Vishwas B S is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Cloud Computing, Big Data and cryptography .

Mr. Vishwas N is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Cloud Computing, Big Data .

Mr. Prasanna Kumar M, Associate professor, Department of CSE, East West Institute of Technology. His areas of interest includes Cloud Computing and Software Engineering.

