International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Secure Log scheme for cloud forensics

Shweta N.Joshi Mrs.Geetha R.Chillarge

Dept.of Computer Engg MMCOE, Pune

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Cloud computing provide new way of computing which is different from traditional computing. Traditional computing lacks in providing confidentiality, integrity and privacy about user data.In such environment cloud forensics is difficult as it has to face few challenges such no physical access to cloud logs due to distributed nature, reduced level of control over cloud, absence of standard log format, multi tenancy and decentralization. Cloud log contains valuable information which helps in forensics investigation. Previously designed logging systems have some security breaches and are unable to provide secure logging environment. This Secure logging scheme is provided by encrypting cloud logs using advance encryption method and it detects DDoS (distributed denial of service) attack on cloud infrastructure. It is detected by analyzing available cloud logs in the cloud server. Searchable encryption (SE) algorithm will be used to increase the security of logging mechanism and to maintain confidentiality and privacy of user data.

Keywords: *Cloud forensics; Distributed denial of service; Searchable encryption.*

Introduction

National Institute of Standard Technology (NIST)defined cloud computing as "Cloud computing can be defined as a model in favor of about enable ubiquitous, useful, on-request network accessibility toward a shared pool about configures computing assets it can be quickly provided as well as launched about minimum managing efforts or else service carrier interaction.". It is pay per use service & low cost method. Hence small and high level companies are attracted towards cloud computing. Client need not have to set up any kind of local infrastructure setup. Cloud infrastructures often suffer from security issues especially with remark to computer forensics. There are certain drawbacks which allows malicious individual to scan easily and exploit the power of cloud computing. An attacker can make the malicious activity on applications running within the cloud. These issues are the primary concerns of Cloud Forensics. Due to the essential nature about cloud technologies, conventional digital forensic procedures as well as tools need to be updated to hold the same usefulness and appropriateness in a cloud environment. Log files are the initial data source for monitoring of network. A log file is a system-generated data file it maintain information about usage patterns, activities, as well as operations within an operating system, application, server or any another device.

Types of log file:

Application log

- Logs that are recorded by an application.
- Situation of an application running on the server. e.g.:- web application.

System log

Contain information regarding data and time of the logcreation; type of message, such as debug, error.

Security log

- Logs contain security related information to determine malicious behaviour found in the system or network. For instance, malware detection, file quarantines, time of malicious detection, and various others.
- Managed by security administrator e.g.:- unsuccessful logins, rejected IP addresses

Setup log

Setup logs capture the events occur during performing the installation of an application.

Network log

It contains detailed information related to different activities which is occurred on the network. e.g.:- network traffic, packet drops, and bandwidth delays.

Web-server log

Records all events occur on the web-server such as access time, IP address, date & time, request method.

Audit log

- Unauthorized access to the system or network.
- Analyzing malicious activities at the time of the attack.
- It contains information about source as well as destination addresses, user login information, and timestamps etc.

Cloud virtual machines (VMs) could be located remotely; it is not physically accessible and can be distributed over multiple physical devices. Hence seizing the machine about forensic analysis it is not possible in most of the investigations. Data residing within a VM may be volatile and could be lost once the power is off or the VM terminates. The server (CSP) plays an important role in the collection of evidential data. Normally CSP writes the activity log (cloud log) for each user. The log contains valuable sensitive information which should not be damage with by CSP, other user or investigator. Thus, preventing modifications of the logs, maintaining a proper chain of custody and ensuring data privacy is crucial [1]. In most existing mechanism, sensitive information in these logs is kept plain text which is vulnerable to attack and tempering. It is proposed to solve this problem by encrypting total log using advanced encryption like a searchable encryption. Searchable encryption defined as cryptographic technique it provide search about particular information in an encrypted form. DDoS attack is detected to validate security of logging mechanism. DDoS Attack is perpetrated by one or more compromised systems controlled by an attacker to flood predeter- mined target using series of malformed or malicious packets that flood the allocated resources. The result of this is not able to access of cloud services. Limitation of the system is processing time required to search the log entry is more as tags are associated with log entry to ease search. Each log entry is having one separate tag.

Literature Survey

Anwar et al. [2] proposed the solution for cloud forensics by providing secure logging with operating system and the security logs. Cloud computing environment of Eucalyptus was set up using Snort, Syslog, and Log Analyzer. They examined characteristic of Eucalyptus and preserved all the logs of Eucalyptus objects. They launched a DDoS attack from two virtual machines and from the logs on the Cloud Controller (CC) machine; they identified the attacking machine IP, browser type and content requested. Security, access control and verification of log were not considered in this work.

Kranti Mehato and Moriwal [4] proposed a scheme for secure data accessing with maintaining its privacy by using strong cryptographic algorithm. To keep track the actual data contents in terms of document features hash table management and indexing techniques are used. These may help for encrypting user data and identifying the user data and privacy. They listed number of methods of searchable encryption to secure the data in cloud storage.

Zawoad et al. [3] proposed a secure logging service called “SecLaaS” that is designed to collect data from one or more log sources, parse the data and then store the parsed data in persistent storage to minimize the risk associated with data volatility. Before storing of data, it encrypts the log and generates a log chain to maintain confidentiality and integrity respectively. SecLaaS encrypts the logs using the investigating agency’s public key and stores the encrypted logs in a cloud server to ensure privacy and confidentiality of the cloud user unless user is subject to an investigation via a court order.

SecLaaS generates proof of past log (PPL) with the log chain and publishes it publicly after each predefined epoch to facilitate log integrity. It stores the PPL in other clouds to minimize the risk of a malicious cloud entity altering the log. In SecLaaS, it is difficult to verify that the CSP is writing the correct information to the log, or that any information required to investigation is not omitted or modified. It does not provide the user the ability to verify the accuracy of the log.

In the work of Lokhande and Mane [5] bloom filter based R-tree is used to accumulate and publish proof of past logs. Logs integrity is protected by hash chain scheme and proofs of past logs are published by the cloud provider. The confidentiality and integrity of the extracted logs is preserved so that logs become proved to be authenticated proof in investigation.Server can add, modify, change and delete Activity logs.

Ray et al. [6] presented a framework, where cloud server gets series of logs through authenticated channel from a logger or log accumulator. Then, the cloud server tries to maintain confidentiality, integrity, availability and verifiability of secure logs. They encrypt log entries with a chain of sequentially generated keys to protect logs from privacy violation and to preserve integrity they use another set of keys generated in the same way. To protect confidentiality and privacy they use symmetric key encryption so there is no option for public verifiability.

Sofia and Gandhi [7] create a framework for Cloud resilience system, which have the ability to provide the service for the clients even when the system is flooded with multiple requests. When the incoming request exceeds the limit then the server will not be able to process the request and may crash. In order to prevent the server from crashing, a Stealthy DDoS Detection Mechanism has been introduced. In this mechanism, the server monitors the number of incoming request given by each individual user. The server is initially given a limited amount of capacity to process the request of a single IP address. When the server load increases it checks all the request given by each user, if the request given by an individual user exceeds the servers limit then all the request from that particular IP address is blocked and all the services which are provided to that IP address is also denied.

Schneier and Kelsey [8] proposed a log management scheme based on forward integrity. The forward integrity property in the approach is ensured using a secret key which is the initial point of a one-way hash chain and message authentication code rather than PRF. Due to keeping a small and secret piece of information with each log entry, log entry can be verified later on for its integrity. Such schemes require the presence of an online trusted server to maintain the secret key and to verify its integrity.

Proposed Architecture For Secure Log Scheme

The main aim to create a framework for distributed Cloud system, which has the ability to detect DDOS attack, is to validate designed logging system whether it is secure and reliable and proves to be helpful in cloud forensics. This is done by flooding system with multiple requests. When the incoming request exceeds the limit then the server will not be able to process the request and may crash or not able to provide service to legitimate user. In the proposed mechanism, the user generates activity logs, analyzing available cloud logs that will help to detect DDoS attack on cloud infrastructure. To implement http based DDoS attack, java code will be used to start multiple tabs sending streams of randomized http requests to Cloud server. Multiple Http requests flooded onto the server in such a way that it cannot serve to the legitimate user request.

Cloud Deployment Details

- Server like miles web or layershift is used to deploy the code. Project .war file and database SQL file is uploaded.
- Project link and database link is provided by server to user.
- Program input is given by providing activity log generation and by generating DDOS attack and output is detection of attack in the form of attackers IP addresses.

A. Architecture for secure log scheme

In proposed framework activity logs of user are generated & fully encrypted using standard encryption/AES (Advanced Encryption Standard) and saved in SQL database. As part of project database will be generated and log format will be set. The logs corresponding to particular user are saved based on their IP address.Server publishes it on internet to preserve for future investigation.

When any malicious activity is to be detected like DDoS attack, corresponding logs are encrypted and saved with time stamp of particular user. The investigator compares these logs with the logs in database which were already published by Server. If logs are matched then IP address corresponding to logs are fetched and decrypted. Hence the IP address of malicious users is identified. Thus this system helps in cloud forensics procedure.

The graphical user interface of system contains following

I. User Login:

In user login, user is registered who want service from cloud. User is registered on cloud by providing details like Email, name, mobile no, address and password. User select the cloud server plan which service want to use.

II.Proof Generation

In proof generation activity logs are generated & stored on cloud.

III. Encrypted Logs

All logs are stored in enceypted format using AES algorithm.

IV.SERVER:

Server has given authority either accept or reject a user request. If Server rejects the user he has not eligible to get the particular service from Server. The user becomes authorized once his request has been accepted.Server published log data to internet to preserve the activity logs of particular user which are become useful for to detect DDoS attack.

V. Cloud:

Once the user is authenticated by Server, and then only he is able to use computer resources provided by Server and can login as valid user in cloud. If Server rejects user's request, cloud resources are not accessible to that user.

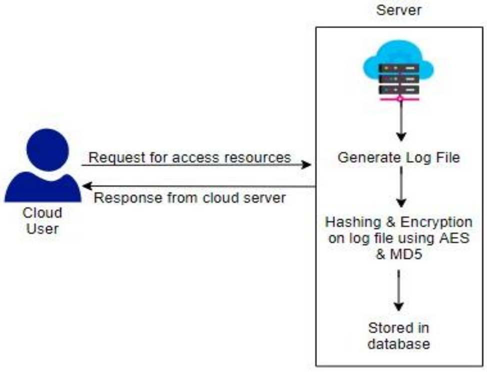

Cloud Server
Cloud User
Request for access resources
Response from cloud server
Generate Log File
Hashing & Encryption on log file using AES & MD5
Stored in database

Fig. 1 Proposed System architecture for secure log scheme

VI.Proof Publication

Server encrypts these logs and published it on internet to preserve for future investigation.

VII.Proof Of Past Log

In cloud, analyzing the data, only retrieve current content not previous one but through proof of past logs retrieve previous contents.

A. Algorithm

- Through Searchable encryption it is easy to search data in encrypted state. In this Scheme for searchable encryption that uses data-retrieval tags to determine whether data correspond to search item is match orl not. These tags are generated from the random number that is used when respective cipher text is created [9].
- In proposed work when activity logs are fully encrypted using AES, a tag for search purposes is created by using MD5 (Message Digest 5) algorithm and is attached to their respective cipher texts. MD5 and AES based hybrid cryptographic algorithm is used for providing the security.

Detection of ddos attack

Step1:
User Login into system, using login id and password. Login id of user is its valid email address using which User is registered.

Step 2:
User performs some activities like addition, deletion or sharing of files and corresponding activity logs are generated.
These logs are stored in database in following format. Log entry (LE) contains following fields originating IP (FromIP), time of log (TL), User ID and Activity of user (Act). LE= < FromIP, TL, Act, User ID >

Step 3:
Logs are stored in encrypted form and generate the message
digest of IP address ie TAG. (In main table) LE= TAG < FromIP, TL, Act, User ID >

Step 4:

Http based DDoS attack is executed by running a java code to start multiple tabs to send stream of randomized http requests from multiple users to server to exhaust its communication channel or bandwidth resources. Server's bandwidth is exhausted and it is not able to provide legitimate request or provide poor performance.
Step 5:
All DDoS logs are recorded and stored in encrypted form using encryption method and generate message digest of IP address (In DDoS table).
Step 6:
At investigator site, investigator investigates DDoSattacker by comparing encrypted IP with users stored IP using its message digest tag.

Mathematical Model:

Let S be the Whole system which consists: S= {IP, Pro, OP}

Where,

- IP: - It is the input of the system.
- Pro: - It is the procedure applied to the system to process the given input.
- OP:-It is the output of the system.

Input: IP = {AUTH, REQ, Act} Where,

- AUTH: - It is the authetication of user for send request to server for access resources.
- REQ:-It is requesting from user to server for access some resources.
- Act:-It is activity perform by user like share, delete, and update data on cloud.

 Process PRO= Logger () Where,

Logger () = {Log generation LG,
Log File Encryption LE,
Log File Stored in database LS}

- LG= {IP, Time of log, UserID, Activity of user}
- LE= {E1, E2}

Where,

- E1= $E1_{AES}$ {IP, Time of log, UserID, Activity of user}
- E2=$E2_{MD5}$ {IP}

Output: OP= Secured Log File

Contributions:

The contribution of this paper as follows:

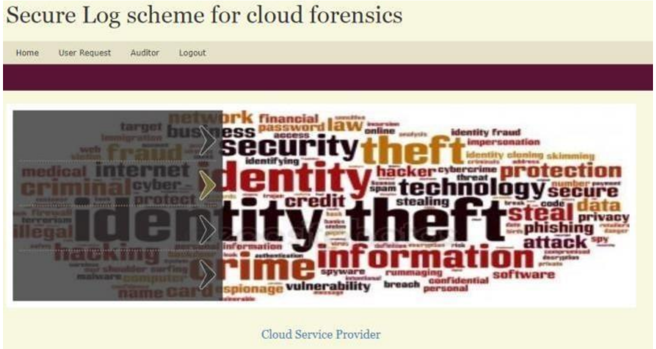
- The system proposes a scheme to cloud user log for preventing unauthorized access on log file using AES.

Result

This system propose most secure logging techniques using advanced encryption methods and validate framework to prevent DDoS attack in cloud computing for cloud forensics. In this secure architecture, activity logs of user are taken as input. By applying MD5 algorithm, hash value for IP address of user is calculated. Logs are encrypted using AES algorithm and saved in database.Server publish the logs on internet so that they are accessible to investigator if court of law ordered. If malicious activity like DDoS attack is happened, investigator compares tags associated with DDoS logs and database logs. If hash value of tags matches with each other, IP address in encrypted form is considered to be same. IP address is extracted and attacker is identified.

System Requirements

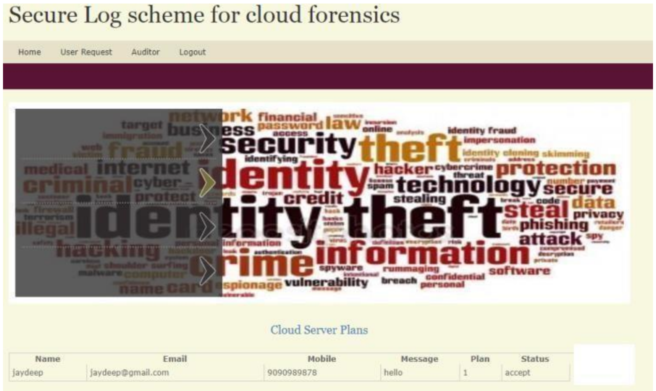
Hard Disk: - 2 GB or more.
Database: - MYSQL
Language: - JAVA
IDE:-Eclipse



Secure Log scheme for cloud forensics

Fig 2: - Server

Authorized user can only able to send request for computer resources to cloud server. User received the resources from server if Server authenticates the user.

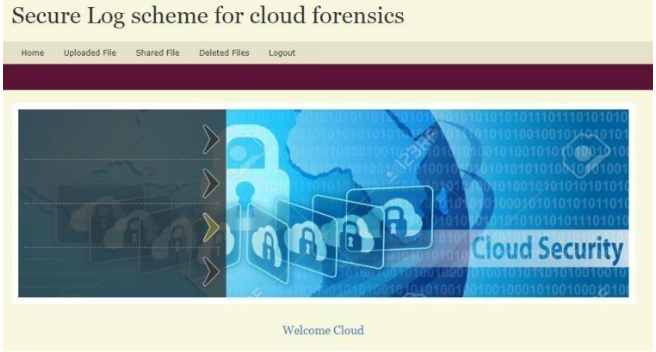


Secure Log scheme for cloud forensics

Name	Email	Mobile	Message	Plan	Status
jaydeep	jaydeep@gmail.com	9090989878	hello	1	accept

Fig 3: - Server provide service to user as per demand

Cloud server provides the resources as per demand of particular user.Server has authority to reject the request to particular user.



Secure Log scheme for cloud forensics

Fig 4: - User activity

Legitimate user interacts with cloud resources by performing different activities and receives response immediately from the cloud. Corresponding logs are always generated and saved at cloud server as these contain valuable information which helps in cloud forensics.

Conclusions

In proposed work, secure log system is designed which will provide secure and reliable logs to investigator for cloud forensics. Secretness and Privacy of cloud user will be preserved by using searchable encryption technique. Modification of logs by server is not possible as logs are fully encrypted. This work can be extended to detect different cloud attacks like man-in-the-cloud-attack, insider attack or other available log analyzer programs for detecting cloud attacks and helping in cloud forensics procedures.

References

[1]. Ahsan MM, Wahab AW, Idris MY, Khan S, Bachura E Choo KK. CLASS: Cloud Log Assuring Soundness and Secrecy Scheme for Cloud Forensics. IEEE Transactions on Sustainable Computing. 2018 May 7.

[2]. Anwar, Faiza, and Zahid Anwar. Digital forensics for eucalyptus. In 2011 Frontiers of Information Technology, pp. 110-116. IEEE, 2011.

[3]. Shams Zawoad, Amit Kumar Dutta, Ragib Hasan, Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service, Dependable and Secure Computing IEEE Transactions on, vol. 13, no. 2, pp. 148-162, 2016.

[4]. Mehto K, Moriwal R. A secured and searchable encryption algorithm for cloud storage. International Journal of Computer Applications. 2015 Jan 1; 120(5).

[5]. Lokhande, Prathmesh, and Vanita Mane. Log based privacy preservation in cloud forensic. (2016).

[6]. Ray, Indrajit, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram. Secure logging as a service—delegating log management to the cloud. IEEE systems journal 7, no. 2 (2013): 323-334.

[7]. Sophia, G.A. and Gandhi, M., 2017, February. Stealthy DDoS detecting mechanism for cloud resilience system. In Information Communication and Embedded Systems (ICICES), 2017 International Conference on (pp. 1-5). IEEE.

[8]. B. Schneier and J. Kelsey, Secure audit logs to support computer forensics, ACM Transactions on Information and System Security

[9]. (TISSEC), vol. 2, pp. 159-176, 1999]http://www.hitachi.com/rd/portal/contents/story/searchable_encryption

[10]. Shams Zawoad, Ragib Hasan," I Have the Proof: Providing Proofs of Past Data Possession in Cloud Forensics", 2012 arXiv.

[11]. J.Ramya Rajalakshmi, M.Rathinraj, M.Braveen," Anonymizing log management process for secure logging in the cloud", 2014 IEEE.

[12]. Tomar Kuldeep, Tyagi S.S, Agrawal Richa," Overview - Snort Intrusion Detection System in Cloud Environment", 2014 International Journal of Information and Computation Technology