As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(05):559-562, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0805085
Available online at: http://www.ijmtst.com/vol8issue05.html

Secure Log Scheme for Cloud Forensics – A study

Roncy K J | Dhanya G S

Departmentof Computer Science, St. Albert's College (Autonomous), Cochin, Kerala, India
Corresponding author Email ID: dhanyagnambiar@gmail.com

To Cite this Article
Roncy K J and Dhanya G S Secure Log Scheme for Cloud Forensics – A study. International Journal for Modern Trends in Science and Technology 2022, 8(05), pp. 559-562. https://doi.org/10.46501/IJMTST0805085

Article Info
Received: 22 April 2022; Accepted: 12 May 2022; Published: 26 May 2022.

ABSTRACT

Organizations nowadays employ cloud infrastructure to store data because there is no requirement for a local configuration in the user system. The user must have internet access in order to get data from the cloud. When the internet enters the picture, a lot of attacks occur on the cloud, and cloud forensics is used to detect and prevent those attacks. It's also crucial to keep a secure user log file on the cloud because the cloud log provides essential information that aids forensics investigations. Previous logging systems had several flaws when it comes to offering security to cloud users. The current system provides security for user files that are uploaded by the user, as well as user login authentication. In this secure logging, the scheme is provided by encrypting cloud logs It detects DDoS (distributed denial of service) attacks on the cloud infrastructure utilizing encryption techniques. It can be identified by looking at the cloud server's available cloud logs. Encryption methods will be used to improve the security of the logging system and to maintain the confidentiality and security of client data.

KEYWORDS: *DDoS, cloud logs, forensics, encryption, confidentiality*

1. INTRODUCTION

Cloud computing can be characterized as a model for providing ubiquitous, useful, on-demand network access to a shared pool of resources. It configures computer assets and can be immediately provisioned and launched with minimal management work or contact from service providers. It is a low-cost approach and a pay-per-use service. As a result, both small and large businesses are being drawn to cloud computing. Customers do not need to configure their systems in any way. Cloud frameworks are typically afflicted by security concerns, notably when it comes to PC criminology. Certain flaws make it easy for a bad person to scan and exploit the power of cloud computing. An attacker can carry out malicious behavior on a cloud-based. Cloud Forensics is mostly concerned with specific issues. Because of the essential nature of cloud advancements, traditional digital forensics methodologies, as well as apparatuses, should be updated to maintain the same value and confidentiality in a cloud domain.

To detect and prevent the attack, forensics in the cloud is used. A digital forensics approach will be used to detect a cloud-based attack. When an attack occurs on the cloud or in another field, the term "forensics" should be used. First and first, occurrences must be identified, the evidence must be collected, the evidence must be examined, and evidence must be presented against attack. The basic information hotspot for system

monitoring is log records. A log of the document is a piece of framework-created information to keep track of usage patterns, exercises, and activities within a working framework, application, worker, or any other device.

2. POSSIBLE VULNERABILITY POINTS FOR CLOUD LOG ATTACK

Log generation: - This is the point of vulnerability when an attack might occur while generating logs on the cloud. This sort of log comprises data such as the host, server information, and so on. So, if an attacker obtains this type of information, he or she can use it to carry out malicious behavior on the host.

Log collection: - During the process of gathering logs from numerous sources.

Network: - This is a network assault that occurs between log collector agents and logs storage resources.

Log storage: - Logs are saved on some resources and collected by log collector agents, as well as other cloud storage resources.

Log analysis: - This is the susceptible point where an attack occurs after the investigator analyses the logs of malicious activities.

3. DIFFERENT TYPES OF THE CLOUD ATTACK

Cloud malware injection: - Create a cloud service with an infected service. Manipulate or steal data from users.
Denial of service attack: - Sending requests from a single machine will Overburden the system. The system is unavailable to legitimate users.
Distributed DDoS: - Send repeated queries from multiple devices to Overload the system.
Man in the middle attack: - The name implies that the attacker sits between the source and the destination and manipulates data.
Side-channel: - Hackers install a virtual machine on the host computer.
Insider: - It is started by a genuine user.

Cloud virtual machines (VMs) can be placed remotely; they are not physically accessible and may be spread across multiple real-world devices. As a result, it is impossible to obtain specifics of the investigations by clinging to the forensic analysis system. Information is made up of a virtual machine that can be unpredictable and can be lost if the force is turned off or the virtual machine is terminated. When it comes to acquiring evidentiary information, the server, or cloud service provider, plays a significant role. Normally, each client's activity log (cloud log) is created by the cloud service provider. The log contains sensitive information that CSP, other users, or investigators should not have access to. As a result, it's vital to prevent making changes to the logs, maintain proper chronological documentation, and ensure data security.
The system's limitation is that the processing time necessary to search the log entry is longer, because tags are attached with log entries to make searching easier. Each log entry is assigned a unique tag. According to the study, there is a paucity of research in cloud forensics, which is why this issue was chosen.
They provide us with security on files that are uploaded to the cloud by the user in the current system. This is equally crucial, but there are few documents that provide protection against sensitive information and insider attacks, which is why this system provides excellent security against sensitive information and detects insider attacks.

4. LITERATURE SURVEY

The authors [2] employ Eucalyptus for the analytic cloud application, Eucalyptus logs, and IaaS to construct their dataset. Eucalyptus is hosted on a virtual machine in this paper, and they constructed a VM that looks like it. 1) The Cloud Controller (CLC) is a Software Programme that manages the cloud. -be a part of a team of administrators 2) The Cluster Controller (CC) is responsible for communicating with the storage controller. 3) Create cache and detect DDoS attacks with the Node Controller (NC). The absence of encryption is a flaw in this study.

Because individual cloud databases may act maliciously, the Integrity database is created with a secure logging structure [3]. This is why the system is integrated with a database. The log and block data are stored in MongoDB.

Three blocks make up block data. The first virtual machine is used to write the log, the second is used to provide secure log service, and the third is used to run the cloud database. Because three machines share a single host, the time spent increasing logs is longer. The

disadvantage is that a single host cannot properly handle three virtual machines; two hosts are required. The public key is used in this work to encrypt log auditor and verify log data integrity. A secret key is used to construct a block of data and a signature, after which the log auditor sends a logging request to the secure logging service to verify the log data's integrity. HSM is a physical device for storing secret keys that leverages an Oracle cloud Virtual Box.

Authors employ REST as a web service, i.e. (Representational State Transfer) services are stateless, allowing several servers to process different requests at the same time, improving server scalability. Web services that focus on a system's resources can be created using REST. The resource for logging as a service is logs and log proofs. HTTP standard methods (eg. GET, PUT, POST, DELETE) are used to construct RESTful web services. The GET action is used on a resource to retrieve it according to the REST principle. The HTTPS protocol and the Snort tool are used to ensure the security of REST web services. It employs a private cloud and leverages OpenStack as a cloud open-source platform.

OpenStack is a cloud open-source technology in which users produce private keys using AES and then share those keys with other users. A sharing cloud can be created as a result of this. If the user wants to exchange data, the public key is utilized. T p' s bloom filter has modified, which is why bloom tree was introduced. Encrypt logs with the user's private key, then distribute the key to various CSPs via public keys in the cloud. The bloom filter is used in hashing, while the Rabin fingerprint is used to avoid duplicate data.

5. PROPOSED ARCHITECTURE FOR SECURE LOG SCHEME

- The code is deployed via a server such as miles web, layer shift, Heroku, and others. The database SQL file and the project. war file has been submitted.
- There are a variety of choices for creating log entries, including Syslog-ng, Eucalyptus, and other programs, as well as some cloud hosting.
- The server provides the user with project and database links.

In the proposed technique, the user first logs into the system, after which he or she can choose a server plan (number of processors, memory, disc space, and price). A user makes a request for cloud access services to a cloud service provider (CSP). Once the CSP confirms the user's request, the user performs cloud-based activities such as uploading, deleting, sharing, and updating files. User log entries are generated and encrypted (email, MAC, and IP addresses are encrypted, and I p digest is done using hashing). If a DDos attack is launched, DDos logs are generated; CSPs and investigators then validate and access logs from the database, revealing the attacker's IP address. Insider DDoS attacks are detected by this system, which has 150 thresholds for detecting DDoS attacks. If the insider value surpasses the threshold, the system will display user information. A password-based AES algorithm is employed in the proposed system, which includes iteration, a secret key, and 256 bits of the same key for encryption and decryption. In this method, salt is also used during encryption, and there are two iteration counts; the goal of utilizing iteration is to increase difficulty and slow down the attack pace. In this system, a secret key is generated first, and then a random string (salt) is added at the end.

6. RESULTS

This system presents the most secure logging approaches for cloud forensics utilizing modern encryption methods and validates a framework to detect DDoS attacks in cloud computing. The MD5 technique is used to calculate the hash value for the user's IP address. The user's sensitive information is encrypted and saved in the database using the AES technique.

The AES technique is used to encrypt user sensitive data, and MD5 hashing is utilized to hash encrypted IP, MAC, and email addresses. Because attackers can easily obtain IP addresses and attack on the system if sensitive information is kept in plain text, this system provides twofold protection on sensitive information.

If a malicious act, such as a DDoS assault, has occurred, the investigator will display information about the perpetrator.

Many cloud attacks occur, but invader or insider attacks must be identified, and this technology is designed to detect insider DDoS attacks. The system is set at a threshold value for this attack, and if an insider tries to launch an attack, the value is exceeded, and all of the attacker's information is displayed on the console.

7. CONCLUSION & FUTURE WORK

The proposed effort will create a secure log system that will offer investigators with secure and trustworthy logs for cloud forensics. Cloud users' privacy and secrecy will be protected thanks to a searchable encryption mechanism. The encryption system employs a password-based AES method that includes iteration, salt, and MD5 hashing on encrypted IP addresses. The current system and a small number of authors focused on user sensitive information, but new system is more robust because it encrypts and hashes sensitive data and detects insider DDoS attacks.

When compared to the previous method, our approach is more secure because it focuses on the user's sensitive information, such as their IP address. Email address and MAC address While other solutions focus on safeguarding files, user authentication, and so on, encrypting user sensitive information is also essential because anyone may obtain the user's IP address and launch a cloud attack.

This work might be expanded to identify various cloud assaults, encrypt files uploaded by users, and define parameters for CSPs to allow or reject cloud user requests

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Ahsan, M. M., Wahab, A. W. A., Idris, M. Y. I., Khan, S., Bachura, E. & Choo, K.K. R. (2018), 'Class: Cloud log assuring soundness and secrecy scheme for cloud forensics', IEEETransactions on Sustainable Computing.Anwar, Faiza, and Zahid Anwar "Digital forensics for eucalyptus. In 2011 Frontiers of Information Technology", pp. 110-116. IEEE, 2011.

[2] Chung-Yi Lin, Ming-Che Chang, Hua-Chou Chiu, and Keh-Hwa Shyu "Secure Logging Framework Integrating with Cloud Database",2015 IEEE.

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

[4] Shams Zawoad, Ragib Hasan," I Have the Proof: Providing Proofs of Past Data Possession in Cloud Forensics", 2012 arXiv.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[5] Ali, A., Ahmed, M., Ilyas, M. & Ku¨ ng, J. (2017), MITIS-An Insider Threats Mitigation Framework for Information Systems, in 'International Conference on Future Data and Security Engineering', Springer, pp. 407–415.

[6] Ali, A., Ahmed, M., Khan, A., Ilyas, M. &Razzaq, M. S. (2017), A trust management system model for cloud, in 'International Symposium on Networks, Computers and Communications (ISNCC), 2017', IEEE, pp. 1–6.

[7] Amar, M., Lemoudden, M. & El Ouahidi, B. (2016), Log file's centralization to improve cloud security, in '2ndInternational Conference on Cloud Computing Technologies and Applications (CloudTech), 2016', IEEE, pp. 178–183.

[8] Blass, E.-O. &Noubir, G. (2017), 'Secure Logging with Crash Tolerance.',IACR Cryptology ePrint Archive 2017, 107.

[9] Bonomi, F. (2011), Connected vehicles, the internet of things, and fog computing, in 'The eighth ACM international workshop on vehicular internetworking (VANET), Las Vegas, USA', pp. 13–15.

[10] Bonomi, F., Milito, R., Zhu, J. &Addepalli, S. (2012), Fog computing and its role in the internet of things, in 'Proceedings of the first edition of the MCC workshop on Mobile cloud computing', ACM, pp. 13–16.

[11] Boyle, B. (2015) (accessed December 20, 2016), Edge market will boost demand for micro data centers. URL: http://www.datacenterdynamics. com/powercooling/edge-market-will-boost-demand-for-micro-data-centers/95070

[12] Chong, C. N., Peng, Z. &Hartel, P. H. (2003), Secure audit logging with tamper-resistant hardware,in 'IFIP International Information Security Conference', Springer, pp. 73–84.

[13] Henze, M., Wolters, B., Matzutt, R., Zimmermann, T. &Wehrle, K. (2017), Distributed configuration, authorization and management in the cloud-based internet of things, in 'Trustcom/BigDataSE/ICESS, 2017 IEEE', IEEE, pp. 185–192.

[14] Holt, J. E. (2006), Logcrypt:forward security and public verification for secure audit logs, in 'Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54', Australian Computer Society, Inc., pp. 203–211.

[15] Ko, R. K., Jagadpramana, P. & Lee, B. S. (2011), Flogger: A file-centric logger for monitoring file access and transfers within cloud computing environments, in 'IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011', IEEE, pp. 765–771.

[16] LOGalyze - Open Source Log Management Tool, SIEM, Log Analyzer (n.d.). Accessed on May10,2018. URL:http://www.logalyze.com/

[17] Ma, D. &Tsudik, G. (2007), Forward-secure sequential aggregate authentication, in 'IEEE Symposium on Security and Privacy,2007. SP'07', IEEE, pp. 86–91.