2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

CLOUD LOG ASSURING SOUNDNESS AND SECRECY SCHEME FOR CLOUD FORENSICS

#1MALLEPALLY KAVITHA, #2K.DEEPTHI

[1]M.TECH STUDENT, DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM, RANGAREDDY,T.S.

[2]ASSISTANT PROFESSOR, DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM, RANGAREDDY,T.S.

Abstract:- We introduce the challenges to digital forensics introduced by the advent and adoption of technologies, such as encryption, secure networking, secure processors and anonymous routing. All potentially render current approaches to digital forensic investigation unusable. Cloud information repository is involved with issues of information integrity, data security and information access by unapproved users. Hence, an autonomous reviewing and auditing facility is necessary to guarantee that the information is effectively accommodated and used in the cloud. In this paper, a comprehensive survey on the state-of-art techniques in data auditing and security are discussed. Challenging problems in information repository auditing and security are presented. Finally, directions for future research in data auditing and security have been discussed.

Key Words:- *Cloud Forensics; Challenges.*

I. INTRODUCTION

Cloud storage, security and privacy are fairly established research areas [1-7], which is not surprising considering the widespread adoption of cloud services and the potential for criminal exploitation (e.g. compromising cloud accounts and servers for the stealing of sensitive data). Interestingly though, cloud forensics [8- 10] is a relatively less understood topic. In the event that a cloud service, cloud server, or client device has been compromised or involved in malicious cyber activity (e.g. used to host illegal contents such as radicalization materials, or conduct distributed denial of service (DDoS) attacks) [11, 12], investigators need to be able to conduct forensic analysis in order to "answer the six key questions of an incident – what, why, how, who, when, and where" [13].Due to the inherent nature of cloud technologies, conventional digital forensic procedures and tools need to be updated to retain the same usefulness and applicability in a cloud environment [14]. Unlike a conventional client device, cloud virtual machines (VMs) can be supported by hardware that might be located remotely and thus would not be physically accessible (e.g. out of the jurisdictional territory) to an investigator.

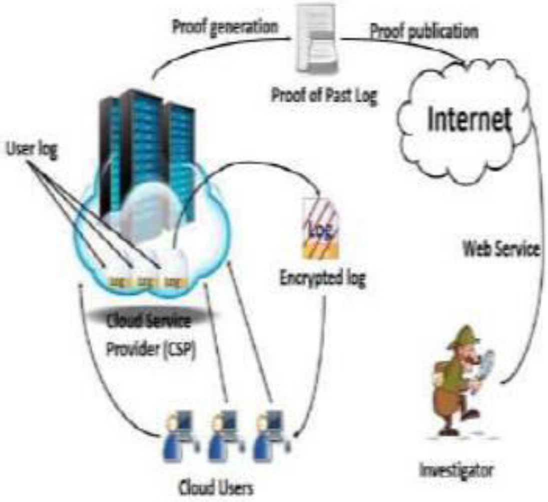


Fig.1. overview of class scheme process

In addition, VMs can be distributed across multiple physical devices in a clustered environment or they can exist within a pool of VMs on the same physical components. Therefore, seizing the machine for forensic analysis is not In addition, VMs can be distributed across multiple physical devices in a clustered environment or they can exist within a pool of VMs on the same physical components. Therefore, seizing the machine for forensic analysis is not viable in most investigations. Furthermore, data residing in a VM may be volatile and could be lost once the power is off or the VM terminates. Hence, the cloud service provider (CSP) plays a crucial role in the collection of evidential data (e.g. cloud user's activity log from the log). For example, the CSP writes the activity log (cloud log) for each user. Thus, preventing modification of the logs, maintaining a proper chain of custody and ensuring data privacy is crucial [15]. This research considers "activity log data" as any recorded computer event that corresponds to a specific user. Such data must be maintained confidentially to preserver user privacy and to facilitate potential investigative activities.

II. RELATED WORK

Reliable cloud logs play a crucial role in forensic investigations. Log acquisition, maintaining confidentiality, integrity and forward secrecy, validity verification and accessibility by investigators (or another approved party), area unit a number of the numerous totally different dimensions a rhetorical investigator and scientist ought to listen to. Anwar et al. [20] tried to deal with a number of these challenges by distinctive

the chance of Sys log or snort log to help within the detection of cloud attacks. The authors conducted cloud rhetorical investigations supported the logs generated by Eucalyptus, associate ASCII text file cloud computing code. Specifically, they generated their own dataset by simulating a DDoS attack on Eucalyptus and known the offensive machine informatics address by analyzing the log. Security, access management, and verification of log weren't thought of. Patrascu and Patriciu [21]

planned a rhetorical module to be maintained as a part of the cloud's controller module, that is meant to speak with a unique stack of cloud assets (e.g. virtual filing system, computer memory, network stack, and call interface) so as to gather and store logs. Similarly, security of the collected log (either in transmission or in storage) wasn't thought of.

Ranking: Ranking algorithm performs the k-result set generation based on TF-IDF scores. The data retrieved will be the most relevant to users. It uses how frequently a term occurs in a document. Every outsourced file is different in size; it is possible that a term would appear much more times in high size documents. Thus, the term frequency is often divided by the total number of terms in the document to get more accurate result. how term frequency is arrived. Inverse Document Frequency (IDF) is the measure of total number of files in cloud storage by an owner to the number of files containing term „t‟. One approach to securely support kNN is to use distance-preserving transformation (DPT) to encrypt data points [27] so that the distance between any two encrypted points in E(DB) is the same as that between the corresponding original points in DB."

J. Oberheide, K. Veeraraghavan in, 2008 [2] proposed the storage level security of cloud storages. A model is proposed, in which mobile antivirus functionality is moved to an off-device network service employing multiple virtualized malware detection engines. In his work, they moved detection capabilities to a network service. Thus each file is analyzed by multiple detection engines. We then propose a cloud-aided frequent item set mining solution, which is used to build an association rule mining solution. Our solutions are designed for outsourced databases that allow multiple data owners to efficiently share their data securely without compromising on data privacy. Our solutions leak less information about the raw data than most existing solutions. In comparison to the only known solution achieving a similar privacy level as our proposed solutions, the performance of our proposed solutions is three to five orders of magnitude higher. Based on our experiment findings using different parameters and data sets, we demonstrate that the run time in each of our solutions is only one order higher than that in the best non-privacy-preserving data mining algorithms. Since both data and computing work are outsourced to the cloud servers, the resource consumption at the data owner end is very low.

Analysis of Forensic Model: Analysis of the evaluation in discussion of the literature, it can be deduced that progress is being made on building digital forensic systems capable of being deployed on cloud environments. More work still needs to be done on digital forensic systems aimed for the cloud as well as on systems that support digital forensic readiness. A larger amount of work still had be done on standardising digital forensic processes as this aspect is the least supported in model. Live forensics as well still requires more attention from researchers an implementers of digital forensic systems.

III. PROPOSED METHOD

By Extending SecLaaS, we propose a secure cloud logging scheme, Cloud Log Assuring Soundness and Secrecy (CLASS), designed to ensure CSP accountability (i.e.writing the correct information to the log) and preserve the users privacy–i.e. our contribution in this paper. Specifically, we include the capability for the user to verify the accuracy of their log. To do this, the log will be encrypted using the user's public key (rather than the agency's public key). To avoid introducing unnecessary delays to the forensic investigation, during user registration with the cloud service, both the CSP and the user will collectively choose a public private key pair referred to as contentconcealing key (CC-key) for the user. The corresponding (content concealing) private key will be shared with other CSPs using Shamir's [17] or Blakley's [18] secret sharing schemes. This would allow the private key to be regenerated whenever necessary. We also demonstrate how we can leverage Rabin's fingerprint [19] and bloom filter in PPL generation to establish log veracity We then implement CLASS in Open Stack and evaluate its performance.

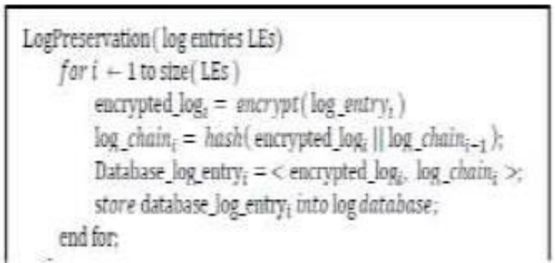
IV.ALGORITHM

1. CLASS algorithms:

can be categorized into two major groups: One for Log Preservation and one for Proof Accumulation. The Log Preservation algorithm can take log entries individually or in a batch and performs processing prior to storage in a log database. This algorithm encrypts for secrecy and generates hash digest for consistency. The Proof Accumulator algorithm performs daily processing of all log entries corresponding to an IP address to prepare and publish proof of past log(PPL).

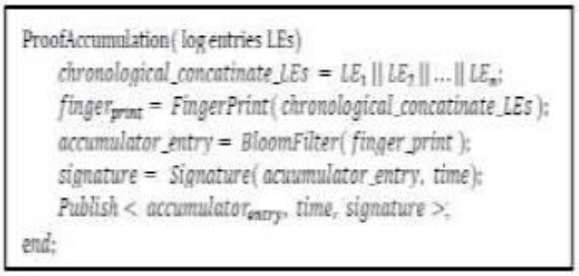
2. Shamir's secret sharing algorithm:

Small information will be extracted from private key following Shamir's secret sharing algorithm and each portion will be shared to one CSP. After getting secret portions of a particular user, the host cloud can reconstruct the private key to decrypt the log of that user using Shamir's secret sharing algorithm.



```
LogPreservation( log entries LEs)
    for i ← 1 to size( LEs )
        encrypted_log_i = encrypt( log_entry_i )
        log_chain_i = hash( encrypted_log_i || log_chain_{i-1} );
        Database_log_entry_i = < encrypted_log_i, log_chain_i >;
        store database_log_entry_i into log database;
    end for;
```

Algorithm 1. LogPreservation pseudocode for processing log entries

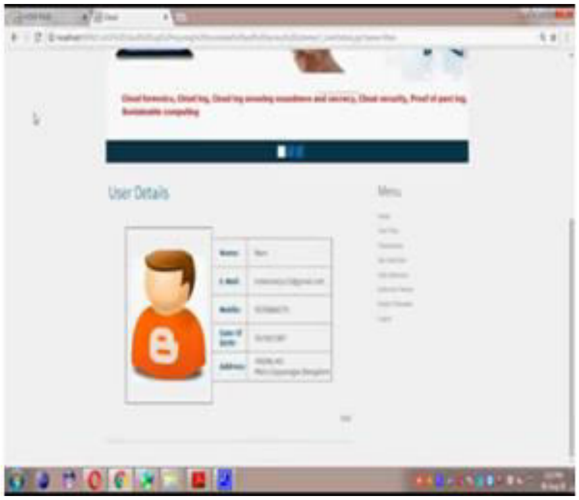


```
ProofAccumulation( log entries LEs)
    chronological_concatinate_LEs = $LE_1 || LE_2 || ... || LE_n$;
    $finger_{print}$ = FingerPrint( chronological_concatinate_LEs );
    accumulator_entry = BloomFilter( finger_print );
    signature = Signature( acuumulator_entry, time);
    Publish < $accumulator_{entry}$, time, signature >;
end;
```

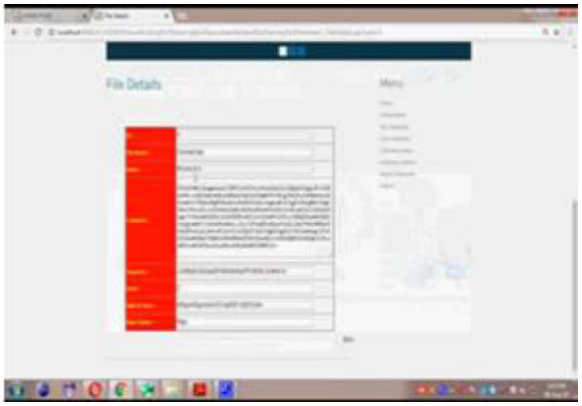
V. RESULTS

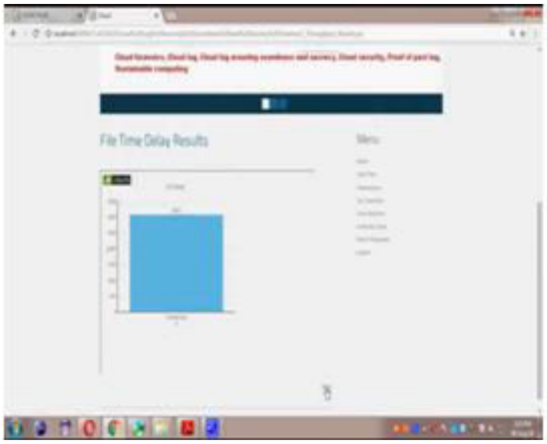
Cloud Login:

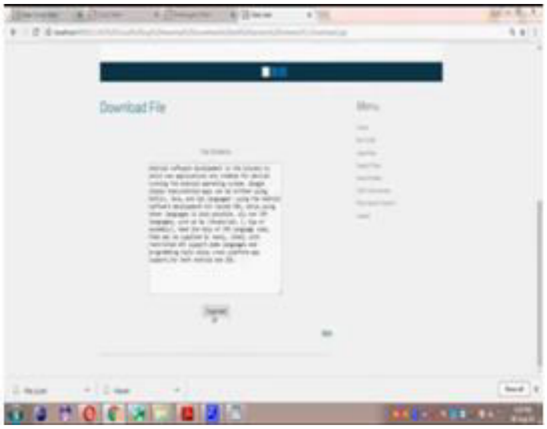
User Details:



Files details:




Cloud forensics, Cloud log, Cloud log ensuring soundness and secrecy, Cloud security, Proof of past log, Sustainable computing
File Time Delay Results
Menu



VI. CONCLUSION

In this paper, we proposed a secure logging scheme (CLASS) for cloud computing with features that facilitate the preservation of user privacy and that mitigate the damaging effects of collusion among other parties. CLASS preserves the privacy of cloud users by encrypting cloud logs with a public key of the respective user while also facilitating log retrieval in the event of an investigation. Moreover, it ensures accountability of the cloud server by allowing the user to identify any log modification. This has the additional effect of preventing auser from repudiating entries in his own log once the log has had its PPL established. Our implementation on Open Stack demonstrates the feasibility and practicality of the proposed scheme. The experimental results show an improvement in efficiency thanks to the features of the CLASS scheme, particularly in verification phase.

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 Transactions on Cloud Computing, 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," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 1259-1268, 2017.

[7] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-Scalable Byzantine Fault-Tolerant Services," in *ACM Symposium on Operating Systems Principles (SOSP)*, 2005, pp. 59–74.

[8] M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in *International Conference on Dependable Systems and Networks (DSN)*, 2005, pp. 336–345.

[9] W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doublyiterated, ideal ciphers," in *Advances in Cryptology (CRYPTO)*, 1998, pp. 390–407.

[10] C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, "Robust Data Sharing with Key-value Stores," in *ACM SIGACTSIGOPS Symposium on Principles of Distributed Computing (PODC)*, 2011, pp. 221–222.

[11] A. Beimel, "Secret-sharing schemes: A survey," in *International Workshop on Coding and Cryptology (IWCC)*, 2011, pp. 11–46.

[12] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: Dependable and Secure Storage in a Cloud-ofclouds," in *Sixth Conference on Computer Systems (EuroSys)*, 2011, pp. 31–46.

[13] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology (CRYPTO)*,1984, pp. 242–268.

[14] V. Boyko, "On the Security Properties of OAEP as an All- ornothing Transform," in *Advances in Cryptology (CRYPTO)*, 1999, pp. 503–518.

[15] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption," in *Proceedings of CRYPTO*, 1997.

AUTHOR'S PROFILE:

[1]. **MALLEPALLY KAVITHA,** Pursuing *M.Tech in CSE* **at** Scient Institute Of Technology, Ibrahimpatnam, Rangareddy, T.S.

[2]. **Mrs.K.Deepthi,** She pursued her B.Tech in GNITS from JNT University Hyderabad, M.Tech Software Engineering from JNT University Hyderabad, She is currently working as Asst Prof in the Department of CSE at **Scient Institute of Technology Ibrahimpatnam**. She has 11 years of Academic experience. Her research areas include Software Engineering and Data mining. She has published 4 international journals and participated in One International Conference. She Attended Many Workshops in different areas.