ISSN 2395-1621

A Survey on Secure Log Schemes for Cloud Forensics

[#1]Shweta N.Joshi, [#2]Prof.Geetha R.Chillarge

[#12]Dept.of Computer Engineering

MMCOE, Pune

ABSTRACT

Cloud Computing is becoming so popular because of simplicity, large storage, availability, Easy maintenance, Automatic system, on-request self-service, pay per use & so on. Companies also used the cloud to store their data because they do not require any local infrastructure setup. Digital forensics is a subcategory of cloud forensics. Implement all the processes of digital forensics within the cloud environment being called cloud forensics. Investigators play a necessary role in cloud forensics, but there is an absence of assist for cloud forensics. User activity logs play a major role during cloud forensic investigations and also, secure the trustworthiness and honesty about this type of logs are important. Logging scheme plays a critical role within cloud forensics so lots of schemes introduced to secure log have been devised. This paper considers various techniques and schemes for secure log in cloud computing.

Keywords— Cloud Computing, Types of cloud, Service models, Cloud Forensics.

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

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[4]

Cloud-based computing offers unlimited resource access as well as less-cost computing. Consequently, cloud-based computing is very famous computing within the latest years. Today, companies are widely using cloud-based computing because it's not necessary any kind of local infrastructure setup. Cloud-based Computing is an essential interchange in how we save data as well as run applications. In place of runnable programs as well as data on the desktop computer, everything is hosted over the cloud, as well as all your document & data can be access from anywhere. Cloud- based computing offers unlimited framework resources very commodious pay-per-use service as well as less-cost computing. Cloud-based computing is based upon internet technology it is utilizing hardware as well as software as computing resources to give service through the internet. Cloud computing usages are increasing nowadays allowing the end-user to create as well as use software from wherever at any moment. Every entry of log includes details related to a specific incident such has happened inside a system otherwise within a network. The logs have been used to troubleshooting problems, such as optimized the system, to look at the execution about the network, record the activity of users, as well as provide valuable data for find suspicious activity. Cloud computing mostly useful for business and IT organizations. Malicious activity easily exploits the security of cloud-based computing. An attacker can make the malicious activity on applications running within the cloud. These problems are the essential point of Cloud Forensics so forensic experts are devising new approaches for digital forensics.

A Distinct variety of cloud

A. Public Cloud
B. Private Cloud
C. Hybrid Cloud
D. Community Cloud

Public Cloud: - Public cloud computing services are provided by third-party providers and making them available publicly so anyone can use it or purchase them. It may be free or sold on-demand, according to customer usages. [20]

Private Cloud: - Private clouds shall be built as well as manage by a within a company or by a cloud provider because the private cloud is maintained by internal resources.

Hybrid Cloud: - Hybrid Cloud is nothing but a composite about public & private cloud.

Community Cloud:-Community cloud provides several companies can operate on a similar platform because they have the same need & concern. It is either managed by companies or by a third party. [4]

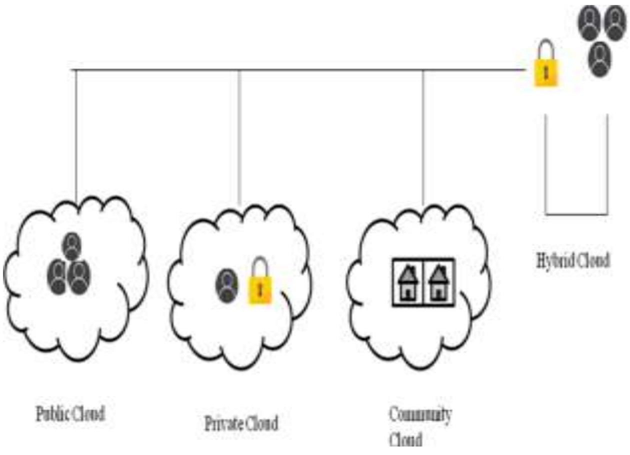

Fig 1:-Types of cloud [18]

Service Models

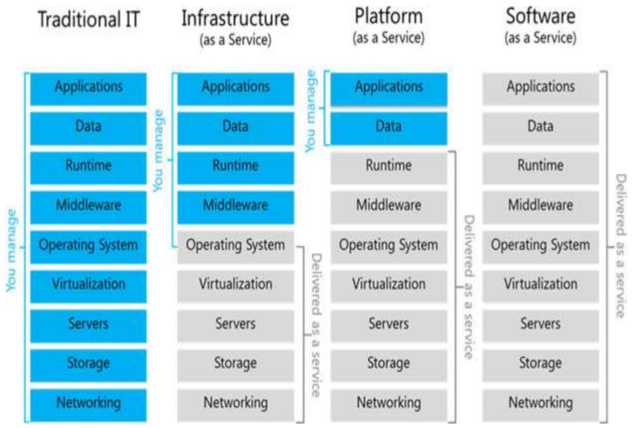

Fig 2:- Service models in a cloud [19]

To identify the attack in the cloud environment, we must apply digital forensics process in cloud computing. Currently, wide research is going on to protect clouds from attackers may be internally or externally. If the attack happens then we need to investigate it and protect the cloud from attack.there is a lack of research on cloud forensics and also more research is required for benefit of digital forensics within cloud environments. [4]

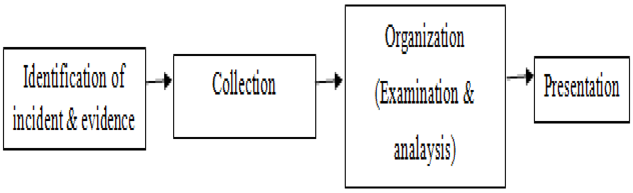
Identification of incident & evidence
Collection
Organization (Examination & analaysis)
Presentation

Fig 3:- Digital forensics [4]

II. RELATED WORK

Secure Log Schemes

From [1] authors, proposed scheme which is not based on any secure hardware like HSM (Hardware Security Module) they provide secure logging through unique authentication tag they generate public & private key also provides signature-based technique & proposed verification algorithm & also detect insider & outsider attacks & also proposed public & private verifiable schemes.

From [2] authors proposed the scheme to secure proof for investigators to generate a proof for analyze the honesty about log. For analysis data required previous content but in the cloud, only current content retrieved so this author proposed a scheme for accessing previous content.

From [3] authors the solution for cloud forensics by providing secure logging with the operating system and the security logs. Cloud computing environment of Eucalyptus was set up applying Snort, Syslog, as well as Log Analyzer. They examined the characteristics 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.

From [6] author presented a framework, where the cloud server gets a series of logs through authenticated channels from a logger or else log accumulator. Then, the cloud server tries to maintain confidentiality, integrity, availability, and verifiability of secure logs.

From [7] D.Esther Grace Vinitha, J.Shiny Duela proposed Efficient Privacy Protection Scheme (EPPS) in this scheme authors implement two-fold encryption that is hash function & encryption algorithm for a secure log.

From [8] Authors proposed a novel scheme that is Homomorphic Encryption in this scheme authors implement Homomorphic algorith& in this they used encryption, secret key, hash function & also used tor network to provide security, companies can share their private data on the public network securely.

From [9] Tomar Kuldeep, Tyagi S.S, Agrawal Richa talk about snort. Snort is Intrusions Detection Systems which handle attacks. Intrusions Detection Systems (IDS) in a cloud environment become more ensure and efficient to detect the intrusion on host or any network.

From [10] authors identifies 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 the user is subject to an investigation via a court order.

From [11] authors proposed a secure log on cloud with the help of HSM (Hardware Security Module) it is a physical device based on cloud to provide extra security on the cloud. In this secure logging framework they use the public key for verify the honesty about log & secret key to generate signature of log & also they use cloud database for stored log data & all keys are stored into HSM hardware.

From [12] authors proposed a secure log scheme through bulletin board it is open source & useful to stored log in secure way.

From [13] authors discussed various methods for encrypting user data and identifying the user data and privacy. They listed the number of methods of searchable encryption to secure the data on cloud storage.

From [14] proposed a secure logger with the processor & chip.it prevents for modification in logs which is stored on the cloud.

From [15] Haonan Su, Dong Zheng, Yinghui Zhang proposed convergent encryption to reduce duplicate data from cloud & this encryption mostly use in cloud computing.

From [16] authors proposed a scheme which is maintaining security & integrity.in this if a hacker tries to access password then system blocked that person.only authroize person can access data.

From [17] authors proposed a scheme for the security of log they used secret key as encryption algorithm & they generate daily proof so that investigators easily investigate attack if happen.

Sr. No	Paper title	Methodology	Description	Remark
1	A new approach to secure logging	public & private verifiable schemes	They use Forward-Secure & Sequential Aggregate technique & this technique not depend on any Secure hardware.	We can not trust on any hardware or third party that is why this technique is more secure.
2	I Have the Proof: Providing Proofs of Past Data Possession in Cloud Forensics	Proofs about Past Data Possession	The design for checking integrity of log using bloom filter.	Bloom filter contain membership data which is helping to authenticate user when accessing the data from cloud or upload file on the cloud.
3	Digital Forensics for Eucalyptus	Open source cloud computing tool	Security, access control and verification of log were not considered in this work.	Examining logs through an Open source cloud computing tool it may or may not be secure because sometimes tools are not working properly so we can not analyze logs.
4	Secure Logging As a Service-Delegating Log Management to the Cloud	Forward Integrity as well as Secrecy for Log Records, Tor network	They encrypt log entries with a chain of sequentially generated keys to protect logs from privacy violation & to preserve integrity. To protect security they use symmetric key encryption & no choice for public verifiability.	In this paper, it provide security & integrity in the all phases of log using tor network but tor network is open source so it is not so much secure because anybody can install it & use it.
5	A secure event log storage management system in cloud computing	Two-fold encryption	Author’s use hash function & encryption for secure log storage.	Author’s uses hash function but the hash function has cryptographic weakness & If you lose the key to the encryption, you have lost the data associated With it.
6	Anonymi-ing log management process for secure logging in the cloud	Homomorphc encryption	They implement Homomorp ic RSA algorithm & property of Paillier algorithm.	Homomorphic encryption gives more security than other encryption algorithms & it is mostly use for cloud security.

7	Overview- Snort Intrusion Detection System in Cloud Environment	Snort	It is used snort for intrusion detection & preventation system & it is used for anlysis real time traffic & data flow in network.	Snort might give you false positive results & it requires a lot of configuration before it used.
8	Towards Building forensics enabled cloud through secure logging as a service	Accumulator	Authors use the accumulator namely the RSA accumulator & Bloom filter to check the integrity of the log.	Bloom filter having a 1% chance to give false-positive results.
9	Secure logging Framework integrity with cloud database	HSM (Hardware Security Module)	They proposed a physical device for stored keys & cloud database for log storage it provides extra security on the cloud.	The Drawback of HSM Expensive in terms of cost. Difficult to upgrade. & also because of cloud database it may face security issues
10	Design & formal verification of a cloud compliant secure logging mechanism	bulletin board	This paper uses a bulletin board to stored logs in a secure way.	It is not so much secure because it is open source anyone can easily attack on it.
11	A Secured and Searchable Encryption Algorithm for Cloud Storage	MD5 AES	Proposed a scheme for secure data accessing with maintaining its privacy by using a strong cryptographic algorithm. For keeping track of data that means document features hash table management and indexing techniques are used	Use of MD5 & AES has some drawback so It requires some feasible solution.
12	Cloud based secure logger for medical devices	Secure logger	This paper use TPM chip for stored all they keys securely & modern Intel CPU which contains SGX that is set of security -related codes built into CPU.	Use of this technique is secure but it is expensive so the use of this technique can be extending for cloud attacks.
13	An Efficient and Secure Deduplicati on Scheme Based on Rabin Fingerprinti ng in Cloud Storage	Rabin fingerprint Convergent encryption	They mention convergent encryption to reduce duplicate data from the cloud.	This work useful to investigators for cloud forensics.
14	Access Control for Cloud Forensics through Secure Logging Services	AES RSA Session key	It uses multiple encryptions for secure log.	It is fewer chances that Hackers can not easily hack logs from the cloud because of the session key.
15	CLASS : Cloud Log Assuring Soundness & Secrecy Scheme for cloud forensics	Two accumulators Secret key	This paper use schemes for secure log storage & used snort for network analyzer.	They use multiple techniques (secret key) for secure logs & prevent logs from the hacker.

III. DISCUSSION

A study of the number of approaches for secure log on a cloud using encryption algorithms, hardware, and accumulators, open-source tools, etc. open-source tools may or may not be secure for analyze logs. The paper also considers a lot of encryption algorithms like MDS, AES, RSA, homomorphic encryption & so on but from that all encryption homomorphic encryption is more secure as compared to other encryption algorithm & also some hardware used for secure log but it is expensive so from this study we conclude that though there are many techniques to provide security for logs but there are no benchmarks for security on cloud logs. Hence we need a system which can provide better security to the cloud logs and in turn prevent the system from intruders and other attacks.

IV. CONCLUSION

In this paper, a study of various schemes to secure log on cloud for cloud forensics is made. The secure logging system should be designed in such a way that it will provide secure and reliable logs to investigators for cloud forensics. Modification of logs is difficult because logs are fully encrypted from homomorphic encryption which is found good as compared to other encryption algorithms & also accumulator is useful for avoiding forbidden access of log.

REFERENCES

[1] ma, tsudik,” A new Approach to Secure Logging”, ACM Transactions on Storage, Vol. 5, No. 1, Article 2, Publication date: March 2009.

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

[3] Zafarullah, Faiza Anwar, Zahid Anwar,” Digital Forensics for Eucalyptus”, 2011 IEEE.

[4] Peter Mell, Timothy Grance,” The NIST Definition of Cloud Computing”, 2011 NIST Special Publication.

[5] Zawoad, Ragib Hasan,” Digital Forensics in the Cloud”, CrossTalk—September/October 2013

[6] Ray, Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram,” Secure Logging As a Service-Delegating Log Management to the Cloud”, 2013 IEEE.

[7] D.Esther Grace Vinitha, J.Shiny Duela,” A secure event log storage management system in cloud computing”, 2014 IEEE.

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

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

[10] Shams Zawoad, Amit Kumar Dutta, and Ragib Hasan,” Towards Building Forensics Enabled Cloud through Secure Logging-as-a-Service”, 2015 IEEE.

[11] Chung-Yi Lin, Ming-Che Chang, Hua-Chou Chiu, Keh-Hwa Shyu,” Secure logging Framework integrity with cloud database”,2015 IEEE.

[12] Tahir Sandıkkaya, Tolga Ovatman, Ali Emre Harmancı,” Design & formal verification of a cloud compliant secure logging mechanism”, The Institution of Engineering and Technology 2015.

[13] Krati Mehto, Rahul Moriwal,” A Secured and Searchable Encryption Algorithm for Cloud Storage”, 2015 International Journal of Computer Applications.

[14] Nguyen, Acharya, Ivanov, Haeberlen, T.X. Phan, Sokolsky, Jesse Walker, Weimer, Hanson, Lee,” Cloud-based secure logger for medical devices”,2016 IEEE.

[15] Haonan Su, Dong Zheng, Yinghui Zhang,” An Efficient and Secure Deduplication Scheme Based on Rabin Fingerprinting in Cloud Storage”, 2017 IEEE.

[16] Sekhar, Murali,” Access Control for Cloud Forensics through Secure Logging Services”, 2017 IEEE.

[17] M A Manazir Ahsan, Ainuddin Wahid Bin Abdul Wahab, Mohd Yamani Idna Bin Idris, Suleman Khan, Eric Bachura, Kim-Kwang Raymond Choo.” CLASS: Cloud Log Assuring Soundness and Secrecy Scheme for cloud forensics”, 2018 IEEE.

[18]https://www.uniprint.net/wpcontent/uploads/2017/05/Cloud-deployment-structures-diagram.png

[19] https://images.app.goo.gl/qbJ3b6x4WztWKUkq7

[20]https://azure.microsoft.com/en-in/overview/what-is-a-public-cloud/