International Journal of Science Engineering and Advance Technology

# Providing Cloud Data Security By Using Proof of Past Log

[1]B.Anila , [2]B.Maha Lakshmi Rao
[1,2]Department of Cse, Kakinada Institute of Engineering & Technology,
Korangi, East Godavari Dist.

**ABSTRACT:**

We propose the Cloud Log Assuring Soundness and Secrecy (CLASS) process as an elective plan for the verifying of logs in a cloud domain. In CLASS, logs are scrambled utilizing the individual client's open key so just the client can unscramble the substance. So as to anticipate unapproved alteration of the log, we create evidence of past log (PPL) utilizing Rabin's unique mark and Bloom channel. Such a methodology lessens check time fundamentally. Discoveries from our trials conveying CLASS in Open Stack exhibit the utility of CLASS in a genuine setting.

**KEYWORDS:** Networks, Protocols, Clustering

**INTRODUCTION:**

Because of the inborn idea of cloud advancements, traditional computerized measurable methods and instruments should be refreshed to hold a similar helpfulness and appropriateness in a cloud environment [14].Unlike an ordinary customer gadget, cloud virtual machines (VMs) can be upheld by equipment that may be found remotely and in this manner would not be physically open (for example out of the jurisdictional domain) to an examiner.

What's more, VMs can be conveyed over different physical gadgets in a bunched domain or they can exist inside a pool of VMs on the equivalent physical segments. In this manner, holding onto the machine for measurable examination isn't suitable in many examinations. Besides, information living in a VM might be unstable and could be lost once the power is off or the VM ends. Subsequently, the cloud specialist organization (CSP) assumes a significant job in the accumulation of evidential information (for example cloud client's action log from the log). For instance, the CSP composes the action log (cloud log) for every client. In this way, counteracting alteration of the logs, keeping up an appropriate chain of guardianship and guaranteeing information security is crucial[15].This research considers "action log information" as any recorded PC occasion that compares to a particular client. Such information must be kept up privately to preserver client protection and to encourage potential analytical exercises.

**LITERATURE SURVEY:**

**1] R. Curtmola, J. Garay**, we build another plan (KR-PEKS) the KResilient Public Key Encryption with Keyword Search. The new plan is secure under a picked watchword assault without the irregular prophet. The capacity of developing a Public Key Encryption with Keyword Search from an Identity Based Encryption was utilized in the development of the KR-PEKS. The security of the new plan was demonstrated by demonstrating that the utilized IBE has a thought of key protection.

**2]** K. Emura, A. Miyaji, M. S. Rahman we broaden the security of SCF-PEKS, calling it versatile SCF-PEKS, wherein an enemy (demonstrated as a "malevolent yet authentic" beneficiary) is permitted to issue test inquiries adaptively. We demonstrate that versatile SCF-PEKS can be conventionally built by unknown character based encryption as it were. That is, SCF-PEKS can be developed with no extra cryptographic crude when contrasted and the Abdalla et al. PEKS development (J. Cryptology 2008), despite the fact that versatile SCF-PEKS requires extra functionalities. We likewise propose other versatile SCF-PEKS development, which isn't completely nonexclusive yet is productive, contrasted and the first.

**PROBLEM DEFINITION:**

SecLaaS encodes the log(s) utilizing the examining organization's open key and stores the scrambled log(s) in a cloud server. This guarantees security and secrecy of the cloud client, except if the specific client is liable to an examination (for example by means of a court request). To encourage log respectability, SecLaaS creates verification of past

log (PPL) with the log chain and distributes it openly after each predefined age. A trust model was likewise recommended that stores the PPL in different mists to limit the danger of a vindictive cloud substance changing the log.

**PROPOSED APPROACH:**

We propose a protected cloud logging plan, Cloud Log Assuring Soundness and Secrecy (CLASS), intended to guarantee CSP responsibility (for example composing the right data to the log) and protect the client's security. In particular, we incorporate the ability for the client to check the precision of their log. To do this, the log will be encoded utilizing the client's open key (instead of the organization's open key).
To abstain from acquainting pointless postponements with the legal examination, during client enlistment with the cloud administration, both the CSP and the client will altogether pick an open/private key pair alluded to as substance disguising key (CC-key) for the client.

**SYSTEM ARCHITECTURE:**

Fig-1: Architecture of the system

**PROPOSED METHODOLOGY:**

**Preservation Of Log &Its Proof**
Parser gathers the log from log source. At the point when a log record changes (for example new lines affix) it triggers the parser to check the change and to begin preparing new log. Recovering log from log source, the parser parses the log and gets the important data. We will probably keep log substance secure given a parser that will give the framework a log message in string position, paying little heed to content. The configuration of the log is out of the extent of this work.

**Accumulator Design**
Blossom channel as a proof of past information ownership, which is neglects to represent Bloom channel's characteristic potential for false positives. When utilizing a Bloom channel method, there is an exchange off between the quantity of false positives and the size of the channel. To alleviate this issue, a cryptographic single direction gatherer could be used. Be that as it may, this requires noteworthy computational overhead. In SecLaaS, they utilized their own information structure Bloom Tree that decreased the quantity of false positive occurrences yet requires an expanded number of examples of logs and huge computational assets at confirmation time. This is genuine paying little heed to the quantity of passages being checked. What's more, despite everything it stays helpless against false positives (though diminished)

**Verification**
Just a confirmation procedure that sets up validness will most likely decide the nearness of log defilement. There are two sorts of checks in our methodology. First is confirmation where the client checks if the CSP is composing right log sections or not.

Second is confirmation by any gathering: client, agent, law requirement specialist (LEA) or official courtroom to confirm PPL to check for log change. In the two cases, the CSP can give a little utility check programming or the client/examiner can get it from individual programming merchant (ISV) to confirm.

**Secret Key Sharing**
We propose, in CLASS, to scramble the log with the client's private key (CC-key). In acknowledgment this may prompt lasting loss of log information (notwithstanding for analytical substances), as the private key of a client's CC-key is known uniquely to the client, we propose to share singular client's private key as indicated by Shamir's or Blackley's mystery key sharing methodology among numerous CSPs. This sharing plan requires institutionalization. We can manufacture sharing mists for such a reason when a client buys in to a cloud administration. The CSP and client together pick a couple of open/private key that is known as the substance.

**RESULTS:**

Fig-2: Number of log vs generation time

**CONCLUSION:**

we proposed a protected logging plan (CLASS) for distributed computing with highlights that encourage the conservation of client security and that alleviate the harming impacts of intrigue among different gatherings. CLASS safeguards the protection of cloud clients by scrambling cloud logs with an open key of the particular client while additionally encouraging log recovery in case of an examination. Also, it guarantees responsibility of the cloud server by enabling the client to distinguish any log adjustment. This has the extra impact of keeping a client from revoking sections in his very own log once the log has had its PPL set up.

**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,

[5]L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data incloud 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]L. Li, R. Lu, K.-K. R. Choo, A. Datta, and J. 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]K.-K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, pp. 77-78, 2016.

[9]C. Esposito, A. Castiglione, F. Pop, and K.-K. R. Choo, "Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective," IEEE Cloud Computing, vol. 4, pp. 13-17, 2017.

[10]Z. Qi, C. Xiang, R. Ma, J. Li, H. Guan, and D. S. Wei, "ForenVisor: A tool for acquiring and preserving reliable data in cloud live forensics," IEEE Transactions on Cloud Computing, vol. 5, pp. 443-456, 2017.

[11]C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, pp. 152-163, 2013.

[12]O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework," Journal of Network and Computer Applications, vol. 67, pp. 147-165, 2016.

[13]N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," IEEE Cloud Computing, vol. 3, pp. 50-59, 2016.

[14]B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud

computing," Digital Investigation, vol. 9, pp. 71-80, 2012.

[15]S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, et al., "Cloud log forensics: foundations, state of the art, and future directions," ACM Computing Surveys (CSUR), vol. 49, p. 7, 2016.

Ms. B. Anila is a student of Kakinada institute of Engineering &Technology korangi . presently she is pursuing her M. tech [Computer Science Engineering ] from this college and she received her B. Tech from Kakinada Institute of Engineering &Technology for Women in the year 2017.Her area of interest includes cloud computing and object oriented programming languages ,all current trends and techniques in computer science

Mr. B.Maha Lakshmi rao, well known Author and excellent teacher received M.Tech(CS) From Jawaharlal Nehru Technological University is working as Associate professor Department M. tech Computer Science Engineering ,Kakinada Institute of engineering & Technology . He has 8 years of teaching experience. To his credit couple of publications both national and international conferences .Hus area of interests includes cloud and hadoop technologies ,data mining and other advances in computer Applications