International Journal of Computer Science Engineering & Technology
IJCSET
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)- NEW DELHI INDIA .
ISSN :2455-9091

SURVEY: - THIRD PARTY AUDITING CLOUD COMPUTING SECURITY PROCESS

[1] MENAGA N
[1] Ph.D Resrearch Scholar
[1] Hindusthan College of Arts & Science ,
[1] Tamilnadu India.

ABSTRACT- The Cloud computing is a latest technology which provides various services through internet. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we survey to third party auditing cloud computing security process techniques.

Keywords: [Third Party Auditing, Security, Cloud Server & Computing.]

1. INTRODUCTION

Cloud computing is seeing quick developments in the ongoing years. It has two principle assignments putting away and getting to information and projects by methods for Internet instead of utilization of a PC's hard drive. The substance cloud introduces a broad scope of administrations. It lessens the intricacy of the systems, makes arrangement for customization, versatility, productivity and so on. Moreover, the data put away on cloud is by and large not effectively lost. As a result of its on-request nature, you could commonly purchase cloud computing a similar way you would purchase power, telephone utilities, or Internet access from a service organization. It is so natural with the cloud since one can include additional administrations (or take them away) immediately as the business needs change. As cloud innovation is winding up increasingly broad, the challenges((like spilling of touchy information, hacking, decoded information in danger associated with keeping up the innovation is additionally expanding. Cloud security, the arrangements, advancements, controls and so forth that are utilized to ensure the information, the different applications on the cloud and the related foundation, is turning into an essential field of research in the field of Network Security, and all the more extensively in Computer Security. The advancement of the Cloud Security strategies is similarly imperative to stay aware of the cloud issues. As a sort of rising business computational model, Cloud Computing disseminates calculation errand on the asset pool which comprises of a substantial number of PCs and as needs be the application frameworks gain the calculation working quality, the storage room and programming administration as indicated by its interest. The working of cloud computing can be seen by two unmistakable highlights One is the cloud foundation which is the building hinder for the upper layer cloud application. The other is the cloud application. Cloud computing has accomplished two vital objectives for the dispersed computing by the methods for three specialized strategies. High Scalability the cloud foundation can be extended to vast scale even to a huge number of servers and high Availability with the goal that the administrations are accessible notwithstanding when a significant number of servers come up short.

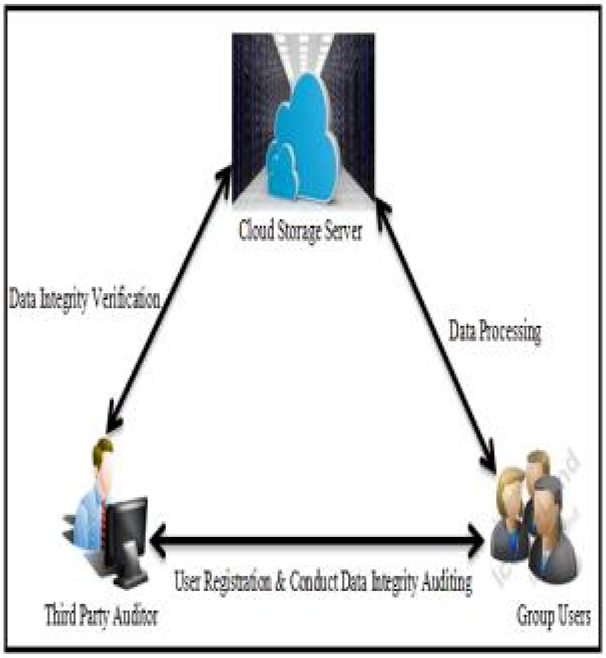
Cloud Storage Server
Data Integrity Verification
Data Processing
User Registration & Conduct Data Integrity Auditing
Third Party Auditor
Group Users

Figure 1: Third Party Auditing

To address these issues, our work uses the strategy of mystery key based symmetric key cryptography which empowers TPA to play out the auditing without requesting the neighborhood duplicate of client's put away information and in this way seriously derives the transmission and calculation overhead when contrasted with the clear information auditing approaches. Accordingly incorporating the encryption with hashing, our convention ensures that the TPA couldn't take in any learning about the information content put away in the cloud server amid the proficient auditing process. Cloud Computing, which gives Internet based administration and utilization of PC innovation. This is less expensive and more solid processors, together with the product as an administration (SaaS) computing engineering, are changing information into server farms on enormous scale. The expanding system and adaptable system associations influence it even conceivable that clients to would now be able to utilize astounding administrations from information and gives remote on server farms. Putting away information into the cloud offers incredible help to clients since they don't need to think about the issues of equipment issues. While these web based online administrations do give immense measures of storage room and adjustable computing assets, this computing stage move, be that as it may, is keeps away from the duty of nearby machines for information support in the meantime. Therefore, clients are at the enthusiasm of their cloud specialist co-ops for the accessibility and respectability of their information the one hand; in spite of the fact that the cloud administrations are considerably more intense and dependable than individualized computing gadgets and wide scope of both inner and outside dangers for information honesty still exist. Precedents of blackouts and information misfortune occurrences of important cloud stockpiling administrations show up every once in a while. Then again, since clients may not keep a neighborhood duplicate of outsourced information, there exist different motivating forces for cloud specialist organizations (CSP) to act unfaithfully towards the cloud clients with respect to the status of their outsourced information. Our work is among the initial couple of ones in this field to consider circulated information stockpiling security in Cloud Computing.

2. LITERATURE SURVEY

Wang et al., set up Static Index (SI) and Dynamic Index (DI) for Public-key Encryption with Keyword Search (PEKS) to make seek secure and proficient. SI and DI assist PEKS with decreasing the heap separately in two sections: If information clients are looking questioned watchword out of the blue, SI is utilized or something bad might happen, DI is utilized, SI and DI are simultaneously practical with PEKS and upgraded as Secure Hybrid Indexed Search (SHIS) plot that utilizations deterministic encryption (DE) and is merged. SHIS is enhanced further for numerous beneficiary applications yet this expansion, bolster just for one catchphrase accessible ciphertext.

Gu et al., proposed Public Key Encryption with Keyword Search (PEKS) plot utilizing cross sections. PEKS is a technique for looking on encoded information. It empowers the client to send a mystery esteem Tw to a server. It empowers the server to put all encoded messages containing the watchword, however without getting the hang of anything, yet with a probabilistic consistency. The plan is secure with the hardness of the standard Learning With Errors (LWE). The plan centers around security however not on calculation cost.

Ache et al., exhibited a general system for multiuser boisterous watchword based accessible symmetric encryption in a blame tolerant way. Existing endeavors on multi-client accessible symmetric encryption (SSE) have concentrated on correct catchphrase seek, yet these outcomes are not connected to the circumstance where the watchwords related with the records are loud information. A development which consolidates a solitary client boisterous catchphrase based SSE conspire with a private-key unique communicate encryption plot is outlined. This plan allows the information proprietor to proficiently and progressively repudiate the clients. It enables the approved clients to look through the scrambled report set utilizing their picked uproarious watchwords with the help from a legit yet inquisitive server. It is secure and effectively understands the objective of multi-client loud catchphrase look.

Lu et al., planned a novel cryptographic crude - extend predicate encryption - to construct a Logarithmic Search over Encrypted Data (LSED) framework. This plan is provably secure with respect to plain-content secrecy, predicate protection and backings logarithmic inquiry over scrambled information, question validation and secure information refresh. The LSED framework uncover the entrance examples of figure writings to the cloud server. Besides, all database refresh activity and question approval depends on the database proprietor which turns into a solitary purpose of disappointment.

Xia et al., proposed a plan for essential comparability look over encoded pictures in view of a safe change strategy that secured the data about highlights, and don't debase the outcome precision. The proposed plot ensure the secrecy of picture database, highlight vectors, and client's question. Also, the picture proprietor could refresh the encoded picture database and additionally the safe record effortlessly. This plan guarantee the classification of the information, result exactness and question unlinkability. The time multifaceted nature of question on upset record is O(n), which can be additionally upgraded by utilizing better file to decrease seek time.

Goh et al., have sketched out a protected file and surrounded a security worldview intended for files and is known as semantic security against versatile picked catchphrase assault (ind − cka). Secure records can be utilized for analyzing over encoded information just in multi-client gatherings, as the scrambled information documents and its files put away at the remote server are routinely advised. A proficient ind − cka secure file worldview called z − idx utilizing pseudo-arbitrary capacities and Bloom channels is produced. what's more, to execute seeks over encoded information that is put away on a remote server collected hashing plans, scrambled and accessible review logs, database that considers private inquiries utilizing a semi-confided in third party, and testing set enrollment safely are constructed. This inquiry worldview has high proficiency, with O(1) look time per document, and deals with packed information, variable length words, Boolean and certain standard articulation inquiries. z−idx lists penances get to design security for productivity.

Liu et al., have examined an effective protection saving watchword seek conspire in cloud computing. The cloud server supplier does not know any data about indicated watchwords and scrambled messages. It can ensure client information and client questioned watchword amid hunt process.The development depends on bilinear maps on elliptic bend to assemble a proficient Identity-Based Encryption (IBE) and security depends on Bilinear Diffe-Hellman(BDH) suspicion. The plan is semantically secure however the investigation isn't performed on the scrambled information.

Jiang et al., have introduced another way to deal with build productive Disjunctively Oblivious Keyword Search (DOKS) convention which allows quick hunt and short figure content. It gives solid security on clients side and cloud stockpiling suppliers. The calculation and storage room is less contrasted with past Oblivious Keyword Search (OKS) conventions. The security and effectiveness are better in DOKS convention. The client submits two pursuit catchphrases that are not discernable and require not know the connection between the figure content of the report and hunt watchwords. The coordinating reports recover without uncovering measurable data on the hunt inquiry however the plan does not bolster multi-watchword look.

Goldreich et al., have proposed unaware RAM that utilizations Square-root calculation and various leveled arrangement. RAMs enable customers to totally conceal the information get to designs from the cloud server supplier. It tends to be utilized related to encryption, to empower more grounded protection ensures. Be that as it may, using careless RAM as a rule brings exponential number of collaborations between the client and the server for each inquiry ask.

Tune et al., have portrayed distinctive viable methods for inquiry on scrambled information. The Crypto Systems are secure for encoded information and untrusted server can't take in anything about the plain content in light of the query items. Two methods viz, Hidden inquiries and question segregation are presented in this work. The shrouded inquiries looks word without uncovering the data to the server and question disengagement server adapts nothing aside from the query items. The calculations are basic, quick, without space and correspondence overhead. Consecutive sweep isn't proficient and is moderate for an extensive number of archives.

Wang et al., have proposed catchphrase look encryption system to determine the issue of encoded information through question restriction. The recommended technique consolidates the fine-grained get to control and watchword look encryption to make accessible access controls of a few clients in the cloud setting described by scrambled information security. The drawback of this plan is that as the quantity of access classes of the inquiry records expands, the quantity of question tokens raises. The worldview furnishes information stronghold with high secure quality.

CONCLUSION

Here in this paper we survey a system in which we have assessed diverse papers on auditing procedure where the bunch auditing and single record auditing is performed. We talked about the protection saving method and security approaches while working with the multi duplicate bunch auditing. In this paper we have talked about various security and auditing approach over the cloud and along these lines the most extreme protection safeguarding procedure to review the different duplicate check utilizing effective mark based plan is have to quit for the further work.

REFERENCES

[1] O. Goldreich and R. Ostrovsky, “Software Protection and Simulation on Oblivious RAMs,” in Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.

[2] C. H. Wang and C.-C. Hsu, “Integration of Hierarchical Access Control and Keyword Search Encryption in Cloud Computing Environment,” in International Journal of Computer and Communication Engineering, vol. 3, no. 2, pp. 333–337, 2013.

[3] Q. Liu, G. Wang, and J. Wu, “An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing,” in Proceedings of the International Conference on Computational Science and Engineering CSE’09, vol. 2, pp. 715–720, 2009.

[4] D. Boneh and M. Franklin, “Identity-based Encryption from the Weil Pairing,” in Proceedings of the Advances in Cryptology—CRYPTO 2001, pp. 213–229, 2001.

[5] Z. Jiang and L. Liu, “Secure Cloud Storage Service with an Efficient DOKS Protocol,” in Proceedings of the IEEE International Conference on Services Computing (SCC), pp. 208–215, 2013.

[6] S. KumarVerma, S. Mathew, S. Srivastava, and S. Venkataesan, “An Efficient Dictionary and Lingual Keyword based Secure Search Scheme in Cloud Storage,” in International Journal of Computer Applications, vol. 68, no. 15, pp. 40–43, 2013.

[7] Y. Lu, “Privacy-Preserving Logarithmic-Time Search on Encrypted Data in Cloud.” in 19th Annual Network and Distributed System Security Symposium, (NDSS), 2012.

[8] Z. Xia, Y. Zhu, X. Sun, and J. Wang, “A Similarity Search Scheme over Encrypted Cloud Images based on Secure Transformation,” International Journal of Future Generation Communication and Networking, vol. 6, no. 6, pp. 71–80, 2013.

[9] X. Pang, B. Yang, M. Zhang, and H. Wang, “Multi-user Noisy Keyword Search over Encrypted Data,” Journal of Computational Information Systems, vol. 9, no. 5, pp. 1973–1981, 2013.

[10] C. Gu, Y. Guang, Y. Zhu, and Y. Zheng, “Public Key Encryption with Keyword Search from Lattices,” in International Journal of Information Technology, vol. 19, no. 1, pp. 1–10, 2013.

[11] W. Wang, P. Xu, H. Li, and L. T. Yang, “Secure Hybrid- Indexed Search for High Efficiency over Keyword Searchable Ciphertexts,” Future Generation Computer Systems, 2014.

[12] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure Ranked Keyword Search over Encrypted Cloud Data,” in Proceedings of the IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 253–262, 2010.

[11] D. X. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searches on Encrypted Data,” IEEE Symposium on Security and Privacy, pp. 44–55, 2000.

[12] Tao Jiang Xiaofeng Chen and Jianfeng Ma, “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation” IEEE Transactions On Computers, Vol. 65, No. 8, August 2016 .

[13] PushkarZagade,“Group User Revocation and Integrity Auditing of Shared Data in Cloud Environment” International Journal of Computer Applications (0975 – 8887) Volume 128 – No.12, October 2015

[14] NishantSahani,“A Review on Cryptographic Hashing Algorithms for Message Authentication” International Journal of Computer Applications (0975 – 8887) Volume 120 – No.16, June 2015.

[15] S. Kamara and K. Lauter, "Cryptographic cloud storage, " in Financial Cryptography and Data Security, ed: Springer, 2010, pp. 136-149.

[16] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. 2013, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6.