World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:2, 2020

A Secure Auditing Framework for Load Balancing in Cloud Environment

R. Geetha, T. Padmavathy

***Abstract*—**Security audit is an important aspect or feature to be considered in cloud service customer. It is basically a certification process to audit the controls that deliver the security requirements. Security audits are conducted by trained and qualified staffs that belong to an independent auditing organization. Security audits must be carried as a standard of security controls. Proper check to be made that the cloud user has a proper reporting and logging facilities with the customer's system and hence ensuring appropriate business and operational flow of data through cloud service. We propose a cloud-based secure auditing framework, which enables confided in power to safely store their mystery information on the semi-believed cloud specialist co-ops, and specifically share their mystery information with a wide scope of information recipient, to diminish the key administration intricacy for power proprietors and information collectors. Unique in relation to past cloud-based information framework, data proprietors transfer their mystery information into cloud utilizing static and dynamic evaluating plan. Another propelled determination is, if any information beneficiary needs individual record to download, the information collector will send the solicitation to the expert. The specialist proprietor has the Access Control. At the off probability, the businessman must impart the primary record to the knowledge collector, acknowledge statistics beneficiary solicitation. Once the acknowledgement for the records is over, the recipient downloads the first record and this record shifting time with date and downloading time with date are monitored by the inspector. In addition to deduplication concept, diminished cloud memory area using dynamic document distribution has been proposed.

***Keywords*—**Cloud computing, cloud storage auditing, data integrity, key exposure.

I. Introduction

DISTRIBUTED computing forecasts noteworthy change by the way we store data and run applications. Rather than running projects and data [8], [10] on an individual work station, everything is facilitated in the "cloud"- An indistinct gathering of PCs and servers got to by means of the Internet. Distributed computing gives you a chance to get to every one of your applications and archives from anyplace on the planet, liberating you from the limits of the work area and making it simpler for gathering individuals in various areas to team up. Distributed computing has pulled in far reaching consideration and backing in numerous fields. In the distributed computing condition, numerous administrations, for example, asset leasing, application facilitating, and administration re-appropriating demonstrate the center idea of an on-request administration in the IT field. As of late, numerous IT investors are building up their business distributed computing framework, for example Amazon's EC2, Amazon's S3, Google App Engine and Microsoft's Azure and so on. Distributed computing can give adaptable processing capacities, lessen expenses and capital figuring abilities, diminish expenses and capital consumptions and charge as per use.

Despite the fact that the distributed computing worldview brings numerous advantages, there are numerous unavoidable security issues brought about by its innate qualities, for example, the dynamic intricacy of the distributed computing condition, the transparency of the cloud stage and the high grouping of resources [16]. One of the imperative issues is the way to guarantee the security of client information. Security issues, for example, information security and security protection [11] in distributed computing, have turned out to be not dismissive hindrances which, if not properly tended to, will keep the advancement and wide utilization of distributed computing later on. Security concern [7] in an appropriated record framework has been a noteworthy issue amid the most recent decades. There are numerous security worries in dispersed record frameworks. A portion of the worries are the manner by which to make a disseminated record classified and to control its entrance. Conventional client control components keep client experts in an Access Control List (ACL) in a gathering or a various leveled structure. At that point, it adds get to control credit to a document utilizing a confided in server for verification and approval. Nonetheless, these customary methodologies intensely rely upon security of the entrance control list. Once ACL were undermined, it would embroil the entrance control administration. When the process is over, the entrance control systems send symmetric key more often and open cryptographic plans to verify the entrance control list.

II. Related Work

Wang et al. [1] proposed an adaptable dispersed capacity honesty examining instrument, using the homomorphic token and circulated deletion coded information. The proposed plan enables clients to audit [9] the distributed storage with exceptionally lightweight correspondence and calculation cost. The inspecting result guarantees solid distributed storage accuracy ensure, yet in addition at the same time accomplishes quick information blunder confinement, i.e., the distinguishing proof of getting rowdy server. Considering that the cloud information is dynamic in nature, the scheme that is proposed is secure. It also takes care of effective unique tasks on re-

Dr.R.Geetha is with Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India (Corresponding author, e-mail: geetha@saec.ac.in).

T. Padmavathy is with Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India (e-mail: padmavathyt@saec.ac.in, lallithashri@saec.ac.in).

appropriated information, including square adjustment, erasure, and attach. Examination demonstrates that the proposed plan is exceptionally effective and strong against Byzantine disappointment, vindictive information adjustment assault, and much server conniving assaults.

Wang et al. [2] propose the primary protection safeguarding component that permits open examining on shared information put away in the cloud. Specifically, we abuse ring marks to figure the confirmation data expected to review the trustworthiness of shared information. With our component, the personality of the underwriter on each square in shared information is kept private from an outsider examiner (TPA), who is as yet ready to openly check the trustworthiness of shared information without recovering the whole record. Our exploratory outcomes show the adequacy and effectiveness of our proposed component while examining shared information.

A reasonable CA engineering has important component and procedures [3]. At last, we talk about advantages and difficulties that must be handled to diffuse the idea of persistent cloud administration evaluating. We add to information and practice by giving appropriate inside and outsider inspecting philosophies for examiners and suppliers, connected together in a theoretical design. Further on, we give groundings to future research to actualize CA in cloud administration settings.

Wang et al. [4] propose a safe distributed storage framework supporting protection saving open examining. We further stretch out our outcome to empower the TPA to perform reviews for numerous clients at the same time and effectively. Broad security and execution investigation demonstrate that the proposed plans are provably secure and exceedingly proficient. Our primer test led on Amazon EC2 example further shows the quick execution of the structure.

Wolke et al. [5] provide the results of an extensive experimental analysis of both capacity management approaches on a data center infrastructure. We show that with typical workloads of transactional business applications, dynamic resource allocation does not increase energy efficiency over the static allocation of VMs to servers and can even come at a cost, because migrations lead to overheads and service disruptions.

III. Resilient Scrutiny System (RSS)

We propose a cloud-based secure information framework, which enables confide in power to safely store their ambiguity information on the semi-believed cloud specialist co-ops. It specifically shares the ambiguity information with a wide scope of information recipient, to lessen the key administration multifaceted nature for power proprietors and information beneficiaries. Not the same as past cloud-based information framework, data proprietors transfer their mystery information into cloud utilizing static and dynamic evaluating plan. Another propelled determination is, if any information beneficiary needs individual document to download, the information collector will send the solicitation to the expert. The specialist proprietor has the Access Control. The owner has to divulge the main record to the knowledge collector and acknowledge the information to the recipient. Once the acknowledgement for the records is over the recipient downloads the primary record and this record shifting time with date and downloading time with date is monitored by the inspector. Then capsulated deduplication is done for decreasing cloud memory house. Also, documents are dispensed utilizing dynamic record portion. So we change our record area and erase undesirable documents from distributed storage list. At last the record area utilizing static and dynamic document portion is regulated. So documents are apportioned appropriately. Also, auditing is the procedure to keep an eye on the exercises occurring in the cloud framework. This is put as an extra layer in the virtual machine to screen the exercises on the framework that are identified with state change and different components that impact the accessibility of the asset. Another viewpoint to be considered is that numerous nations have their own characterized laws for distributed computing where the client information ought to be kept classified inside the national limit and this makes it important to have a review set up.

Security evaluation is a very important perspective to be considered in the cloud administration client side. It is fundamentally a confirmation procedure to review the controls that convey the security prerequisites. Security reviews are directed via prepared and qualified staffs that have a place with a free inspecting association. Security reviews must be conveyed as a standard of security controls.

Information deduplication is a particular information pressure procedure for disposing of copy duplicates of rehashing information away. The system is utilized to improve capacity use and can likewise be connected to arrange information transfers [6] to lessen the quantity of bytes that must be sent. Rather than keeping numerous information duplicates with a similar substance, deduplication disposes of repetitive information by keeping as it were. Deduplication can happen at either the document level or the square dimension. For record level deduplication, it disposes of copy duplicates of a similar document. Deduplication can likewise happen at the square dimension, which wipes out copy squares of information that happen in non-indistinguishable documents.

Static Allocation plans assign fixed property to the cloud client or application. For this situation, the cloud client should know the quantity of asset cases required for the application and what assets are mentioned and should expect to affirm the application's pinnacle load demands. However, the restriction for static allotment is typically influenced by the over-usage or under-use of figuring assets dependent on the ordinary outstanding task at hand of the application. This is not financially savvy and is identified with inadequate utilization of the asset amid off-crest periods.

Dynamic Allocation schemes give cloud assets on the fly when the cloud client or application is mentioned, explicitly to maintain a strategic distance from over-use and under-usage of assets. A conceivable disadvantage when required assets are mentioned on the fly is that they probably will not be open. In this manner, the administration provider must apportion assets

from various partaking cloud server farms. Asset allotment methodology is identified with consolidating cloud supplier capacities for using and doling out rare assets inside the limits of the cloud framework so as to suit the interest of the cloud application.

IV. Result and Discussion

The owner of the data can be able to login only if they are already registered with the audit. The owner can login and upload their data in a secured manner [14], [15]. The receiver should log on to the process to get the data from the sender of the process in a secured manner. The receiver can only be able to download the data when the sender accepts the receiver request. The auditor is the one who is able to audit the complete process by using the dynamic auditing scheme. The auditor is able to block and unblock both sender and the receiver of the file when not needed.

The time of auditing processes with different number of challenged Blocks is discussed in Fig. 1. In scheme [13], the secret keys are updated in different time periods. The exposure of key cannot affect the security of authenticators that are developed before the key exposure time period.

In proposed scheme, the secret keys are updated by the data owners into the cloud using static and dynamic auditing scheme.

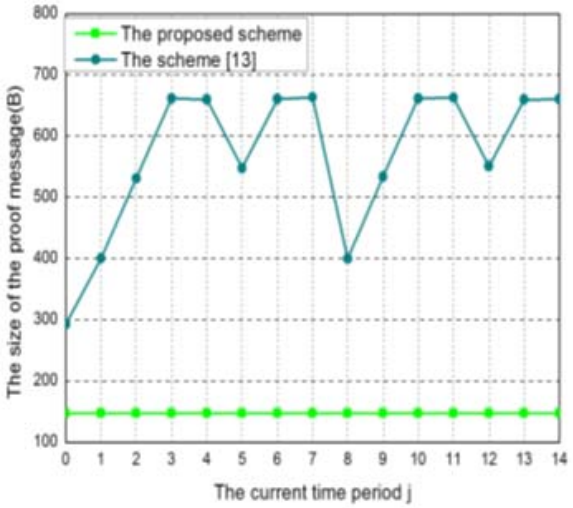

Fig. 1 Time of Auditing Process

Fig. 1 represents the current time and the size of the message that are uploaded by the proposed scheme [13]. The proof overhead with different number of challenged blocks is discussed in Fig 2.

The time taken by the auditing process is shown using the proof generation and the verification generation process in the cloud auditing scheme. The process of proof generation and verification generation can verify with change in the challenge generation process during each update of the key in the cloud storage.

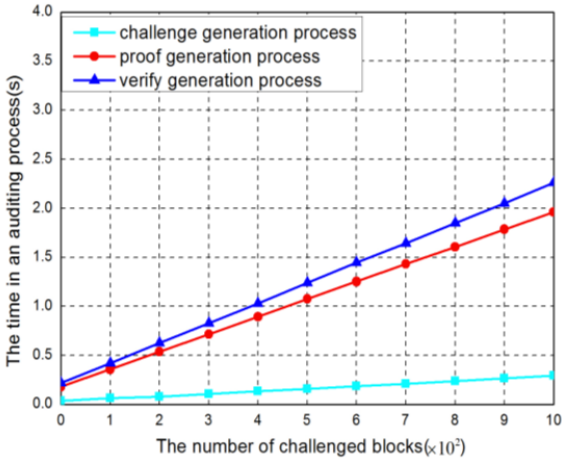

Fig. 2 Overhead of challenged blocks

V. Conclusion

A cloud based secure data system is proposed in this paper to enable secure data storage in semi-trusted cloud service providers. In this approach the data owners upload their data using static allocation scheme. The data owner can change their data location using dynamic data allocation scheme. When the data receiver wants to download the data, the request will be sent to the authority. In this case, the authority owner will have the Access Control. The data owner will share the secret data to the data receiver. First receiver request is received by data owner. Then receiver will be able to download the original data. In addition to the deduplication concept of this system, more focus on reducing memory space requirement has also been given.

References

[1] Cong Wang, Qian Wang, KuiRen, Ning Cao, and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, Volume: 5, Issue: 2, April-June 2012.

[2] Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 2, April-June 2013.

[3] Qingji Zheng, Shouhuai Xu, "Fair and Dynamic Proofs of Retrievability", Proceedings of the first ACM conference on Data and application security and privacy, CODASPY '11, pp 237-248, 2011.

[4] Zhengwei Ren, Lina Wang, Qian Wang, Rongwei Yu, and Ruyi Deng "Dynamic Proofs of Retrievability for Coded Cloud Storage Systems". Zero-knowledge Proofs of Retrievability, Science China: Information Sciences, vol. 54, no. 8, pp. 1608-1617, 2011.

[5] Alptekin Kupcu, "Official Arbitration with Secure Cloud Storage Application", The Computer Journal 58(4):831-852, 2013.

[6] Decio Luiz Gazzoni Filho, Paulo Sergio Licciardi Messeder Barreto, "Demonstrating data possession and uncheatable data transfer", IACR Cryptology eprint Archive, pp 150-150,2006.

[7] Ms. Ashwini Mandale, Prof. Shriniwas Gadage, "Cooperative Provable Data possession for integrity verification in multicloud", International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015.

[8] Zhuo Hao, Sheng Zhong, and Nenghai Yu "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", IEEE Transactions On Knowledge And Data Engineering, Vol. 23, No. 9, September 2011.

[9] Mehul A. Shah, Mary Baker, Jeffrey C. Mogul, Ram Swaminathan, "Auditing to Keep Online Storage Services Honest", Proceedings of the

11th USENIX workshop on Hot topics in operating systems, HOTOS'07, Article No. 11 2007.

[10] Francesc Sebe, Josep Domingo-Ferrer, Senior Member, Antoni Martınez-Balleste, Yves Deswarte, and Jean-Jacques Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures", IEEE Transactions On Knowledge And Data Engineering, Vol. 20, No. 8, August 2008.

[11] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 978-1-4244-5837-0/10/$26.00 ©2010 IEEE.

[12] Boyang Wang, Baochun Liand Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Transactions on Cloud Computing, Volume: 2, Issue: 1, Jan.-March 2014.

[13] Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, February 2013.

[14] Benoit Libert and Damien Vergnaud, "Adaptive-ID Secure Revocable Identity-Based Encryption", The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009.

[15] Jae Hong Seoand Keita Emura, "Revocable Identity-Based Encryption Revisited: Security Model and Construction", Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 – March 1, 2013.

[16] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, "Identity-based Encryption with Efficient Revocation", Proceedings of the 15th ACM conference on Computer and communications security ,pp 417-426,2008.

Dr. R .Geetha is the Professor in the Department of Computer Science and Engineering, S.A. Engineering College, Chennai, Tamilnadu, India. She is a Life member of ISTE, CSI and IAENG. Her areas of interest include Security in Wireless Sensor Networks, Mobile Ad-Hoc Networks and Cloud Computing. She has published papers in Springer and other reputed journals.

Ms. T. Padmavathy is the Assistant Professor in the Department of Computer Science and Engineering, S.A. Engineering College, Chennai, Tamilnadu, India. She is a Life member of ISTE and CSI .Her areas of interest include Security in Cloud Computing.