International Journal of Science Engineering and Advance Technology

Data integrity and Auditing for Secured Cloud Data Storage

D.UshaRaj[#1], CH.Udaya Bhaskar[*2]
[#]M. Tech. Student, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Peddapuram, East Godavari Dist., Andhra Pradesh, India
[1]usharazzd@gmail.com
[*] Associate Professor, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Peddapuram, East Godavari Dist., Andhra Pradesh, India
[2]cudayab@rediffmail.com

Abstract

Time and Trend has its own significance to build the technology smarter, better and easier to the end user.To the Better stretch of the Information Technology, the Innovation and renovation has changed computing approach to the next level. For this paper, we try giving the glimpse of the contextual virtual storage in cloud in the public data distribution. These days cloud storage become common, but having the constrainttowards the technical advancement is the Security. If we consider behavioral aspect of the cloud data storage, we will come across much aspect. Hence,In this we have overcome the public protection in terms of the privacy towards the authorization of public audit,tag based data uploading with the help of the SecCloud and SecCLoud+ based processing with the aim to maintain the integrity and data consistency. Metadata with the protocol to prevent the leakage of the dataset, which we call it as the best to the trend of the acknowledgement based identification with the cryptographic model where ever the node to the parallel cloud distributed elastic stretchableenvironment with the high end cloud data center marinating the graphics of the flow triggering the security in the public Domain.

Index Terms—Data storage, Deduplication, privacy preserving, public auditability, cloud computing, Data Integrity.

1. Introduction

Technology and its advancement lead us to research for the next level of the advancement. In the context of the Cloud computing which we can tell as the technological advancement plays the vital role in the industry of Information Technology. In the modern age of the cloud computing generation, the idea of regarding data confidentiality, all three providers claim that they provide and support encryption. Many cloud providers allow their customers data to encrypt before sending data to the cloud storage. The Standard evolution of science in computers and also along with the decline of hardware prices, the cloud computing usage instead of classic or traditional networks architecture has recently become a reality in the current situation. In order to optimize and increase the resources in the data centers or reasons for maintenance, cloud providers often have to migrate from the physical server to another server. In the CloudCover scalespractical limit to parallelization stemming from the fixedoverhead of the mappers and also the reducers.Once deployed on a Hadoop cluster consisting of 12Data Nodesand also of 4Name Nodes of which runs on the computer of commodity processor and other hardware component.

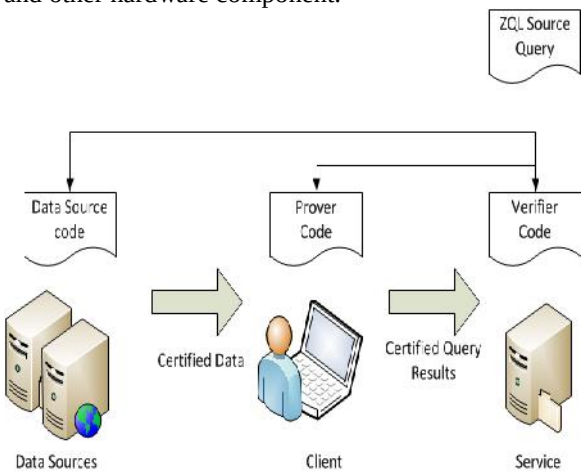

Fig.2.1. Data CentertoMonitor the Data Flow

As the Technology clustered mechanism, each software or the technology used needs to be installed in the data node making ready of the environment for the Hadoop based distributed scheduler or batch process, consists of the checkpoints in the Hadoop framework which uses the concept of the master slave communication in order to know which data node will be the next available channel for transferring files to minimize transfer cost and storage cost.

3. Methodology

Technology has its own significance at the time when people having the extension for the more and more research and it's from Abacus to today's' cloud Computing. In the context of revolution of technology and its great advantage to its social, behavioral and other technical aspect where we come across the best of the cloud to province the virtual global village as the global world. In the architectural view of the framework, which gives immense security to the vulnerability of the malicious attack are the only decrypt able access tokens or credentials that the name node or can call as the master node and other communications involving though the master node. If we consider the Tor browser master node or the node is the only un-trusted endpointand thus have a little smaller attack surface because they do not process cloud user submitted computations. In this methodology of that therefore assumes that the master node or manager is the trustworthy having p slave node or name node and furthermore, collide with the malicious master node or hub in an end goal tobreak the privacy. Here we have concurrent checkpoint equality correspondence checking procedure in our usage implementation in order to have the security at each level of the communication to the master node where stacks that can be partitioned arbitrarily into sub-stacks that can all be checked in similar for comparability equivalence.Here, as Hadoop based framework internally uses java based technological language implementation, we have come across the concept of the object inside the checkpoints, amap can divert them to another map by submitting new job works in Hadoop.

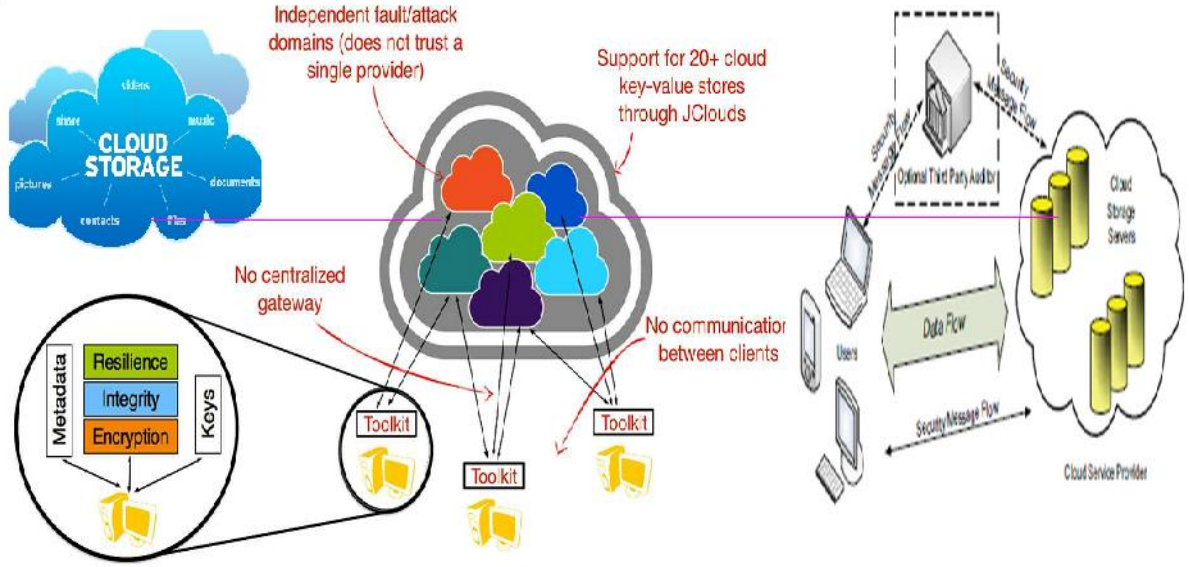

Fig.3.1. Architecture Design of the Secured Public Data in the Network

Hence, using this naval approach not only the security additionallyprivacy concerns of cloud consumers can be tended to all the more adequately and effectively, but also the burden of overseeing end-clients identities and fine-granular access control will be diminished from administration servicecloud providers. As the Two states are equivalent, which consists of the cryptographically verifiable compositionswhose corresponding slots contain equivalent values and objectswith confidentialfields to which the continuation object needs access to offers ascend access to the typical trivial solution withconfidentialfields to which continuation of the objects lacks its access. Hence, the encoding mechanisms which give the object module comparison the map and reduce give the equivalence concept which reducestheintrudervulnerability and other subcomponent level in the master node.

3.1 Evaluation and Analysis

In the phase of the analysis the devices which have adopted the technologies rely on software obfuscation. In the high peak traffic the communications overhead conceivably invites denial-of-service attacks by customers who request irrationally long circuits, where master node can manage the anonymous hits managing the encrypted ownership data they are received amidthe authentication.

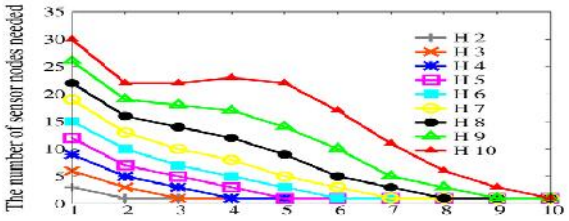

Fig.3.1.1. Node with the Peak Value

In the fig.3.1.1. the sensor node will get recommendation of the protocol mechanism needed on the traffic or connection which dynamically increase the load balance in to other to avoid the anonymous user , gives the mandatory upper limit for controlling the congestion.

4. Conclusion and Future work

Cloud computing is an emerging perspectivein which its cost-effectiveness and also the edibility have given it anenormous momentum. In this paper, we try to put forward the concept of the cloud in the aspect of the privacy preserving towards the public shared node data. It may lead to the extent of the cloud with the variant of the most suitable technological advancement of the recent solution. In the Public shared cloud computing where the data passed through the network which needs to be robust, secure and highly preserved in the sense no can replicate the data while reaching to the next node of the cloud server. Hence, we can make the sense of the cloud for the further research oriented making the global world as the data can be secured in the cloud architectural designs model of the Data center.However, there are numerous security challengesand that is not, tended to well, and may hindrance its quick adoption and development. This dissertation mainly addresses the issue of sharing, overseeing, and keeping up alongside controlling accessto the sensitive resources and also the services in an integrated cloud environment. The primary and essential conclusion of this research is that reception or adoption of user-centric security models and moving certain parts of correspondence communication and calculation to the client side allows us to furnish the cloud consumers with more visibility and control over their assets or the resources.

ACKNOWLEDGMENT

I would like to express my gratitude to my Guide Mr. CH.Udaya Bhaskar, M. Tech.,(Ph.D), Associate Professor, without his guidance, this paper is not possible. His understanding, encouragement and personal guidance have provided the basis for this paper.

Reference

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf.Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, andM. Zaharia, "A View of Cloud Computing," Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the PublicCloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protectionfor the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing EncryptedCloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for ObtainingDigital Signatures and Public Key Cryptosystems," Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978.

[8] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession atUntrusted Stores," Proc. 14th ACM Conf. Computer and Comm.Security (CCS '07), pp. 598-610, 2007.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and InformationSecurity: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[11] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computerand Comm. Security (CCS'09), pp. 213-222, 2009.

[12] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling PublicVerifiability and Data Dynamic for Storage Security in CloudComputing," Proc. 14th European Conf. Research in Computer Security(ESORICS'09), pp. 355-370, 2009.

[13] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data StorageSecurity in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS'09), pp. 1-9, 2009.

[14] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote DataChecking for Network Coding-Based Distributed Storage Systems,"Proc. ACM Workshop

Cloud Computing Security Workshop(CCSW'10), pp. 31-42, 2010.
[15] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S Yau,"Dynamic Audit Services for Integrity Verification of OutsourcedStorages in Clouds," Proc. ACM Symp. Applied Computing(SAC'11), pp. 1550-1557, 2011.
[16] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-BasedSecure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM,2012.
[17] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing forData Integrity in the Cloud," Proc. IEEE Conf. Comm. and NetworkSecurity (CNS'13), pp. 276-284, 2013.
[18] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

AUTHORS PROFILE

D. UshaRaj received the B. Tech. Degree in Computer Science and Engineering from Bapatla Engineering College permanently affiliated to A.N.U. Guntur, Andhra Pradesh, India. Presently working for M. Tech. Degree in Computer Science and Engineering at Aditya Engineering College, affiliated to J.N.T.U. Kakinada, Andhra Pradesh, India.

Ch.Udaya Bhaskarreceived the B.Tech degree in Computer science and Engineering from G.I.E.T Engineering College, Rajahmundry in 2002. He completed M.Tech in Computer Science and Engineering from Aditya Engineering College, Kakinada in 2012. He is having nearly 12 years of teaching experience. He is currently working as Associate Professor in the Dept of C.S.E., Aditya Engineering College, Kakinada, Andhra Pradesh, India. His research interests include Information security, Security challenges in Clouds. He is a life member of ISTE. He has published research papers in various National conferences, and International Journals.