IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

Securing Cloud Application using SHA-256 Hash Algorithm and Antiforgery Token

Ms. A. S.Athira[1], B. Veera Maheswara Reddy[2], M. V. Mohan Krishna Sai[3], N. Madhukar SreeSai[4]
Assistant Professor, Department of Computer Science & Engineering[1]
Students, Department of Computer Science & Engineering[2,3,4]
Dhanalakshmi College of Engineering, Chennai, India

Abstract: *The cloud supplier has no proposals for cloud data and information that is put away anyplace in the cloud and served around the world. Encryption technology generally serves as the foundation for privacy protection strategies. There are numerous ways of safeguarding security by keeping information from being moved to the cloud. A cloud-based three-tier storage structure is what we propose. The proposed structure is secure and able to make full use of cloud storage. The Hash-Solomon code, which is intended to divide the data into various parts, is utilized in this algorithm. We have lost data-related information in the event that just one piece of data is missing. In this design, we use calculations in light of the idea of containers and information assurance, and afterward can show the security and adequacy of our plan. Additionally, this algorithm is capable of calculating the cloud, cloud, and local computer distribution ratios, respectively, in terms of computational intelligence. SaaS (software as a service): A customer provides a hosted application that can be accessed by a variety of clients over a network. utilized by users With the possible exception of a few user configuration settings, the underlying cloud infrastructure is not managed or controlled by the customer. Examples of SaaS include Microsoft Office 365 and Google Apps.*

Keywords: Cloud Computing, Computational intelligence, Hash-Solomon

REFERENCES

[1]. P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.
[2]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.
[3]. J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.
[4]. H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.
[5]. Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv.Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.
[6]. L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.
[7]. R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.
[8]. J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.
[9]. R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts., vol. 13, no. 1, pp. 68–96, First Quarter 2011.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

[10]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.