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 7, May 2023

Privacy Preservation and Data Leakage Detection in Cloud Computing

Dr. B.S Borkar[1], Ms. Neha Pawar[2], Ms. Rohini Nagare[3], Mr. Mayur Gosavi[4], Mr. Mahesh Gophane[5]
Professor, Department of IT, Amrutvahini College of Engineering, College, Maharashtra, India[1]
Student, Department of IT, Amrutvahini College of Engineering, College, Maharashtra, India[2,3,4,5]

Abstract: *With vast growing internet as giant, data through these nets needs to be private and secured. Cloud Servers act as major resource to store data. Thus, Cloud server need to be secured and cannot be exposed to the possibility of being misused for disclosure or theft by hackers. For this they need strategic schemes to ensure the security and privacy check of the data. The system proposed utilizes three schemes to ensure security of data. The schemes are encryption of data, distributing of data over multiple clouds and giving authenticity to share data through secret key only. First, system is designed for sharing of data through secure channel of encryption wherein Lightweight algorithm is used for encryption of data, then data is distributed over different clusters with help of DROP algorithm and data is replicated over clouds to contain any loss. Third only private key can give access to different segments of data to explicit people who need to know the information. Trapdoor is generated to detect any unethical request to share data, request is blocked and identity of the person is pursued for any data leakage.*

Keywords: Energy Efficient Algorithm; Manets; Total Transmission Energy; Maximum Number of Hops; Network Lifetime.

REFERENCES

[1] Y. Kao, K. Huang, H. Gu and S. Yuan, "UCloud: A user-centric key management scheme for cloud data protection", IET Inf. Secur., vol. 7, no. 2, pp. 144-154, Jun. 2013.
[2] A. Al-Haj, G. Abandah and N. Hussein, "Crypto-based algorithms for secured medical image transmission", IET Inf. Secur., vol. 9, no. 6, pp. 365-373, Nov. 2015.
[3] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, et al., "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing", Future Generat. Comput. Syst., vol. 52, pp. 95-108, Nov. 2015.
[4] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.
[5] H. Liu, X. Li, M. Xu, R. Mo and J. Ma, "A fair data access control towards rational users in cloud storage", Inf. Sci., vol. 418, pp. 258-271, Dec. 2017.
[6] Z. Liu, Z. L. Jiang, X. Wang and S. M. Yiu, "Practical attribute-based encryption: Outsourcing decryption attribute revocation and policy updating", J. Network. Computer. Appl., vol. 108, pp. 112-123, Apr. 2018.
[7] R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Trans. Cloud Computer., vol. 6, no. 2, pp. 344-357, Apr. 2018.
[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, et al., "An efficient attribute-based encryption scheme with policy update and file update in cloud computing", IEEE Trans. Ind. Information., vol. 15, no. 12, pp. 6500-6509, Dec. 2019