IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

# Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-Owner Setting

**Vishal Shejwal**
Student, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

**Abstract:** *Cipher text-Policy Attribute-Based Keyword Search (CP-ABKS) offers fine-grained access management over encrypted knowledge in the cloud while facilitating search queries. The shared multi-owner setting (where every record is commissioned by a set variety of information owners) prevents the use of prior CPABKS schemes because they were created to serve single multi-owner settings and do not allow for the acquisition of high process and storage costs. Additionally, most current systems are vulnerable to off-line keyword-guessing assaults if the keyword house is polynomial in size because of privacy concerns with access controls. Furthermore, since each knowledge user has a similar set of characteristics, it can be difficult to identify rogue users who leak the key codes. In this research, we provide the basic ABKS-SM system, a privacy-preserving CP-ABKS system with hidden access policy, and show how it may be enhanced to facilitate malicious user tracing (modified ABKS-SM system). Then, within the general additive cluster model, we demonstrate that the proposed ABKS-SM systems deliver selective security and thwart off-line keyword-guessing attacks. Additionally, we evaluate their performance using real-world datasets.*

**Keywords:** User, Shared Multi-Owner Setting, Hidden Access Policy, Cypher Text-Policy Attribute-Based Encryption Time Server, Ranking and Tracing.

## REFERENCES

**[1].** J. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-Preserving Multi-Channel Communication in Edge-of-Things ," Accepted Manuscript, S0167-739X(18)30003-7 DOI: https://doi.org/10.1016/j.future.2018.03.043, 2018.

**[2].** JA. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach," Contents lists available at Science Direct Future Generation Computer Systems, 2014

**[3].** Ming Li, Shucheng Yu, Yao Zheng, Kui Ren," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption",IEEE Transactions On Parallel And Distributed Systems Vol:24 No:1 Year 2013.

**[4].** A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham-shirb and, , "Incremental proxy reencryption scheme for mobile cloud computing environment ," © Springer Science Business Media New York 2013.

**[5].** A. Abbas and S. U. Khan , "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds ,"IEEE computer server, weal so indisputable the usefulness of these systems. One drawback of the anticipated ABKS-SM systems is that as the variety of system features expands, so do the costs of procedures and storage. As a result, we plan to increase the ABKS-SM systems' effectiveness in the future. Additionally, we will focus on Journal of Biomedical and Health Informatics ,vol. PP, no. 99, pp. 1–1, 2013.

**[6].** D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP 2000), 2000, pp. 44– 55.

**[7].** D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Internationalconference on the theory and applications of cryptographic techniques (EUROCRYPT 2004), 2004, pp. 506– 522.

**[8].** H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multikeywordsearchsupporting classifiedsubdictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325,2016.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

**[9].** R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "Dual-server public-key encryption with keyword search for secure cloud storage," IEEE transactions on information forensics and security, vol. 11, no. 4, pp. 789–798, 2016.

**[10].** J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in dynamiccredential generation scheme for protection of user identity in mobilecloud computing,"TheJournalof Supercomputing, pp. 1-20, 2013.

**[11].** N. Fernando, S. W. Loke, and W. Rahayu, "Mobile Cloud Computing:A Survey," Future Generation Computer Systems, vol. 29, pp. 84– 106,January 2013.

**[12].** K. Kumar and Y. H. Lu, "Cloud Computing For Mobile Users: CanOffloading Computation Save Energy?," IEEE Journal Computer, vol.43, pp. 51-56, April 2010.

**[13].** E. Lagerspetz and S. Tarkoma, "Mobile Search and the Cloud: TheBenefits of Offloading," IEEE International Conference on PervasiveComputing and Communications Workshops (PERCOM Workshops),pp. 117–122,March 2011.[9] Q. Zhang, L. Cheng, and R.Boutaba, "Cloud computing: state-of-the-art and research challenges," Proc. IEEE Symposium on Security and Privacy (SP [19]D. Slamanig and C. Stingl, "Privacy aspects of 2007), 2007, pp. 321–334.

**[14].** A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A.Madani,"TowardsSecureMobileCloud Computing: A Survey, Future GenerationComputer Systems, vol. 29, pp. 12781299, July 2013.

**[15].** M. Armbrust et al., "Above the Clouds: A Berkeley View of CloudComputing", Technical e-Health," 3rd IEEE international Conference on Availability, Reliability and Security, (ARES '08), March 2008, pp.1226-1233.

**[16].** "Federal Health IT Initiatives," http://www.hhs.gov , accessed December 24, 2012.

**[17].** "CanadaHealth Infoway," http://www.infoway-inforoute.ca, accessed December 24, 2012. Report UCB/EECS-2009-28,EECS Department,University of California, Berkeley, Feb. 2009.

**[18].** Pay-as-You-GowithCloudComputing,http://technology.inc.com/2008/05/01/p ay-as-you-go-with-cloud-computing/, access data: 05 October, 2012.

**[19].** S. Das, D. Agrawal, and A. E. Abbadi, "ElasTraS: An ElasticTransactional Data Store in the Cloud," proc. of the 2009 conference onHot topics in cloud (USENIX '09), June 2009. [15] A. N. Khan, M. M. Kiah, S. A. Madani, and M. Ali, "Enhanced

**[20].** J. Dzenowagis and G. Kernen, "Connecting for health: Global vision, local insight," World Health Organization Press, Report for the World Summit on the Information Society, 2005, pp. 1-36

**[21].** H. J. Cheong, N. Y. Shin, and Y. B. Joeng, "Improving Korean service delivery system in health care: focusing on national e-health system," inIEEE International conference on e-Health, Telemedicine and Social Medicine (TELEMED '09), February 2009, pp. 263–268.

**[22].** L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell, "DACAR platform for e-Health services cloud," in 4th IEEE International Conference on Cloud Computing, July 2011, pp. 219-226.

**[23].** P. G. Goldschmidt, "HIT and MIS:Implications of health information technology and medical information system," Communication of the ACM, Vol. 48, No. 10, October 2005, pp. 69–74.