IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 9, June 2022

Decryptable Attribute-Based Keyword Search on E-Health Cloud

Krishna Sham P[1], Sushant Rao J[2], Nisarga B S[3], Harshit Ganesh H R[4], Umme Hani[5]
Students, Department of Information Science and Engineering[1,2,3,4]
Assistant Professor, Department of Information Science and Engineering[5]
Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

Abstract: *Cloud computing provides lot of benefits to enterprises to offload their data and software services to cloud saving them lot of money that has to be spent on infrastructure setup cost. Enterprises wanted to offload their data to cloud and save on their infrastructure cost. But when offloading the data security and privacy is a important concern. In this work, we focus on the search on encrypted data and provide a effective solution for the search. Searchable symmetric encryption (SSE) allows retrieval of the encrypted data over cloud. We formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that serve-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a secure-channel free ciphertext-policy decryptable attribute-based keyword search (CP-DABKS) scheme on eHealth cloud in the Internet of Things (IoT) platform. Additionally in CP-DABKS, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext.*

Keywords: Medical, eHealth, Attribute-based Keyword search, Cloud computing

REFERENCES

[1]. Ning Cao; Cong Wang; Ming Li; Kui Ren; Wenjing Lou, “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data”, IEEE Transactions on Parallel and Distributed Systems (Volume: 25, Issue: 1, Jan. 2014).

[2]. Jiadi Yu; Peng Lu; Yanmin Zhu; Guangtao Xue; Minglu Li, “Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data”, IEEE Transactions on Dependable and Secure Computing (Volume: 10, Issue: 4, July-Aug. 2013).

[3]. AnuradhaMeharwad, G.A.Patil, “Efficient Keyword Search over Encrypted Cloud Data”, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.

[4]. Ziq ing Guo, Hua Zhang, Caijun Su,n Qiaoyan Wen, Wenmin Li, “Secure multi-keyword ranked search over encrypted cloud data for multiple data owners”, Journal of Systems and Software Volume 137, March 2018, Pages 380-395.

[5]. Larry A. Dunning; Ray Kresman, “Privacy Preserving Data Sharing With Anonymous ID Assignment”, IEEE Transactions on Information Forensics and Security (Volume: 8, Issue: 2, Feb. 2013).

[6]. Jian Wang; Yan Zhao; Shuo Jiang; Jiajin Le , “Providing Privacy Preserving in Cloud Computing”, 3rd International Conference on Human System Interaction, IEEE, 2010.

[7]. Yan-Cheng Chang, Michael Mitzenmacher, “Privacy Preserving Keyword Searches on Remote Encrypted Data”, International Conference on Applied Cryptography and Network Security, Springer, 2015.

[8]. Jin Li , Qian Wang, Cong Wang , Ning Cao , Kui Ren , and Wenjing Lou, “Enabling Efficient Fuzzy Keyword Search over Encrypted Data in Cloud Computing”.

DOI: 10.48175/IJARSCT-5327