IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

Compound Keyword Level Search to conserve Privacy in access of Encrypted Cloud

Dr. P. Karuppasamy[1], Dr. G. Karthikeyan[2] and Mr. R. Sankarganesh[3]
Professor, Department of Electronics and Communication Engineering[1]
P. S. R Engineering College, Sivakasi, India

Abstract: *With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multikeyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure.*

Keywords: Compound Keyword Level.

REFERENCES

[1]. Ning Cao, Member, IEEE, Cong Wang, Member, IEEE, Ming Li, Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Privacy- Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 1, JANUARY2014.

[2]. M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control in the Storage as a Service Model," Proc. IEEE Int'l Conf. Information Reuse and Integration (IRI), 2012.

[3]. E. Bertino and E. Ferrari, "Secure and Selective Dissemination of XML Documents," ACM Trans. Information and System Security, vol. 5, no. 3, pp. 290-321, 2002.

[4]. G. Miklau and D. Suciu, "Controlling Access to Published Data Using Cryptography," Proc. 29th Int'l Conf. Very Large Data Bases (VLDB '03), pp. 898-909,2003.

[5]. N. Shang, M. Nabeel, F. Paci, and E. Bertino, "APrivacy- Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10),2010.

[6]. M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham, "Towards Privacy Preserving Access Control in the Cloud," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom '11), pp. 172-180,2011.

[7]. M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602- 2614, Nov. 2013.

[8]. S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 123-134, 2007.