IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, September 2022
Impact Factor: 6.252

Privacy in Searchable Symmetric Encrypted Cloud Data using Ranked Search

Nutan Pramod Chaudhari[1], Dr. Dinesh D. Patil[2], Prof. Rahul P. Chaudhari[3]
Department of Computer Science and Engineering[1]
Head of Department, Department of Computer Science and Engineering[2]
Associate Professor, Department of Computer Science and Engineering[3]
Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, Maharashtra, India

Abstract: *The appearance of cloud computing, data owners are motivatedfor great flexibility and economic savings to outsource their complex data management systems from local sites to commercial public cloud. For protecting data privacy, to ensure adequate 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. To achieve more competence, ranked searchable symmetric encryption is a cryptography scheme which gives an efficient design by properly utilizing the existing cryptographic primitive it is known as order-preserving symmetric encryption (OPSE). The proposed solution enjoys "as-strong-as possible" security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search.*

Keywords: Ranked Search, Encrypted Cloud, Privacy Preserving Data, Order-Preserving Symmetric Encryption

REFERENCES

[1]. H. Dai, Y. Ji, L. Liu, G. Yang and X. Yi, "A privacy-preserving multi-keyword ranked search over encrypted data in hybrid clouds", Proc. 5th Int. Conf. Artif. Intell. Secur. (ICAIS), pp. 68-80, 2019.

[2]. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" IEEE TRANSACTION ON PARELLEL AND DISTRIBUTED SYSTEMS,VOL.25,NO 1,JANUARY2014.

[3]. Secure Access of Encrypted Cloud Data Based on Top-K Multikeywords with User Side RankingIJERTCONV3IS19214, Volume & Issue : ICESMART – 2015 (Volume 3 – Issue 19)

[4]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg Chengwei Liu, Yixiang Chan, Syed HasnainAlamKazmi, Hao Fu, "Financial Fraud Detection Model: Based on Random Forest," International Journal of Economics and Finance, Vol. 7, Issue. 7, pp. 178-188, 2015.

[5]. S. Grzonkowski, P. M. Corcoran and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services", Proc. IEEE Int. Conf. Consum. Electron., pp. 83-87, Sep. 2011.

[6]. N. Cao, M. Li and W. J. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data", Proc. IEEE INFOCOM, pp. 829-839, Apr. 2011.

[7]. N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy–preserving multi–keyword ranked search over encrypted cloud data", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222-233, Jan. 2014.

[8]. J. Xu, W. Zhang, C. Yang, J. Xu and N. Yu, "Two-step-ranking secure multi–keyword search over encrypted cloud data", Proc. Int. Conf. Cloud Service Comput., pp. 124-130, Nov. 2012.

[9]. C. Yang, W. Zhang, J. Xu, J. Xu and N. Yu, "A fast privacy–preserving multi-keyword search scheme on cloud data", Proc. Int. Conf. Cloud Service Comput., pp. 22-24, Nov. 2012.

[10]. H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou and X. S. Shen, "Enabling fine–grained multi–keyword search supporting classified sub–dictionaries over encrypted cloud data", IEEE Trans. Dependable Secure Comput., vol. 13, no. 3, pp. 312-325, May 2016.

[11]. Z. Xia, X. Wang, X. Sun and Q. Wang, "A secure and dynamic multi–keyword ranked search scheme over encrypted cloud data", IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, Feb. 2016.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, September 2022
Impact Factor: 6.252

[12]. Z. Xiangyang, D. Hua, Y. Xun, Y. Geng and L. Xiao, "MUSE: An efficient and accurate verifiable privacy-preserving multikeyword text search over encrypted cloud data", Secur. Commun. Netw., vol. 2017, Nov. 2017.

[13]. M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in Proc. of CRYPTO, 2007

[14]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, 2009

[15]. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, 2006.