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 2, May 2023

Fast Keyword Search over Encrypted Data with Ciphertext in Cloud

Mr.Abdual Khadar A[1], Swaroop N Swamy[2], Vasuki M[3], Srinidhi B V[4], Jayanth[5]
Assistant Professor, Department of Information Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
SJC Institute of Technology Chickballapur, India

Abstract: *At present times , it's accessible for people to store their data on clouds. To secure the privacy, people tend to encode their data before uploading them to clouds. Due to the wide use of cloud services, public key searchable encryption is necessary for users to search the encrypted files efficiently and rightly. still, the being public key searchable encryption schemes supporting monotonic queries suffer from either infeasibility in keyword testing or inefficiency similar as heavy computing cost of testing, large size of ciphertext or lattice, and so on. In this work, we first propose a novel and effective anonymous key- policy attribute- based encryption(KP- ABE). also by applying Shen etal.'s general construction to the proposed anonymous KP- ABE, we capture an effective and suggestive public key searchable encryption, which to the best of our knowledge achieves the best performance in testing among the existing similar schemes.*

Keywords: Search.

REFERENCES

[1]. J. Aikat, A. Akella, J. S. Chase, A. Juels, M. K. Reiter, T. Ristenpart, V. Sekar, M. Swift, Rethinking security in the era of cloud computing, IEEE Security Privacy 15 (3) (2017) 60–69. doi:10.1109/MSP.2017.80.

[2]. N. Chen, J. Li, Y. Zhang, Y. Guo, Efficient cp-abe scheme with shared decryption in cloud storage, IEEE Transactions on Computers 71 (1) (2022) 175–184. doi:10.1109/TC.2020.3043950.

[3]. J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, D. Wang, Attribute based encryption with privacy protection and accountability for cloudiot, IEEE Transactions on Cloud Computing (2020) 1–1doi:10.1109/TCC. 2020.2975184.

[4]. . Li, X. Lin, Y. Zhang, J. Han, Ksf-oabe: Outsourced attribute-based encryption with keyword search function for cloud storage, IEEE Transactions on Services Computing 10 (5) (2017) 715–725. doi:10.1109/TSC. 2016.2542813.

[5]. D. X. Song, D. Wagner, A. Perrig, Practical techniques for searches on encrypted data, in: Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, 2000, pp. 44–55.

[6]. D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: Advances in Cryptology - EUROCRYPT 2004, 2004, pp. 506–522.

[7]. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Searchable symmet ric encryption: Improved definitions and efficient constructions, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, ACM, New York, NY, USA, 2006, pp. 79–88. doi:10.1145/1180405.1180417. URL http://doi.acm.org/10.1145/1180405.1180417

[8]. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi, Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions, in: Advances in Cryptology – CRYPTO 2005, 2005, pp. 205–222.

[9]. D. Boneh, B. Waters, Conjunctive, subset, and range queries on encrypted data, in: Theory of Cryptography, Springer Berlin Heidelberg, 2007, pp. 535–554.

[10]. J. Katz, A. Sahai, B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in: Advances in Cryptology – EUROCRYPT 2008, 2008, pp. 146–162.

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 2, May 2023

[11]. C.-I. Fan, V. S.-M. Huang, H.-M. Ruan, Arbitrary-state attribute-based encryption with dynamic membership, IEEE Transactions on Computers 63 (8) (2014) 1951–1961. doi:10.1109/TC.2013.83.

[12]. S.-Y. Huang, C.-I. Fan, Y.-F. Tseng, Enabled/disabled predicate encryption in clouds, Future Generation Computer Systems 62 (2016) 148–160. doi:https://doi.org/10.1016/j.future.2015.12.008. URL https://www.sciencedirect.com/science/article/pii/ S0167739X15003921

[13]. J. Lai, X. Zhou, R. Deng, X. Li, K. Chen, Expressive search on encrypted data, in: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013, pp. 243–252.

[14]. A. Guillevic, Comparing the pairing efficiency over composite-order and prime-order elliptic curves, in: Applied Cryptography and Network Security, 2013, pp. 357–372.

[15]. M. H. Ameri, M. Delavar, J. Mohajeri, M. Salmasizadeh, A key-policy attribute-based temporary keyword search scheme for secure cloud storage, IEEE Transactions on Cloud Computing (2018) 1–1.

[16]. Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, J. Zhang, Attribute-based keyword search over hierarchical data in cloud computing, IEEE Transactions on Services Computing (2018) 1–1.

[17]. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, Lightweight fine-grained search over encrypted data in fog computing, IEEE Transactions on Services Computing (2018) 1–1.

[18]. H. Wang, X. Dong, Z. Cao, Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search, IEEE Transactions on Services Computing (2018) 1–1.

[19]. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, in: Advances in Cryptology – EUROCRYPT 2010, 2010, pp. 62–91.

[20]. H. Fei, Q. Jing, Z. Huawei, H. Jiankun, A general transformation from KP-ABE to searchable encryption, in: Cyberspace Safety and Security, Springer Berlin Heidelberg, 2012, pp. 165–178.