Yang, Yang; **Liu, Ximeng**; **Deng, Robert**

Expressive query over outsourced encrypted data. (English) Zbl 1440.68066

Inf. Sci. 442-443, 33-53 (2018).

Summary: Data security and privacy concerns in cloud storage services compel data owners to encrypt their sensitive data before outsourcing. Standard encryption systems, however, hinder users from issuing search queries on encrypted data. Though various systems for search over encrypted data have been proposed in the literature, existing systems use different encrypted index structures to conduct search on different search query patterns and hence are not compatible with each other. In this paper, we propose a query over encrypted data system which supports expressive search query patterns, such as single/conjunctive keyword query, range query, Boolean query and mixed Boolean query, all using a single encrypted index structure. To the best of our knowledge, the proposed system enables the most expressive query pattern search among all the existing solutions. In addition, the system allows data users to simultaneously query over encrypted documents from multiple data owners using one query trapdoor and supports flexible user authorization and revocation. We show that our system is secure and resists keyword guessing attack. We also conduct extensive experiments and demonstrate that the system is more efficient than other public key searchable encryption systems.

MSC:

68P20 Information storage and retrieval of data
68P25 Data encryption (aspects in computer science)
68P27 Privacy of data

Keywords:

query over encrypted data; range search; Boolean search; subset search; multiple users

Full Text: DOI

References:

[1] Barker, E.; Barker, W.; Burr, W.; Polk, W.; Smid, M., NIST special publication 800-57, NIST Special Publication, 800, 57, 1-142 (2007)

[2] Bloom, B. H., Space/time trade-offs in hash coding with allowable errors, Commun. ACM, 13, 7, 422-426 (1970) · Zbl 0195.47003

[3] Boneh, D.; Di Crescenzo, G.; Ostrovsky, R., Public key encryption with keyword search, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, 506-522 (2004), Springer Berlin Heidelberg · Zbl 1122.68424

[4] Boneh, D.; Waters, B., Conjunctive, subset, and range queries on encrypted data, Proceedings of the Theory of Cryptography Conference, 535-554 (2007), Springer Berlin Heidelberg · Zbl 1156.94335

[5] Bresson, E.; Catalano, D.; Pointcheval, D., A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security., 37-54 (2003), Springer Berlin Heidelberg · Zbl 1205.94075

[6] Byun, J. W.; Rhee, H. S.; Park, H. A., Off-line keyword guessing attacks on recent keyword search schemes over encrypted data, Proceedings of the Workshop on Secure Data Management., 75-83 (2006), Springer Berlin Heidelberg

[7] Cash, D.; Jarecki, S.; Jutla, C., Highly-scalable searchable symmetric encryption with support for boolean queries, Advances in Cryptology- CRYPTO 2013, 353-373 (2013), Springer Berlin Heidelberg · Zbl 1311.68057

[8] Chen, R.; Mu, Y.; Yang, G.; Guo, F.; Wang, X., Dual-server public-key encryption with keyword search for secure cloud storage, IEEE Trans. Inf. Forensics Secur., 11, 4, 789-798 (2016)

[9] Do, Q.; Martini, B.; Choo, K. K.R., A forensically sound adversary model for mobile devices, PloS One, 10, 9, e0138449 (2015)

[10] Hore, B.; Mehrotra, S.; Canim, M., Secure multidimensional range queries over outsourced data, VLDB J. Int. J. Very Larg. Data Bases, 21, 3, 333-358 (2012)

[11] Hwang, M. S.; Hsu, S. T.; Lee, C. C., A new public key encryption with conjunctive field keyword search scheme, Inf. Technol. Control,, 43, 3, 277-288 (2014)

[12] Kamara, S.; Mohassel, P.; Raykova, M., Outsourcing multi-party computation, IACR Cryptol., 2011, 272 (2011)

[13] Li, H.; Yang, Y.; Luan, T. H., Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data, IEEE Trans. Dependable Secur. Comput., 13, 3, 312-325 (2016)

[14] Liu, Q.; Wang, G.; Wu, J., Secure and privacy preserving keyword searching for cloud storage services, J. Netw. Comput. Appl., 35, 3, 927-933 (2012)

[15] Liu, X.; Qin, B.; Deng, R., An efficient privacy-preserving outsourced computation over public data, IEEE Trans. Serv. Comput. (2015), Publish Online

[16] Liu, X.; Lu, R.; Ma, J., Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification, IEEE J. Biomed. Health Inf., 20, 2, 655-668 (2016)

[17] Liu, X.; Deng, R. H.; Choo, K. K.R., An efficient privacy-preserving outsourced calculation toolkit with multiple keys, IEEE Trans. Inf. Forensics Secur., 11, 11, 2401-2414 (2016)

[18] Liu, X.; Deng, R. H.; Ding, W., Privacy-preserving outsourced calculation on floating point numbers, IEEE Trans. Inf. Forensics Secur., 11, 11, 2513-2527 (2016)

[19] Liu, X.; Choo, R.; Deng, R., Efficient and privacy-preserving outsourced calculation of rational numbers, IEEE Trans. Dependable Secur. Comput. (2016), Publish Online

[20] Moataz, T.; Shikfa, A., Boolean symmetric searchable encryption, Proceedings of the Eighth ACM SIGSAC Symposium on Information, Computer and Communications Security., 265-276 (2013), ACM

[21] Ohtaki, Y., Partial disclosure of searchable encrypted data with support for boolean queries, Proceedings of the International Conference on Availability, Reliability and Security, 1083-1090 (2008), IEEE

[22] Peter, A.; Tews, E.; Katzenbeisser, S., Efficiently outsourcing multiparty computation under multiple keys, IEEE Trans. Inf. Forensics Secur., 8, 12, 2046-2058 (2013)

[23] Paillier, P., Public-key cryptosystems based on composite degree residuosity classes, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, 223-238 (1999), Springer Berlin Heidelberg · Zbl 0933.94027

[24] Shi, E.; Bethencourt, J.; Chan, T. H.H., Multi-dimensional range query over encrypted data, Proceedings of the IEEE Symposium on Security and Privacy, 350-364 (2007), IEEE

[25] Wang, B.; Hou, Y.; Li, M., Maple: scalable multi-dimensional range search over encrypted cloud data with tree-based index, Proceedings of the Ninth ACM Symposium on Information, Computer and Communications Security., 111-122 (2014), ACM

[26] Wang, B.; Fan, X., Search ranges efficiently and compatibly as keywords over encrypted data, IEEE Trans. Dependable Secur. Comput. (2016), Publish Online

[27] Wen, M.; Lu, R.; Zhang, K., PaRQ: a privacy-preserving range query scheme over encrypted metering data for smart grid, IEEE Trans. Emerg. Top. Comput., 1, 1, 178-191 (2013)

[28] Yang, Y.; Zheng, X.; Tang, C., Lightweight distributed secure data management system for health internet of things, J. Netw. Comput. Appl. (2016), Publish Online

[29] Yang, Y.; Ma, M., Semantic searchable encryption scheme based on lattice in quantum-era, J. Inf. Sci. Eng., 32, 2, 425-438 (2016)

[30] Yang, Y.; Ma, M., Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds, IEEE Trans. Inf. Forensics Secur., 11, 4, 746-759 (2016)

[31] Yau, W. C.; Heng, S. H.; Goi, B. M., Off-line keyword guessing attacks on recent public key encryption with keyword search schemes, Proceedings of the International Conference on Autonomic and Trusted Computing., 100-105 (2008), Springer Berlin Heidelberg

[32] Zheng, Q.; Xu, S.; Ateniese, G., VABKS: verifiable attribute-based keyword search over outsourced encrypted data, Proceedings of the INFOCOM, 522-530 (2014), IEEE