Emekci, Fatih; **Methwally, Ahmed**; **Agrawal, Divyakant**; **El Abbadi, Amr**
Dividing secrets to secure data outsourcing. (English) Zbl 1328.68050
Inf. Sci. 263, 198-210 (2014).

Summary: Data outsourcing or database as a service is a new paradigm for data management. The third party service provider hosts databases as a service. These parties provide efficient and cheap data management by obviating the need to purchase expensive hardware and software, deal with software upgrades and hire professionals for administrative and maintenance tasks. However, due to recent governmental legislations, competition among companies and database thefts, companies cannot use database service providers directly. They need secure and privacy preserving data management techniques to be able to use them in practice. Since data is remotely stored in a privacy preserving manner, there are efficiency related problems such as poor query response time. We propose a new framework that provides efficient and scalable query response times by reducing the computation and communication costs. Furthermore, the proposed technique uses several service providers to guarantee the availability of the services while detecting the dishonest or faulty service providers without introducing additional overhead on the query response time. The evaluations demonstrate that our data outsourcing framework is scalable and practical.

MSC:

68P15 Database theory
68P25 Data encryption (aspects in computer science)

Keywords:

data outsourcing; query processing; data privacy and security

Full Text: DOI

References:

[1] Advances in cryptology - crypto 2007, in: A. Menezes, (Ed.), 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings, CRYPTO, Volume 4622 of Lecture Notes in Computer Science, Springer, 2007.

[2] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, N. Mishra, R. Motwani, U. Srivastava, D. Thomas, J. Widom, Y. Xu, Enabling privacy for the paranoids, in: Proc. of the 30th Int'l Conference on Very Large Databases VLDB, August 2004, pp. 708-719.

[3] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, Y. Xu, Two can keep a secret: a distributed architecture for secure database services, in: CIDR, 2005, pp. 186-199.

[4] G. Aggarwal, N. Mishra, B. Pinkas, Privacy-preserving computation of the k'th-ranked element, in: Proc. of IACR Eurocrypt, 2004, pp. 40-55. · Zbl 1122.68422

[5] R. Agrawal, A. Evfimievski, R. Srikant, Information sharing across private databases, in: Proc. of the 2003 ACM SIGMOD International Conference on Management of Data, 2003, pp. 86-97.

[6] Agrawal, R.; Haas, P. J.; Kiernan, J., A system for watermarking relational databases, (Proc. of the 2003 A CM SIGMOD International Conference on Management of Data, (2003), ACM Press), 674-674

[7] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, Hippocratic databases, in: 28th Int'l Conf. on Very Large Databases (VLDB), Hong Kong, August 2002.

[8] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, Implementing p3p using database technology, in: Proc. of the 19th Int'l Conference on Data Engineering, Bangalore, India, March 2003.

[9] Agrawal, R.; Kiernan, J.; Srikant, R.; Xu, Y., Order preserving encryption for numeric data, (SIGMOD '04: Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, (2004), ACM Press New York, NY, USA), 563-574

[10] Agrawal, R.; Srikant, R., Privacy-preserving data mining, (Proc. of the 2000 ACM SIGMOD International Conference on Management of Data, (2000), ACM Press), 439-450

[11] S. Agrawal, J.R. Haritsa, A framework for high-accuracy privacy-preserving mining, in: ICDE, 2005, pp. 193-204.

[12] E. Bertino, B.C. Ooi, Y. Yang, R.H. Deng, Privacy and ownership preserving of outsourced medical data, in: ICDE, 2005.

[13] Cachin, C.; Micali, S.; Stadler, M., Computationally private information retrieval with polylogarithmic communication, Lecture Notes in Computer Science, 1592, 402-414, (1999) · Zbl 0932.68042

[14] Chor, B.; Gilboa, N., Computationally private information retrieval (extended abstract), (Proc. of the Twenty-Ninth Annual

ACM Symposium on Theory of Computing, (1997), ACM Press), 304-313 · Zbl 0962.68054

[15] Clifton, C.; Kantarcioglu, M.; Vaidya, J.; Lin, X.; Zhu, M. Y., Tools for privacy preserving distributed data mining, SIGKDD Exploration Newsletter, 4, 2, 28-34, (2002)

[16] F. Emekci, D. Agrawal, A.E. Abbadi, Abacus: A distributed middleware for privacy preserving data sharing across private data warehouses, in: ACM/IFIP/USENIX 6th International Middleware Conference, 2005.

[17] F. Emekci, D. Agrawal, A.E. Abbadi, A. Gulbeden, Privacy preserving query processing using third parties, in: ICDE, 2006.

[18] Evfimievski, A.; Srikant, R.; Agrawal, R.; Gehrke, J., Privacy preserving mining of association rules, (Proc. of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, (2002), ACM Press), 217-228

[19] Ganapathy, V.; Thomas, D.; Feder, T.; Garcia-Molina, H.; Motwani, R., Distributing data for secure database services, Transactions on Data Privacy, 5, 1, 253-272, (2012)

[20] H. Hacigumus, B.R. Iyer, C. Li, S. Mehrotra, Executing SQL over encrypted data in the database service provider model, in: SIGMOD Conference, 2002.

[21] B. Hore, S. Mehrotra, G. Tsudik, A privacy-preserving index for range queries, in: Proc. of the 30th Int'l Conference on Very Large Databases VLDB, 2004, pp. 720-731.

[22] B. Hore, S. Mehrotra, G. Tsudik, A privacy-preserving index for range queries, in: VLDB, 2004, pp. 720-731.

[23] S. Kamara, K. Lauter, Cryptographic cloud storage, in: Financial Cryptography Workshops, 2010, pp. 136-149.

[24] M. Li, S. Yu, N. Cao, W. Lou, Authorized private keyword search over encrypted data in cloud computing, in: ICDCS, 2011, pp. 383-392.

[25] Lindell, Y.; Pinkas, B., Privacy preserving data mining, (Proc. of the 20th Annual International Cryptology Conference on Advances in Cryptology, (2000), Springer-Verlag), 36-54 · Zbl 0989.68506

[26] Miyamoto, T.; Doi, S.; Nogawa, H.; Kumagai, S., Autonomous distributed secret sharing storage system, Systems and Computers in Japan, 37, 6, 55-63, (2006)

[27] Parakh, A.; Kak, S., Recursive secret sharing for distributed storage and information hiding, CoRR, abs/1001.3331, (2010)

[28] S. Rizvi, J.R. Haritsa, Maintaining data privacy in association rule mining, in: Proc. of the 28th Int'l Conference on Very Large Databases, August 2002, pp. 682-693.

[29] Shamir, A., How to share a secret, Communications of the ACM, 22, 11, 612-613, (1979) · Zbl 0414.94021