

Searching in encrypted data

Jeroen Doumen
doumen@cs.utwente.nl
University of Twente, Enschede

Abstract

With more and more data being stored on (untrusted) external servers, concerns about this data falling into the wrong hands grows. Thus this database needs to be secured, typically by encrypting it. However, this means that a client will have to retrieve the entire database before being able to do anything useful, such as asking a query. Thus a need arises for a way to avoid this drawback and to be able to perform queries (mainly) on the server.

Song, Wagner and Perrig described a mechanism for this in [1]. However, their method is unpractical for large databases, since each query requires the server to search through the entire database linearly. In [2] we extended their mechanism to XML documents, achieving a much higher query efficiency by avoiding this.

Using Shamir's secret sharing scheme to design a new system [3], enabled us to keep a high query efficiency, as well as be able to handle more complex queries (e.g. AND and OR expressions).

References

- [1] Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *IEEE Symposium on Security and Privacy*, pages 44–55, 2000. <http://citeseer.nj.nec.com/song00practical.html>.
- [2] R. Brinkman, L. Feng, J.M. Doumen, P.H. Hartel, and W. Jonker. Efficient tree search in encrypted data. In E. Fernández-Medina, J. C. Hernández Castro, and L. J. Garcia Villalba, editors, *WOSIS 2004 - Second International Workshop on Security in Information Systems*, pages 126–135, Porto, Portugal, April 2004. Institute for Systems and Technologies of Information, Control and Communication (INSTICC) Press, Portugal. <http://www.ub.utwente.nl/webdocs/ctit/1/000000f3.pdf>.
- [3] R. Brinkman, J.M. Doumen, P. Hartel, and W. Jonker. Using secret sharing for searching in encrypted data. In *Proc. of the Secure Data Management workshop*, Toronto, Canada, August 2004.