Abstract

Critical business data in databases is an attractive target for attack. Therefore, ensuring the confidentiality, privacy and integrity of data is a major issue for the security of database systems. High secure data in databases is protected by encryption. When the data is encrypted, query performance decreases. In our paper we propose a new mechanism to query the encrypted data beside make a tradeoff between the performance and the security. Our mechanism will work over many data-types. We implement our work as a layer above the DBMS; this makes our method compatible with any DBMS. Our method based on replacing the select conditions on the encrypted data with another condition which is faster. The new way must have no security weak that is can’t show an aspect for the plain data. The results of the experiments validate our approach.

References

- Erez Shmueli, Ronen Vaisenberg, Yuval Elovici and Chanan Glezer, “Database Encryption – An Overview of Contemporary Challenges and Design Considerations”; SIGMOD Record, September 2009 (Vol. 38, No. 3)
- H. Hacigumus, Bala Iyer and Sharad Mehrotra, "Providing Database as a Service", Data Engineering, 2002. Proceedings. 18th International Conference
- Yu Han, Zhao Liang Niu Xiamu, "Research on a new method for database encryption and cipher index"; Acta Electronica Sinica, No. 12A 2005
- Wikipedia, the free encyclopedia that anyone can edit http://en.wikipedia.org/wiki/Hash_table, an article on Hash table
- Bertino, E.; Sandhu, R., "Database security – concepts, approaches and challenges"; IEEE Transactions on Dependable and Secure Computing, VOL. 2, NO. 1, JANUARY-MARCH 2005
- Michael Mitzenmacher, "Compressed Bloom Filters"; IEEE/ACM Transactions on Networking, VOL. 10, NO. 5, October 2002
- Yong Zhang, Wei-xin Li and Xia-Mu Niu, "A Secure Cipher Index Over Encrypted
- Lianzhong Liu and Jingfen Gai, “Bloom Filter Based Index for Query over Encrypted Character Strings in Database”, 2009 World Congress on Computer Science and Information Engineering
- Yu Chen and Wesley W. Chu, Fellow, “Protection of Database Security via Collaborative Inference Detection”, IEEE Transactions on Knowledge and Data Engineering, VOL. 20, NO. 8, August 2008
- http://www.cecs.csulb.edu/~monge/classes/share/B+TreeIndexes.html.

**Index Terms**

- Computer Science
- Security

**Keywords**

- Encryption
- Hash Map
- Querying Over Encrypted Data
- Index