Abstract

Online applications are vulnerable to theft of sensitive information because adversaries can exploit software bugs to gain access to private data and because curious or malicious administrators may capture and leak data. DBCrypto provides practical and provable confidentiality to the database by using queries. The proposed system is a middleware between user application and DBMS. The encrypted data is stored in tables by preserving its format and decrypted data can accessible to the user through regular queries. The various encryption and decryption algorithms are implemented at Query Level to secure the data from malicious administrator or from information leak.

References

- Korth Henry F., Silberschatz Avi, Sudarshan S., Database System Concepts 5th
DBCrypto: A Database Encryption System using Query Level Approach

- Stallings William Cryptography and Network Security
- Popa Raluca, Catherine M. S., Zeldovich Nickolai, Balakrishnan Hari 2011. CryptDB: A practical encrypted relational DBMS.
- Marten van Dijk, Gentry Craig, Halevi Shai, VaikuntanathanVinod December 11, 2009 Fully Homomorphic Encryption over the Integers
- Zheli Liu, ChunfuJia, Jingwei Li, Xiaochun Cheng 2010 Format-Preserving Encryption For Date Time IEEE International Conference on Intelligent computing and intelligent Systems(ICIS) Pages 201-205
- Bellare Mihir, Ristenpart Thomas, Rogaway Phillip, Stegers Till. Format-Preserving Encryption Dept. of Computer Science & Engineering, UC San Diego, La Jolla, CA 92093, USA Dept. of Computer Science, UC Davis, Davis, CA 95616, USA 2009
- Mattsson Ulf T. Format-Controlling Encryption using Data type-Preserving Encryption. 2009 IACR Cryptography e-Print Archive
- MySQL Reference Manual 5. 5

Index Terms

Computer Science Data Security
Keywords
Database  Security  Data Security