047

A Structure Preserving Database Encryption Scheme Data Security

Data security is becoming one of the most important issues of the new information driven applications. It is now essential to secure "Data in Motion" - the data while it moves across the network and securing the data at the edge points ("Data in Rest"). Even it is reasonable to think that the problem is with "Data in Motion" - Most attacks are targeted at “Data at Rest” and by intruders with in the organization (like DBA or data owner/client with in the organization)

Goals and Benefits

- Data encryption at table, row and cell level.
- Each cell is encrypted with its unique cell coordinates but only the data of interest needs to be decrypted while performing a query.
- Substitution and statistical attacks are eliminated.
- Each index value is the result of encrypting a plaintext value in the database with its row-id. This ensures that the index does not reveal the statistics or order of the database values and the new database indexing scheme preserves the index structure.
- The new schemes do not impose any changes on the database structure.

Potential Commercial Uses and Strategic Partners

This technology will provide a much better security for all databases based application mainly for "Data in Rest" needs and helps to protect in house as well as external intruders.
Potential Strategic partners are – Oracle, Microsoft, IBM and others.

Development Stage and Development Status Summary

The Preserving Database Encryption Scheme was successfully tested on Oracle 9i database and shows a much better security for both "Data in Rest" and "Data in Motion" needs. The next steps in the development is Implementing the new schemes on other Databases (such as Microsoft MS-SQL and others), perform additional Performance assessment and Key management and expanding the technology to Bi-temporal databases.

Researcher

Prof. Y. Elovici, Dep. of Information Systems Engineering, Ben-Gurion University, Beer-Sheva, Israel; Erez Shmueli, Dep. of Computer Sciences, Ben-Gurion University, Beer-Sheva, Israel.

Patent Status

Patent Pending

Contact for Licensing and Investment Information

Zafrir Levy, VP Business Development, e-mail: zafrirl@bgu.ac.il