BRILLIX

Data Sheet

Sensitive Data Detection and Masking

Physical Data Masking

Sensitive Data Protection

Data Leakage Prevention

Data Privacy

Sensitive Data Mapping and Schema Detection
(for both production and non-production environments)

Physical Data Masking and Automatic Alerting for Non-Production Database Environments
(test, dev, QA, training, integration, etc.)

Regulations and Compliance: EU General Data Protection Regulation (GDPR), PCI-DSS

BRILLIX Ltd.

www.Brillix.com
info@brillix.com
+972 50 404 5058

About JumbleDB

JumbleDB is a simple, robust and intuitive sensitive data detection, classification and masking solution. It delivers ***fast*** and ***smart*** auto sensitive data detection engine based on out-of-the-box templates, with multiple heterogeneous cross-database platforms support.

JumbleDB provides ***real*** and ***meaningful*** alternative data while maintaining business integrity, keeping your data in its original structure, assuring the continuity of your business applications.

JumbleDB is your ***end-to-end*** comprehensive ***one-stop-shop*** solution for all your sensitive data detection and masking needs.

Physical Data Masking

Data Masking, also referred as Data Anonymization and Pseudonymization*, is the technique of completely scrambling and obfuscating the data while reducing the linkability of a data set with the original identity of a data subject. This is done usually in order to reduce the risk of accidental or intentional data disclosure by making the information un-identifiable to an individual or entity.

Data Masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.

Data Masking is often used to de-identify personal data and prevent exposing personal data in less protected environments such as test and development. Although most organizations have stringent security controls in place to protect production data in storage or in business use, sometimes that same data has been used for operations that are less secured. The issue is often compounded if these operations are outsourced and the organization has less control over the environment. In the wake of compliance legislation, most organizations are no longer comfortable exposing real data unnecessarily.

In data masking, the format of data remains the same; only the values are changed. The data may be altered in a number of ways, including encryption, character shuffling and character or word substitution. Whichever method is chosen, the values must be changed in some way that makes detection or reverse engineering impossible.

*__Pseudonymization__ is a process by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

Sensitive data

ID	Name	Credit Card
12345678-9	Kobi Peretz	4580-1111-2222-3333
98765432-1	Dudu Aharon	5326-1003-1234-2222
45678932-5	Eyal Golan	4580-9999-4444-5555

Masked data: Shuffle

ID	Name	Credit Card
98765432-1	Kobi Peretz	4580-1111-2222-3333
45678932-5	Dudu Aharon	5326-1003-4444-55555
12345678-9	Eyal Golan	4580-9999-6666-7777

Masked data: Changed values

ID	Name	Credit Card
98765432-1	Kobi Peretz	4580-1111-2233-4455
45678932-5	Dudu Aharon	5326-1003-4455-6677
12345678-9	Eyal Golan	4580-9999-6677-8899

Figure 1 – Physical data-masking: before and after (2 samples)

Innovative Approach to Physical Data Masking

JumbleDB simple, robust and intuitive sensitive data detection and masking solution was developed to enable organizations conduct an efficient and short data masking project. This unique solution allows information security experts, along with database and infrastructure personnel, to conduct a successful data scrambling project in the fastest and most efficient manner, while meeting various regulations and compliances including **PCI**, **GDPR** and others.

JumbleDB is based on a unique, 3-tier approach: ***Detect → Protect → Alert***

This unique approach enables ongoing scrambling of sensitive data and continuous maintenance of scrambled data in non-production environments.

Step One: Detect

The first step is to detect sensitive data in the database. Using the sensitive data detection tool you can:

- Detect and identify sensitive data using an intelligent search engine, with a comprehensive predefined and extensible library of sensitive data templates
- Detect and identify where sensitive data resides in your database, according to the content, data structure and column names
- Detect relations in the database: database defined relations (foreign keys) as well as relations defined by various applications

Step Two: Protect

The second step is the data masking and scrambling:

- Various scrambling algorithms which are all designed fine-tuned to handle extremely large volumes of data.
- Comprehensive and extensible library of anonymization and masking formats, functions, transformations, and various templates
- Easily mask and scramble personal data and any other types of sensitive data such as credit card numbers, national identifiers, and other personally identifiable information (PII) with an extensive out-of-the-box library of masking and scrambling formats
- Add user-defined methods for scrambling and masking your own sensitive data
- Masking algorithms provide real meaningful data, while maintaining business integrity.

Step Three: Alert

The third step is to prevent sensitive data leakage:

- Ensure, that even after a scrambling project has been completed successfully, no sensitive data will be imported and inserted in an uncontrolled manner
- Prevent sensitive data leakage and automatically alert regarding data and structural changes
- Users will automatically get notified whenever sensitive data is added to an already masked database environment

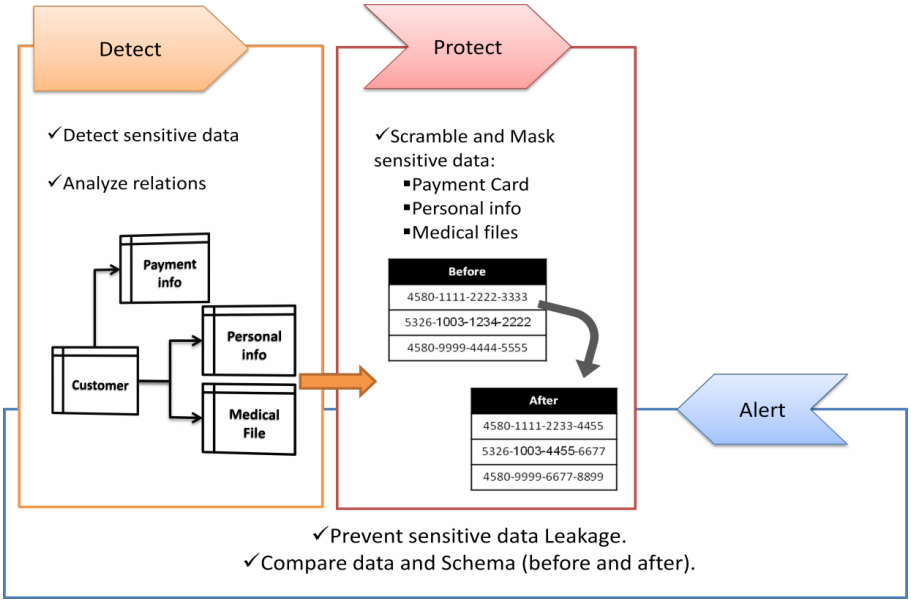

Figure 2 – Innovative approach to physical data masking project

JumbleDB main features include:

- Rich out-of-the-box sensitive data classification dictionary
- Predefined and extensible custom sensitive data masking algorithms
- Automatically detect and analyze sensitive data relations
- Maintain relations and business integrity across heterogeneous database platforms
- Fine-tuned scrambling algorithms to handle extremely large volumes of data
- Automatic alert mechanism to monitor and prevent sensitive data leakage
- Centralized solution for sensitive data detection and scrambling
- Easy and fast installation and deployment
- Masking and scrambling preview
- Supports most common relational databases: Oracle, Microsoft SQL Server, MySQL, DB2

About Brillix Ltd.

Since 2007, we strive to plan, develop and deploy best-of-breed innovative technologies and solutions for your database platforms, data security and big data environments. We are committed to provide the highest quality of products and services delivered by our world renowned dedicated team of industry's top notch data experts.