Database Anomalous Activities: Detection and Quantification*

Elisa Costante, Sokratis Vavilis, Sandro Etalle, Jerry Den Hartog, Milan Petković, Nicola Zannone

ICT.OPEN, 27-28 NOVEMBER 2013 - EINDHOVEN

Problem

Data Leakage: undesired disclosure of the organization's sensitive information, be it intentional or accidental.

Data leakage can cause extensive **monetary loss**, damage to **reputation** and **legal problems**.

Goal

Detect anomalies indicative of data leakage by **monitoring** (**SQL**) database usage/activities.

Advantages of acting at the database level:

- **Better analysis**: the information is still structured;
- **Earlier analysis:** the leakage is detected when the information is leaving the database;
- **Early response:** the leakage can be sealed before data is widely spread.

Approach

1. **Monitor** users'(SQL) activities for the time necessary to capture normal behavior.

2. **Learn** normal behavior profiles based on users' activities .

3. **Detect** anomalous activities and the root cause of the anomaly.

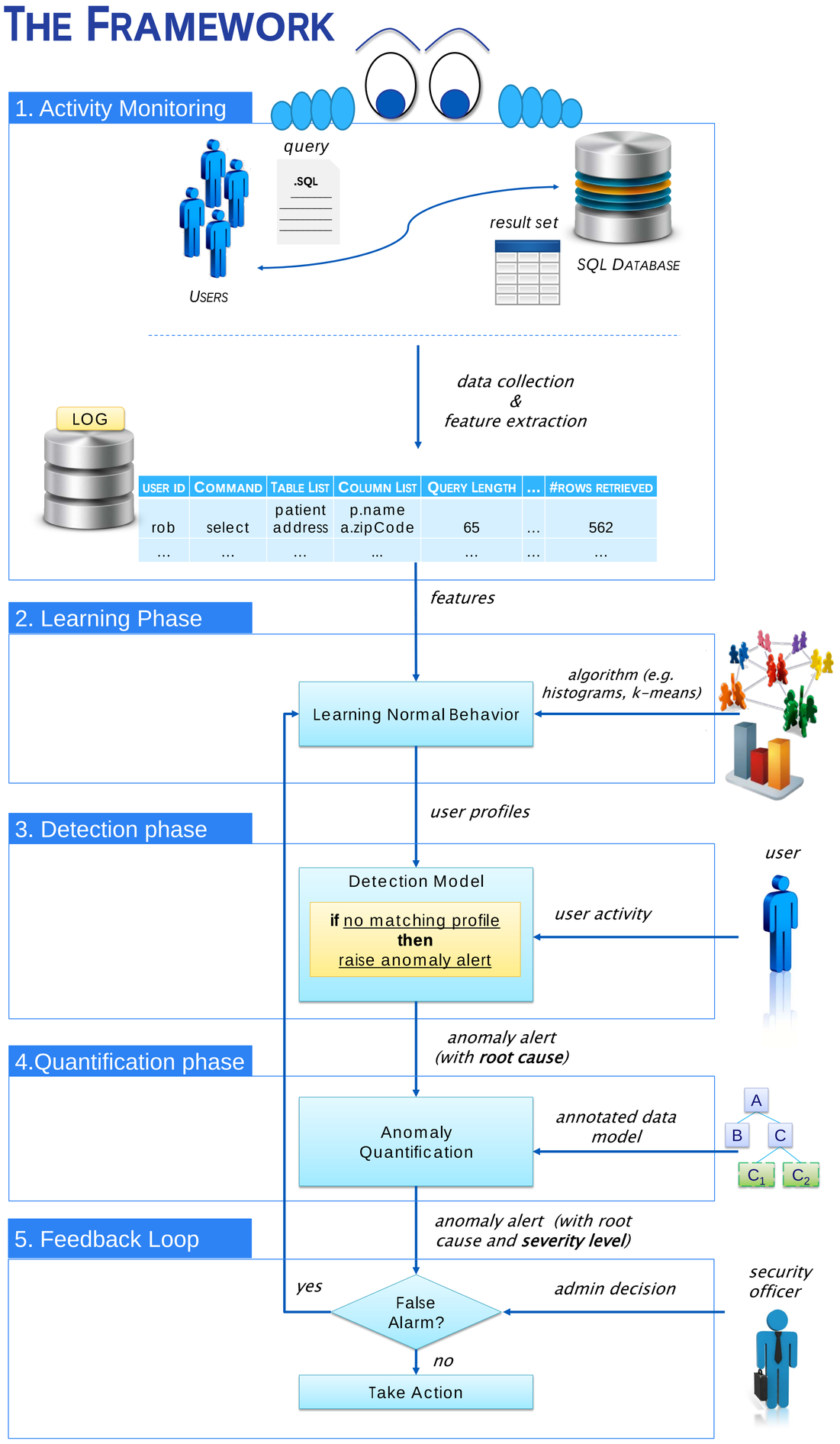
4. **Quantify** the anomaly severity based on data sensitivity (annotated data model).

5. Use **feedback** (e.g. false alarms) to update the user profiles.

What's New

- Profiling considers the **result set** and the **context** in addition to the SQL **query.**
- **Root cause** of an anomaly is explicitly indicated (e.g. the table accessed, or the amount of data retrieved).
- Actual data retrieved is used to rate **severity** of anomalies
- A **feedback loop** is introduced to reduce false alarms (profiles are updated when false alarms arise).

The Framework



Ongoing Work

Development and **validation** of the framework with extensive tests on real data from different application domains:

- **healthcare**;
- **financial** sector;
- service **management**

Acknowledgment: this research has been partially supported by the COMMIT/ THeCS Project.

Contacts: Elisa Costante (e.costante@tue.nl), Sokratis Vavilis (s.vavilis@tue.nl)

*** in Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013.**