UDC 004.9

Pushkar Anton, Postgraduate Student,
Yahup Kateryna, D.Sc., Professor,
Kopp Andrii, Ph.D., Associate Professor
National Technical University «Kharkiv Polytechnic Institute»

TOWARDS ML-DRIVEN ARCHITECTURAL SOLUTION FOR PREVENTING MALICIOUS SQL TRANSACTIONS

SQL injections are the most common vulnerabilities in information systems. They arise from improper handling of input data and errors in the construction of SQL transactions. According to [1], this category of attacks consistently ranks among the most prevalent, accounting for approximately 18.01% of all vulnerabilities. The consequences of SQL injections extend beyond individual services and affect the system architecture as a whole. The integrity of processes is compromised, risks of vulnerability propagation arise, and threats of non-compliance with security standards such as GDPR or ISO/IEC 27001 increase [2]. Existing approaches are often based on static rules and do not account for complex attack patterns. The goal of this study is to develop an architectural approach to prevent malicious SQL transactions based on machine learning methods.

The proposed concept involves integrating an intelligent SQL transaction monitoring tool into the overall architecture of the information system. The tool functions as an intermediary component between the application layer and the database. It analyzes all SQL queries before they are executed. Its main function is to detect potentially harmful transactions and block them.

Architecturally, the proposed system consists of a data collection module, a processing module, and a decision-making module (Fig. 1). This system receives SQL transactions along with their execution context as input. This is followed by preprocessing, which includes SQL code normalization, feature extraction, and conversion into a vector-based format suitable for machine learning. Features may include query structure, the presence of suspicious patterns, string length, and the frequency of key operators.

A key component of the proposed architectural approach (Fig. 1) is a set of machine learning algorithms that classify SQL transactions. The following machine learning algorithms are considered: Single-Layer Perceptron (SLP), Logistic Regression, k-Nearest Neighbors (k-NN), Support Vector Machine (SVM), Naive Bayes, and Decision Trees. Each algorithm should be trained on historical data containing both legitimate and malicious SQL transactions. The result of the analysis is planned as a probabilistic assessment of whether a transaction is malicious.

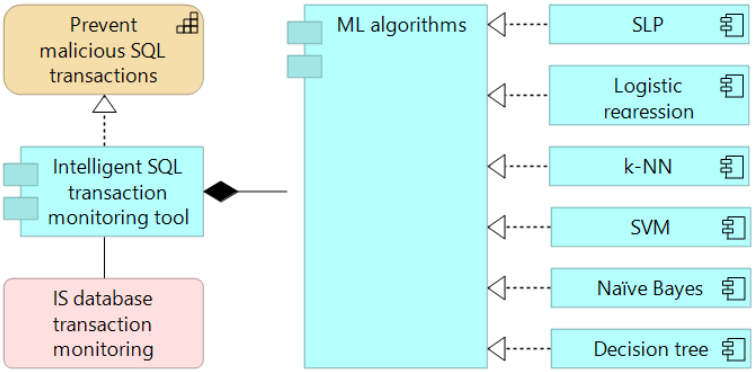

Fig. 1. ML-driven tool for preventing malicious SQL transactions

The formalization of this approach involves an SQL transaction as a feature vector and applying a classification function that maps this vector to a binary decision: to commit or rollback a transaction. To improve accuracy, an ensemble approach can be used, in which the results of multiple algorithms are aggregated. The final decision is made based on a threshold value.

Integrating this tool into the information system ensures continuous monitoring of SQL transactions. This makes possible to detect attacks at an early stage and reduce the risk of vulnerabilities spreading across system components. The proposed architecture (Fig. 1) allows for scalability and adaptation to the new types of attacks through model retraining.

References:

1. Mustapha A. A., Udeh A. S., Ashi T. A., Sobowale O. S. Comprehensive review of machine learning models for SQL injection detection in e-commerce // World Journal of Advanced Research and Reviews. 2024. Vol. 23, No. 1. DOI: https://doi.org/10.30574/wjarr.2024.23.1.2004

2. Imtiaz M. A., Ahmed M. Z., Khalid F. et al. Data exploration with SQL: A machine learning based end-to-end prediction and data security framework for the detection of attack in emerging cloud computing databases and integrated paradigms: analysis on taxonomy, challenges, and opportunities // Sustainable Engineering and Smart Technologies Journal. 2025. URL: https://www.sesjournal.com/index.php/1/article/download/155/149.