ABSTRACT

SQL Injection (SQLi) attacks are cyber threats that exploit web application security holes to access sensitive data. This research develops a dynamic detection system using a deep learning Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model. The model is trained using malicious and benign query datasets through preprocessing, feature extraction, and training stages. The CNN-LSTM model is integrated with the Flask API which functions as a REST API endpoint, accepting input from a Laravel 10 web application. The Flask API processes the input data using the CNN-LSTM model, then returns a JSON response to ensure real-time detection of user input. The CNN-LSTM model in the test process was able to achieve an accuracy of 0.988. The Laravel 10 web integrated with the Flask API system can achieve an average detection speed of 321.54 ms.

Keywords: *sql injection, flask api*, CNN, LSTM*, dynamic detection, deep learning*