ABSTRACT

User access security is a critical issue in the digital era, where systems increasingly rely on network-based platforms. Biometric identification methods, such as keystroke dynamics, are considered more secure than conventional approaches like passwords or personal identification numbers (PINs). This study aims to implement the Multi-Voter Multi-Commission Nearest Neighbor Classifier (MVMCNN) to evaluate the performance of user identification using keystroke biometrics. MVMCNN was chosen for its ability to overcome the limitations of KNN, such as sensitivity to the k value and outliers, by utilizing a multi-voter scheme and neighbor weighting based on the Local Mean Probabilistic Neural Network (LMPNN) approach. This research uses a keystroke dynamics dataset from Telkom University, which has been processed into structured features, including UD, DD, DU, UU, and Duration. Experiments were conducted in three scenarios: (1) determining the optimal vector length (N) with variations of N = 4, 8, 12, 16, 20, and 24, (2) simplifying each feature into mean and median values to assess the effectiveness of simplified feature representations, and (3) applying feature selection using a Variance Threshold (0.1) to eliminate low-variability features. The evaluation was performed using the F1-Score metric as the primary performance parameter. The results indicate that the first scenario, with N = 20, achieved the highest F1-Score of 0.6911. However, feature simplification in the second scenario reduced the model's performance, with the best F1-Score for mean reaching only 0.3031 at k = 9 and 0.3257 for median at k = 3, demonstrating that feature richness plays a crucial role in maintaining identification accuracy. In the third scenario, feature selection using the Variance Threshold produced results similar to the first scenario, indicating that the initial data distribution was already sufficient, and further feature reduction was unnecessary. These findings highlight that data granularity significantly impacts the accuracy of keystroke dynamics-based identification systems.

Keywords: *biometrics, keystroke, user identification, MVMCNN, F1-Score.*