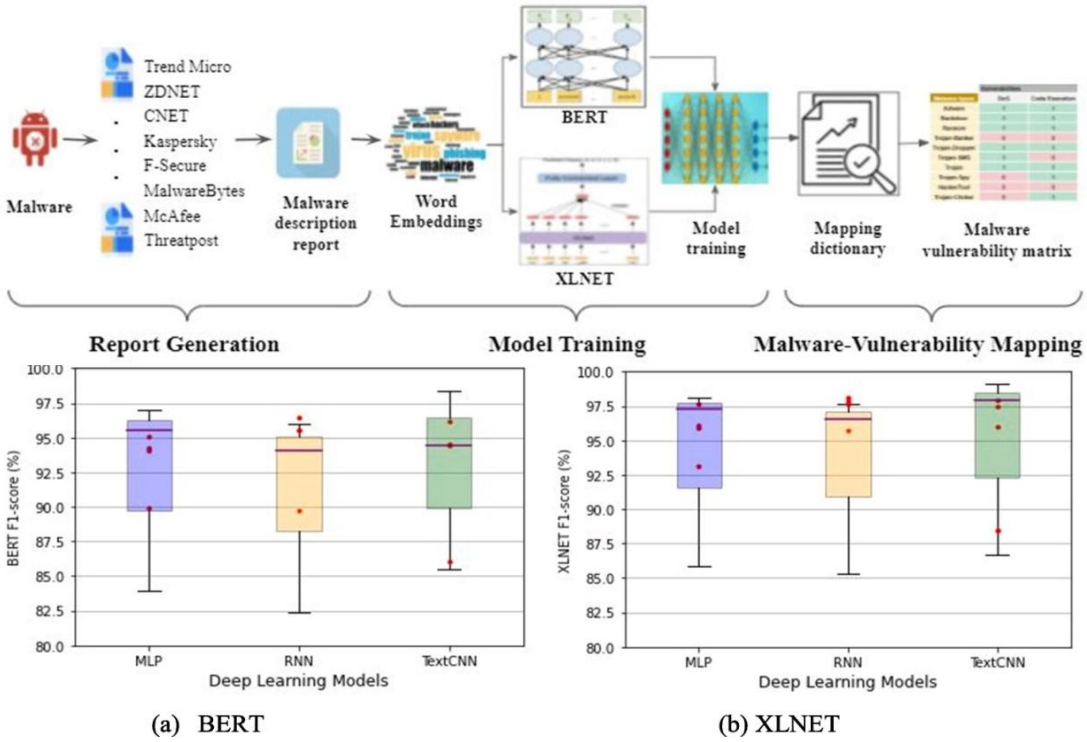
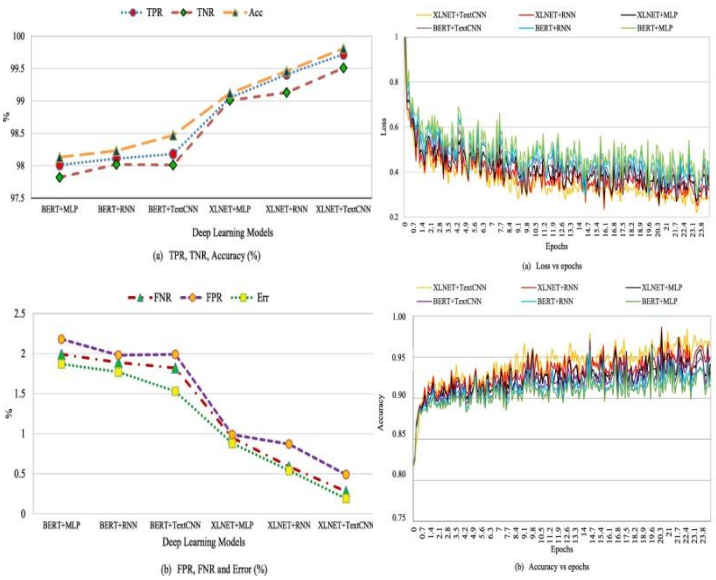
M2VMapper: Malware-to-Vulnerability mapping for Android using text processing

M2VMapper models the malware description reports using semantic modelling techniques such as BERT and XLNET along with to Multi-layer Perceptron (MLP), Recurrent Neural Network (RNN) and Textual Convolution Neural Network.





This mapping can be leveraged to measure the severity of unknown vulnerabilities and malware during the initial phase of application development. The study is a first of its kind and considers 150 malware families from different datasets, such as AMD, CICInvesAndMal2019, and Androzoo with a total of 48 907 malware samples and 9 vulnerability types affecting Android. M2VMapper has delivered highly promising results with an accuracy of 99.81%, when XLNET is used with TextCNN, and precision and F1-scores above 95% using DL.

Shivi Garg, J.C. Bose University of Science & Technology YMCA, Faridabad, India : shivigarg@jcboseust.ac.in and Niyati Baliyan, Indira Gandhi Delhi Technical University for Women, New Delhi India)

Original publication: Garg, S., & Baliyan, N. (2022). M2VMapper: Malware-to-Vulnerability mapping for Android using text processing. Expert Systems with Applications, 191, 116360. https://doi.org/10.1016/j.eswa.2021.116360