Towards Building an Intelligent Anti-Malware System: A Deep Learning Approach using Support Vector Machine (SVM) for Malware Classification

1. Summary The study focuses on using deep learning (DL) models for improving malware classification, highlighting the GRU-SVM model's superior predictive accuracy of about 84.92%. The Malimg dataset, containing diverse malware samples, is utilized for evaluating model performance.

1.1 Motivation/Purpose/Aims/Hypothesis The research is motivated by the need for advanced malware detection methods. It hypothesizes that DL models can more effectively identify unknown malware compared to traditional systems.

1.2 Contribution This paper contributes to the field by integrating DL models with L2-SVM for malware classification, analyzing different models (CNN-SVM, GRU-SVM, MLP-SVM) for their effectiveness in this task.

1.3 Methodology The methodology includes using TensorFlow and related libraries to implement DL algorithms, with the Malimg dataset serving as the primary data source. Standardized preprocessing of the malware images ensures consistent model training and testing.

1.4 Conclusion The GRU-SVM model outperforms others in accuracy due to its complex architecture. However, its longer computing time is a trade-off. The paper suggests enhancing other models' architecture for potentially better performance.

2. Limitations

- **Limited Dataset**: The study's reliance on the Malimg dataset could limit the models' applicability to a broader range of malware types.
- **Computing Efficiency**: The complex architecture of the GRU-SVM model results in longer processing times, which could be impractical in time-sensitive scenarios.

3. Synthesis The findings suggest deep learning models hold promise in malware classification. Future research should focus on balancing model complexity with efficiency and expanding dataset diversity to enhance model applicability in real-world scenarios.