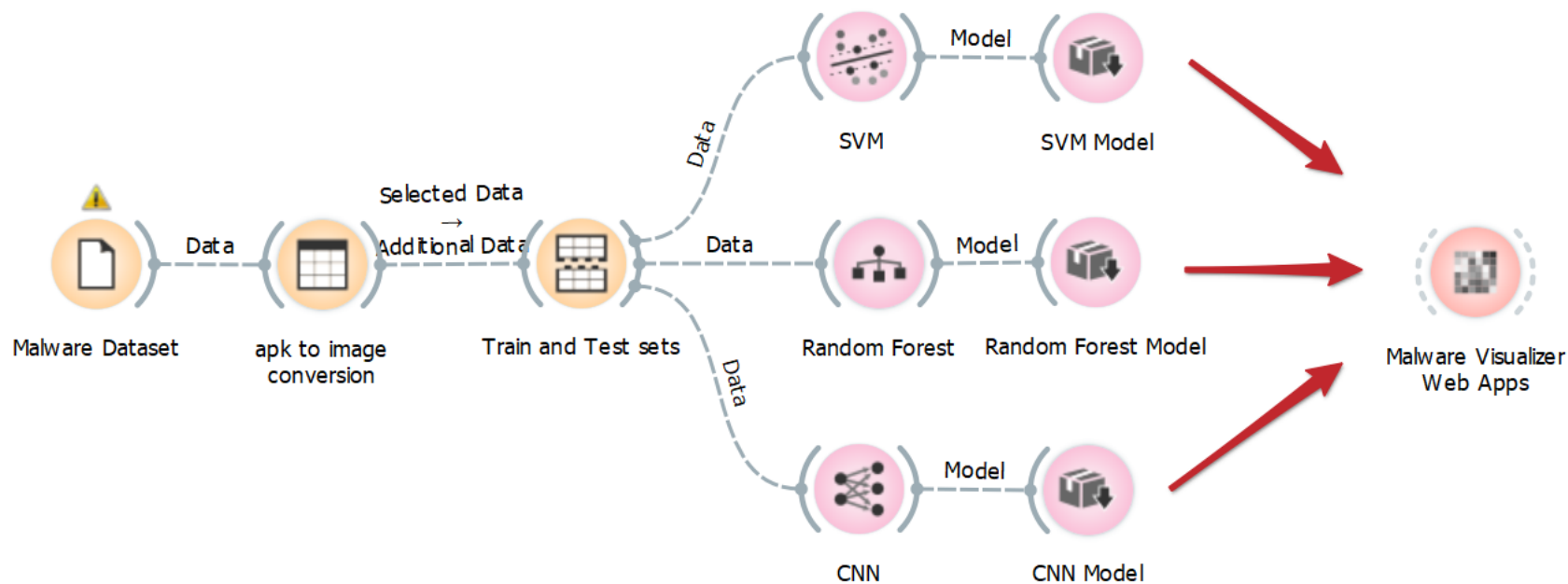# MALWARE VISUALIZER: A WEB APPS MALWARE FAMILY CLASSIFICATION WITH MACHINE LEARNING

INVENTOR: DR. MOHD. ZAMRI BIN OSMAN
FACULTY: FACULTY OF COMPUTING
UNIVERSITY: UNIVERSITI MALAYSIA PAHANG
EMAIL: zamriosman@ump.edu.my
CO-INVENTORS: DR. AHMAD FIRDAUS BIN ZAINAL ABIDIN,
RAHIWAN NAZAR BIN ROMLI

Methods: Modeling of the Malware Family Classification with Random Forest, Support Vector Machine and Convolutional Neural Network

Product Background

Within the past few years, malware has been a serious threat to the security and privacy of all mobile phone users. Due to the popularity of smartphones, primarily Android, this makes them a very viable target for spreading malware. Many solutions in the past have proven to be ineffective and result many false positives. Other than that, most of the solution focuses on the android apk file, instead of visualizing the apk into image-based form.

The objective of this project is to build a web apps to classify malware by transforming the apk file into image-based representation. This project uses three classification algorithm which are Random Forest (RF), Support Vector Machine (SVM), and Convolutional Neural Network (CNN).

The web apps is developed using Python with help of Streamlit with is a Python library for building data-driven web apps. The dataset contains 25 malware classes ranging from Trojan Horses to Spyware and 1 legitimate application class.

Novelty / Originality / Inventiveness

- Machine Learning Web Apps for malware family Classification with machine learning algorithms

Benefits / Usefulness / Applicability

- Can be use in the class especially Artificial Intelligence or Cybersecurity courses which show the usage of machine learning in the computer security domain.
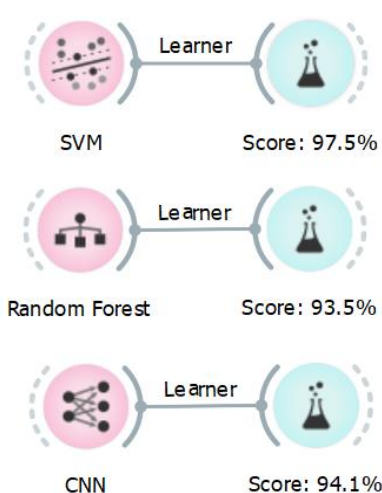- The web apps can be access online.

Status of Innovation

- The product is under prototype status

Publication

- *Android Malware Classification Framework with Optimized Features based on Static-based Analysis*, **2020** (Scopus) – accepted for publication
- Maldroid: Attribute Selection Analysis for Malware Classification, vol 97 no 20, 2419-2429, **2019**

Accuracy Results

Drag and Drop option for uploading the malware image into the Web Apps