Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	26 October 2023
Team ID	2.8
Project Name	Malware Detection and Classification
Maximum Marks	4 Marks

Technical Architecture:

1. TensorFlow: TensorFlow is a freely available software library that empowers developers to create and train machine learning models. It was originally created by Google and has found widespread use in diverse fields, ranging from image and speech recognition to natural language processing and robotics. It is popular both in research and industry for its ability to handle complex computations and its ease of use.
   Usage in Malware Detection:

- Deep Learning Models: TensorFlow is used to construct deep neural networks for processing complex patterns in .exe files.
- Training: The framework facilitates the training of the neural network using the labeled dataset, enabling the model to learn to distinguish between benign and malicious files.
- Inference: Trained TensorFlow models perform fast and accurate predictions, classifying .exe files as either malicious or benign.

2. Keras: Keras is a comprehensive library that offers an array of pre-designed layers to developers, including convolutional layers suitable for processing images, recurrent layers ideal for sequential data, and dense layers for general-purpose computation. In addition, Keras provides an array of training tools, including various optimization algorithms, loss functions, and metrics, that developers can specify while building their models to achieve the desired training outcomes.
   Usage in Malware Detection:

- Simplicity: Keras simplifies the process of building neural networks, allowing quick prototyping and experimentation with different architectures.
- Compatibility: As part of TensorFlow, Keras seamlessly integrates with TensorFlow's ecosystem, providing a high-level interface for creating complex neural networks.

3. ArgParse: ArgParse is a python standard library used for parsing command line arguments and options. It is very useful in creating command line interfaces (CLI) that accept various options, arguments and sub-commands. In this project, ArgParse is used to give a CLI to exe- to-img, and specify startup mode for cnn-model.
   Usage in Malware Detection:

- User Interaction: ArgParse is used to accept user inputs, such as paths to .exe files and trained models, directly from the command line interface.
- Flexibility: Command-line arguments make the system more versatile, allowing users to specify different files and models without modifying the source code.