Cloud-based PE Malware Detection API

by

Naresh Venkataramanan

1. OVERVIEW

   The project builds a model which detect malware on MalConv architecture which is uploaded of Amazon Sagemaker to generate endpoint API.

MalConv Architecture

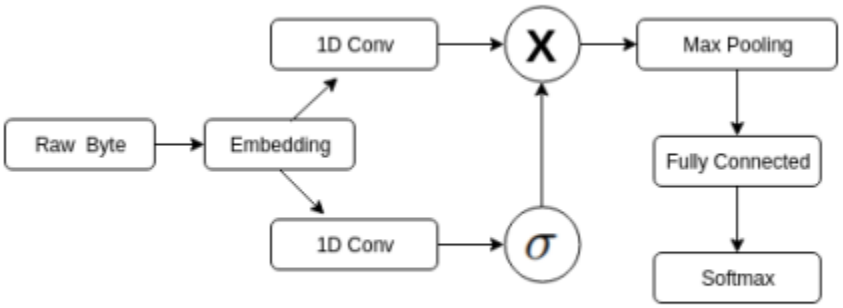

Figure 1: High-Level Diagram of the MalConv Architecture

2. Project Files

   Model: Training a deep neural network based on the MalConv architecture to classify PE files as malware or benign by using a dataset EMBER-2017 v2.
   Cloud: Upload the Model on the AWS Sagemaker.
   Client: Detect the PE file probabilities of Malware.

3. Development

   Load the https://github.com/endgameinc/ember and build a vectored dataset from ember library. The training dataset shape is of two dimension with a shape (9000000,2381). The model is trained on multi-layer neural network with activation layer and dropout (0.4). The batch size of 128 and epoch 1000 for few hours training on the dataset to develop the model.

4. Model

```
def make_model(feature_size):

  tf.compat.v1.disable_eager_execution()

  keras.backend.clear_session()

  model = tf.keras.Sequential()
  model.add(layers.InputLayer(input_shape=(1,feature_size)))
  model.add(layers.Dropout(0.5))
  model.add(layers.Dense(3500, activation='relu'))
  model.add(layers.Dropout(0.5))
  model.add(layers.Dense(1, activation='sigmoid'))

  model.compile(tf.keras.optimizers.Adam(learning_rate=0.001),
            loss='binary_crossentropy',
            metrics=['accuracy',tf.keras.metrics.AUC(),tf.keras.metrics.Precision()])

  model.fit(X_train, y_train,batch_size=128,epochs=1,validation_split=0.2)

  model_json = model.to_json()
  with open(dir+"model.json", "w") as json_file:
        json_file.write(model_json)
  print(model.summary())

  return model
```

5. Aws Sage Maker

Amazon SageMaker is **a** fully managed machine learning service. With SageMaker, data scientists and developers can quickly and easily build and train machine learning models, and then directly deploy them into a production-ready hosted environment.

We will upload the Model and weight on the AWS S3 bucket and use Amazon SageMaker to generate the endpoint [API]

6. Conclusion

Deployment of Model on AWS sage maker is efficient way of transfer the learnt machine learning model transfer for third party service.