Supply Chain Risk Related Classification Challenge Series - (01/03): NLP-based Threat Detection - REPORT

Model Introduction

This model uses the implementation of BERT from the TensorFlow Models repository on GitHub at tensorflow/models/official/nlp/bert. It uses L=12 hidden layers (Transformer blocks), a hidden size of H=768, and A=12 attention heads.

This model has been pre-trained for English on the Wikipedia and BooksCorpus. Inputs have been "uncased", meaning that the text has been lower-cased before tokenization into word pieces, and any accent markers have been stripped. In order to download this model, Internet must be activated on the kernel.

Configurations:

In the configuration section of .ipynb following needs to be set:

```
input_training_master_filepath =
input_training_node_filepath =
input_test_master_filepath =
input_test_node_filepath =
Output_file_path =
bert_module_url = 'https://tfhub.dev/tensorflow/bert_en_uncased_L-12_H-768_A-12/2' # default path'
```

(The BERT module can be downloaded, and local path can be provided)

CSV Files

1. Master.csv

   Columns used for prediction: Title, Subject, Summary, Category, Severity

   Columns not used:

   a. Created Date, Occurrence Date, Last Modified Date: These date fields do not add value for prediction

   b. Main Category: Category field is used instead, which contains more classified information

   c. Country, City: This data is retrieved from Nodes.csv

   d. Source: There is not much information related to this and hence left out.

   e. Subject: This field is used only if it is different from Title. In the given dataset it is same for all rows

2. Node.csv

   Columns used for prediction: Country, City, Node Type, Status

   Columns not used:

   a. Assigned Commodities, Primary Contact Mail, Assigned Products: No data is available for these fields to assess the impact on prediction

   b. Distance: For the model used, this numeric value may not help with predictions

3. Lanes.csv

   There is no data available for including it for training the model.

Concatenated text string created from columns and used for prediction:

1. Severity: This field is taken from the Master.csv
2. Category: This field is taken from the Master.csv
3. Country: This field is taken from the Lanes.csv
4. Status: This field is taken from the Lanes.csv
5. City: There may be a 1-to-many relationship between Master.csv & Node.csv.

   A concatenated list of ‘cities’ impacted is used.
6. Node Type: There may be a 1-to-many relationship between Master.csv & Node.csv.

   A concatenated list of ‘Node Type’ is used.
7. Title: This field is taken from the Master.csv

   Following words are removed from the title since these are already captured by ‘Severity’ field – Extreme, Minor, Severe, Moderate, Incident

   Country is also removed if present, since it is already captured in the ‘Country’ field.
8. Subject: This field is taken from Master.csv is used only if it different from the Title field. All cleaning done for the ‘Title’ field also apply for ‘Subject’ field
9. Summary: Title: This field is taken from the Master.csv

The maximum length of this concatenated string is 128.

The data cleaning and concatenation has been done taking care that there is no dataset specific coding.

Additional Details for the Model

BERT from the Tensorflow Hub is loaded. There are no dense or pooling layers added after last layer of BERT.

Fixed learning rate, batch size, epochs, optimizer. The optimizer used is Adam, with a learning rate between 2e-5 and 5e-5. The model is trained for 3 epochs with a batch size of 32.

The training data is split into 80% train and 20% validation set.

Result csv

‘Alert ID’ column contains binary output- 0 or 1

‘Threat Level’ column contains confidence score