Configuration Manual

MSc Research Project
MSc Data Analytics

Saketh Reddy Atla
Student ID: x22218700

School of Computing
National College of Ireland

Supervisor: Teerath Kumar Menghwar

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	SAKETH REDDY ATLA		
Student ID:	X22218700		
Programme:	MSCDAD_B	**Year:**	2023-2024
Module:	MSC RESEARCH PROJECT		
Lecturer:	TEERATH KUMAR MENGHWAR		
Submission Due Date:	12/08/2024		
Project Title:	PHISHING URL DETECTION USING DISTLBERT AND CAPSULE NEURAL NETWORKS		
Word Count:	**305 Page Count: 5**		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: SAKETH REDDY ATLA

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

SAKETH REDDY ATLA
X22218700

1 Step Google drive Directory

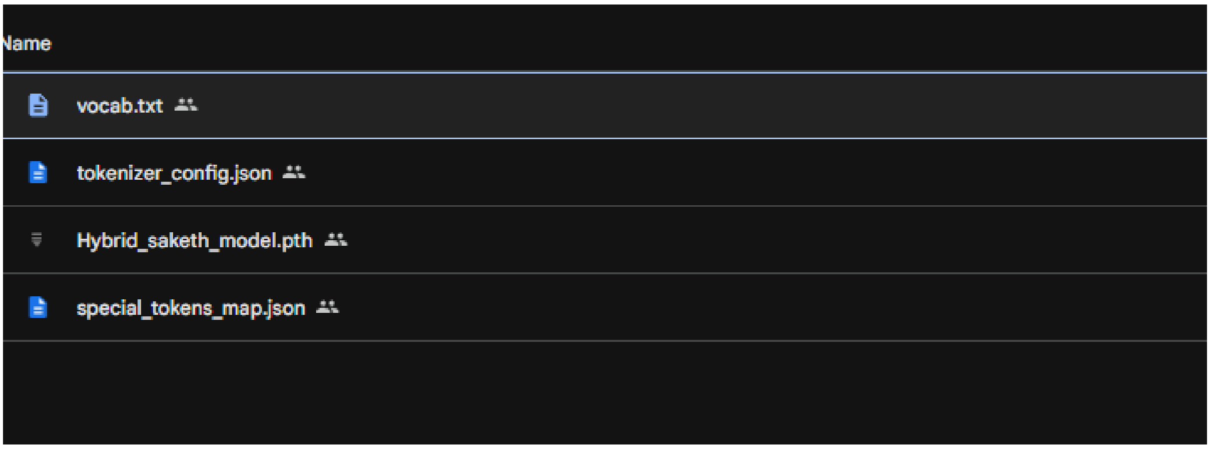
Follow these steps to create a simplified directory structure for your model in Google Drive:

1. Open Google Drive in your web browser.

- Create the main folder:
    - Click "New" > "Folder"
    - Name it "Hybrid_DistilBERT_Capsule_Network"
- Upload base model files to the main folder:
    - Upload "capsule_network.pt"
    - Upload "distilbert.pt"
- Create a subfolder for the hybrid model:
    - Inside "Hybrid_DistilBERT_Capsule_Network", click "New" > "Folder"
    - Name it "hybrid"
- Upload hybrid model files to the "hybrid" subfolder:
    - Upload your hybrid model file
    - Upload the tokenizer files

Your final structure should look like this:

```
Hybrid_DistilBERT_Capsule_Network/
 ├── capsule_network.pt
 ├── distilbert.pt
 └── hybrid/
     ├── [hybrid_model_file]
     ├── tokenizer.json
     └── vocab.txt
```



Name

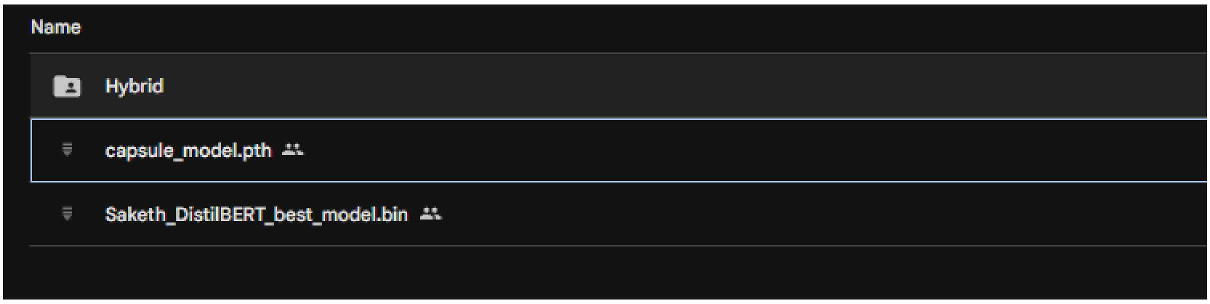
vocab.txt

tokenizer_config.json

Hybrid_saketh_model.pth

special_tokens_map.json

Figure 1 Sample Directory



Name

Hybrid

capsule_model.pth

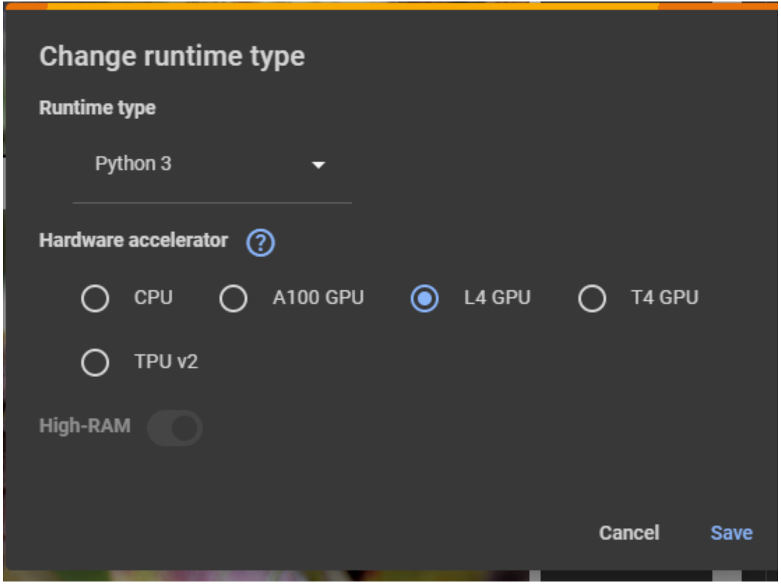
Saketh_DistilBERT_best_model.bin

Figure 2 Sample Directory

2 Setup Google colab

Follow these steps to upload your notebook to Google Colab, connect to Google Drive, and update the model paths:

- Go to Google Colab.
- Click on "File" > "Upload notebook" and select your notebook file and connect to the session.
-



Change runtime type

Runtime type

Python 3

Hardware accelerator

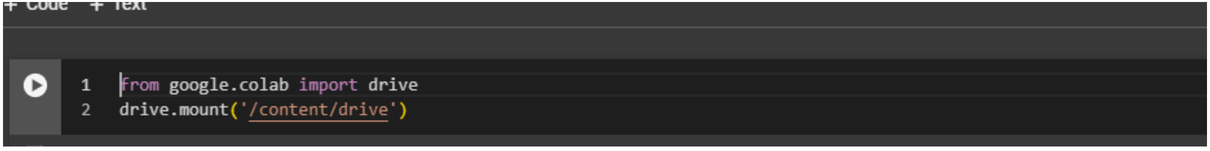
○ CPU ○ A100 GPU ● L4 GPU ○ T4 GPU

○ TPU v2

High-RAM

Figure 3 Connecting to the session after uploading the notebook

- Once the notebook is uploaded, you'll need to mount your Google Drive. Add and run the following code at the beginning of your notebook:

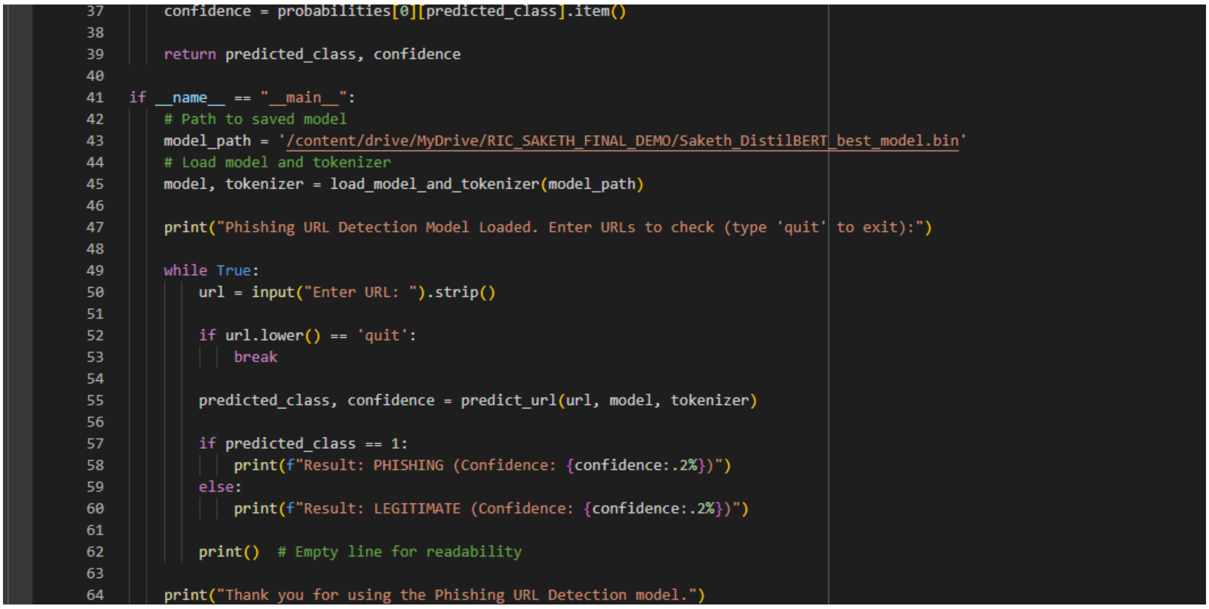


```
from google.colab import drive
drive.mount('/content/drive')
```

Figure 4 Google Mount

3 Changing the paths

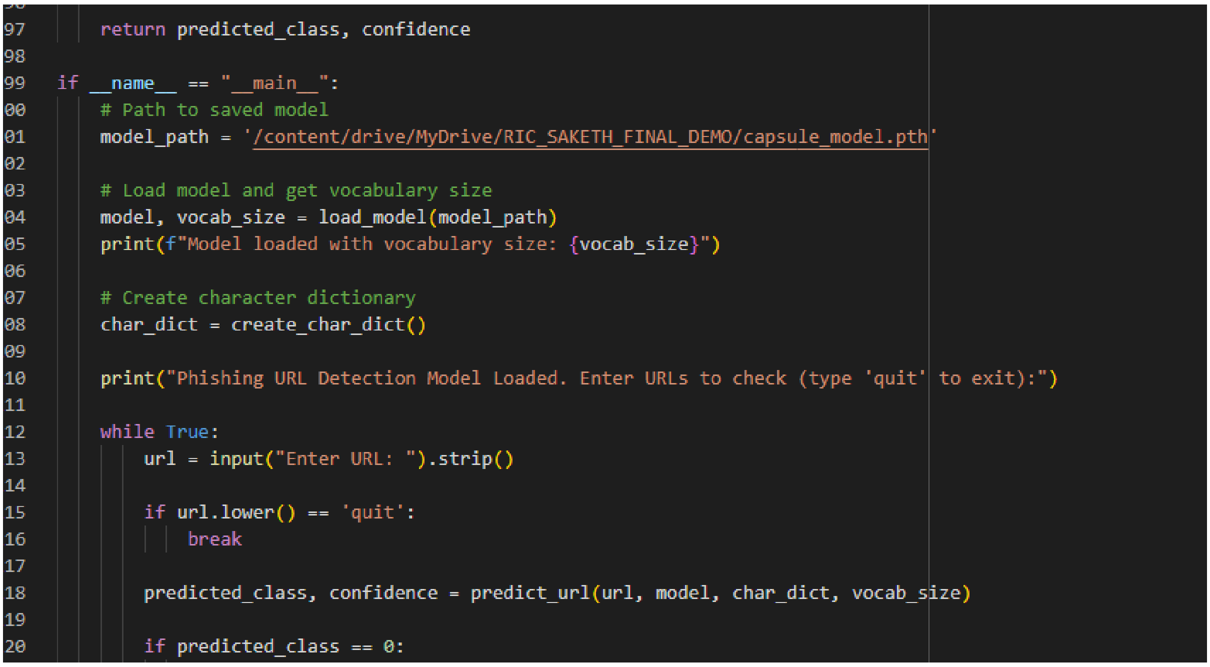
- Change path at 43 line for the Distilbert according to the models uploaded.



```
37        confidence = probabilities[0][predicted_class].item()
38
39        return predicted_class, confidence
40
41    if __name__ == "__main__":
42        # Path to saved model
43        model_path = '/content/drive/MyDrive/RIC_SAKETH_FINAL_DEMO/Saketh_DistilBERT_best_model.bin'
44        # Load model and tokenizer
45        model, tokenizer = load_model_and_tokenizer(model_path)
46
47        print("Phishing URL Detection Model Loaded. Enter URLs to check (type 'quit' to exit):")
48
49        while True:
50            url = input("Enter URL: ").strip()
51
52            if url.lower() == 'quit':
53                break
54
55            predicted_class, confidence = predict_url(url, model, tokenizer)
56
57            if predicted_class == 1:
58                print(f"Result: PHISHING (Confidence: {confidence:.2%})")
59            else:
60                print(f"Result: LEGITIMATE (Confidence: {confidence:.2%})")
61
62            print()  # Empty line for readability
63
64        print("Thank you for using the Phishing URL Detection model.")
```

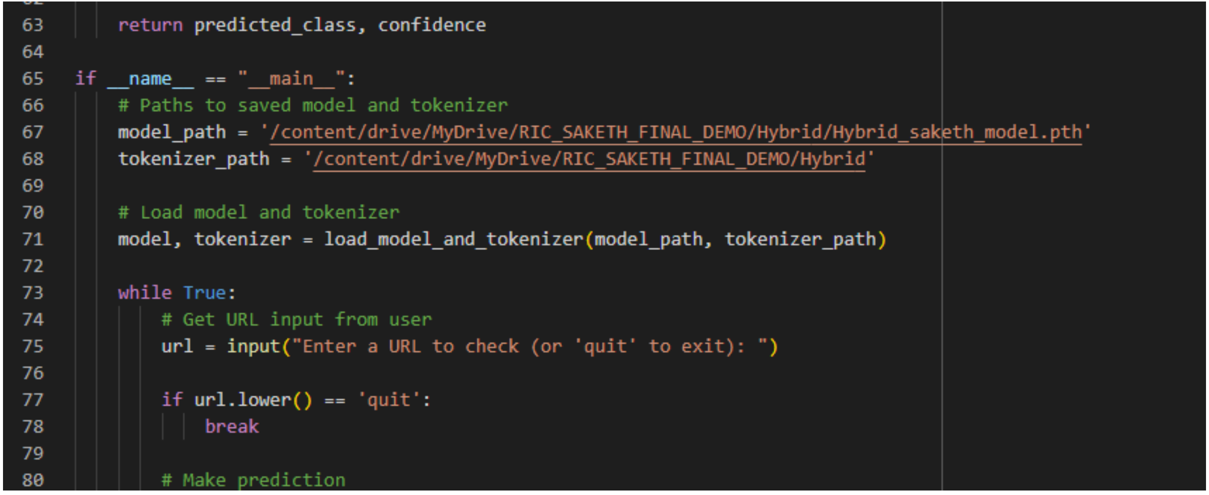
Figure 5 Path change for DistilBERT

- Change path for Capusel_model.pth as per the directory it was stored



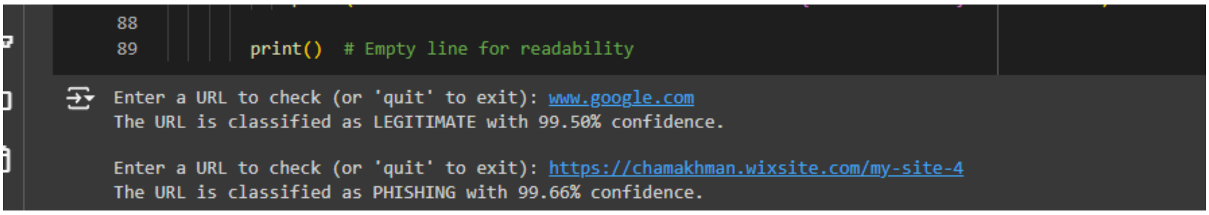
```
    return predicted_class, confidence

if __name__ == "__main__":
    # Path to saved model
    model_path = '/content/drive/MyDrive/RIC_SAKETH_FINAL_DEMO/capsule_model.pth'

    # Load model and get vocabulary size
    model, vocab_size = load_model(model_path)
    print(f"Model loaded with vocabulary size: {vocab_size}")

    # Create character dictionary
    char_dict = create_char_dict()

    print("Phishing URL Detection Model Loaded. Enter URLs to check (type 'quit' to exit):")

    while True:
        url = input("Enter URL: ").strip()

        if url.lower() == 'quit':
            break

        predicted_class, confidence = predict_url(url, model, char_dict, vocab_size)

        if predicted_class == 0:
```

- Change the model path and tokenizer saved path for Hybrid model i.e. DistilBERT-capsule network



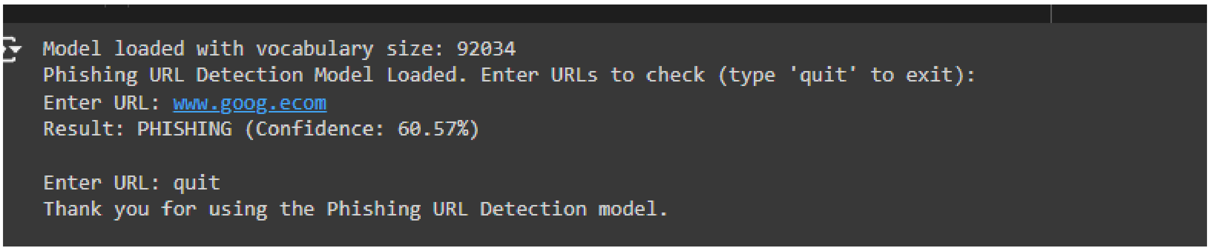
```
    return predicted_class, confidence

if __name__ == "__main__":
    # Paths to saved model and tokenizer
    model_path = '/content/drive/MyDrive/RIC_SAKETH_FINAL_DEMO/Hybrid/Hybrid_saketh_model.pth'
    tokenizer_path = '/content/drive/MyDrive/RIC_SAKETH_FINAL_DEMO/Hybrid'

    # Load model and tokenizer
    model, tokenizer = load_model_and_tokenizer(model_path, tokenizer_path)

    while True:
        # Get URL input from user
        url = input("Enter a URL to check (or 'quit' to exit): ")

        if url.lower() == 'quit':
            break

        # Make prediction
```

4 SAMPLE OUTPUTS

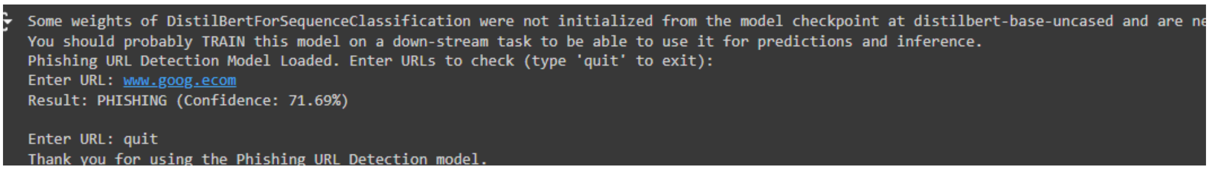


```
            print()  # Empty line for readability
```

```
Enter a URL to check (or 'quit' to exit): www.google.com
The URL is classified as LEGITIMATE with 99.50% confidence.

Enter a URL to check (or 'quit' to exit): https://chamakhman.wixsite.com/my-site-4
The URL is classified as PHISHING with 99.66% confidence.
```



```
Model loaded with vocabulary size: 92034
Phishing URL Detection Model Loaded. Enter URLs to check (type 'quit' to exit):
Enter URL: www.goog.ecom
Result: PHISHING (Confidence: 60.57%)

Enter URL: quit
Thank you for using the Phishing URL Detection model.
```



```
Some weights of DistilBertForSequenceClassification were not initialized from the model checkpoint at distilbert-base-uncased and are ne
You should probably TRAIN this model on a down-stream task to be able to use it for predictions and inference.
Phishing URL Detection Model Loaded. Enter URLs to check (type 'quit' to exit):
Enter URL: www.goog.ecom
Result: PHISHING (Confidence: 71.69%)

Enter URL: quit
Thank you for using the Phishing URL Detection model.
```

5 REFERENCES

Sanh, V., Debut, L., Chaumond, J., & Wolf, T. (2019). DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1910.01108
colab.google. (n.d.). colab.google. https://colab.google/

Sabour, S., Frosst, N., & Hinton, G. E. (2017). Dynamic Routing Between Capsules. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1710.09829