DETECTING EMAIL-BASED PHISHING WEBSITES USING MACHINE LEARNING

2023-123

Team Members

J.M.Lindamulage

Mandira Pabasari L.

Yapa S.P.J.

Perera I.S.S.

Research Question

How to detect phishing websites and phishing emails using machine learning.

Main Objective

To implement a mobile application and a web extension capable of detecting phishing emails and websites utilizing machine learning models.

Sub-objectives

- To employ the visual similarity features to classify phishing websites out of legit websites.
- Detecting Phishing sites using website feature analysis
- To identify phishing emails using the heading and the textual content in the email.
- To discover phishing websites using the URL.

IT20222840 |J.M.Lindamulage

BSc (Hons) Degree in Information Technology (specialization in Cyber Security)

Research Problem

How to use visual similarity of a website to detect similar phishing websites.

Objectives

- To use graph neural network to classify images.
  - Vision GNN: An Image is Worth Graph of Nodes(2022) ✓
  - Was trained on ImageNet dataset.
- To adapt graph neural network to classify phishing websites. ✓
  - This will be trained on the phish-iris dataset.
  - Our study will be the first study that will be utilizing their technique for a phishing website detection using visual features.
- To improve the model accuracy to detect zero-day attacks.
- To optimize the developed model for mobile devices.

Graph Neural Network Concept and Vision GNN

Propose the image as a graph structure and introduce a new Vision GNN (ViG) architecture to extract graph level feature for visual tasks.

- Split the image to several patches which are viewed as nodes.
- Patches are transferred into the feature vector.

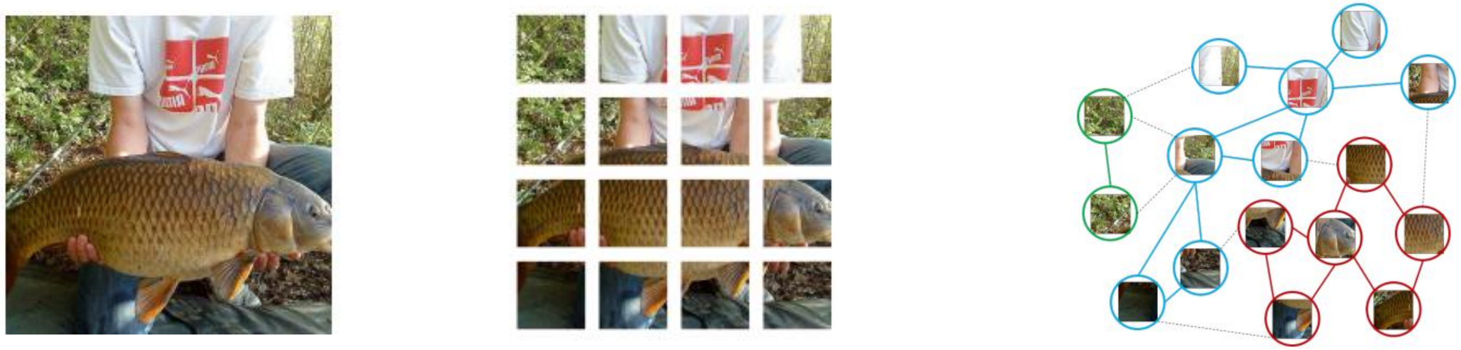


Fig 1. Image to graph construction (source-VisionGNN)

- Original code was implemented to use GPU 8 parallel process.
- Since it was too complex, the necessary files were extracted and code was developed to run on Google colab.

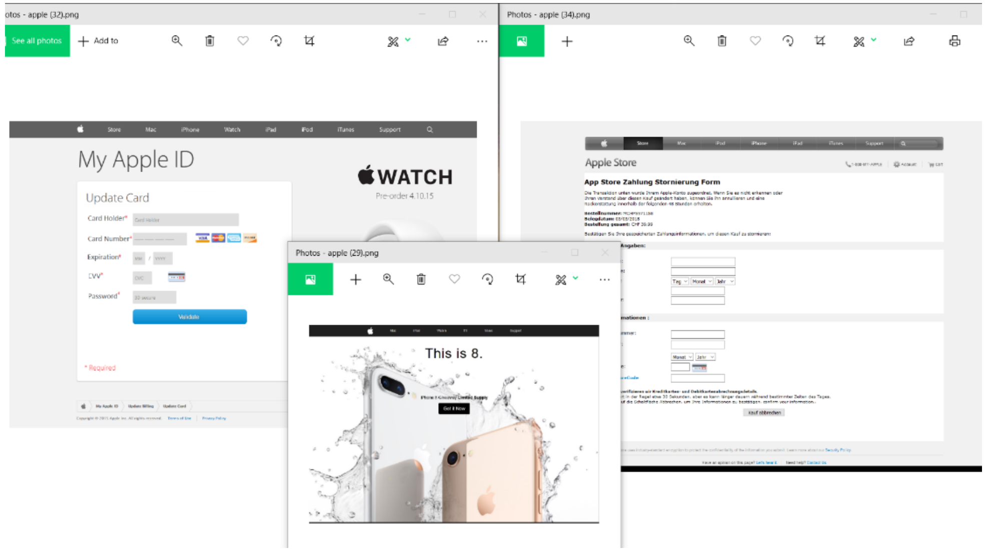
Current progress

Datasets

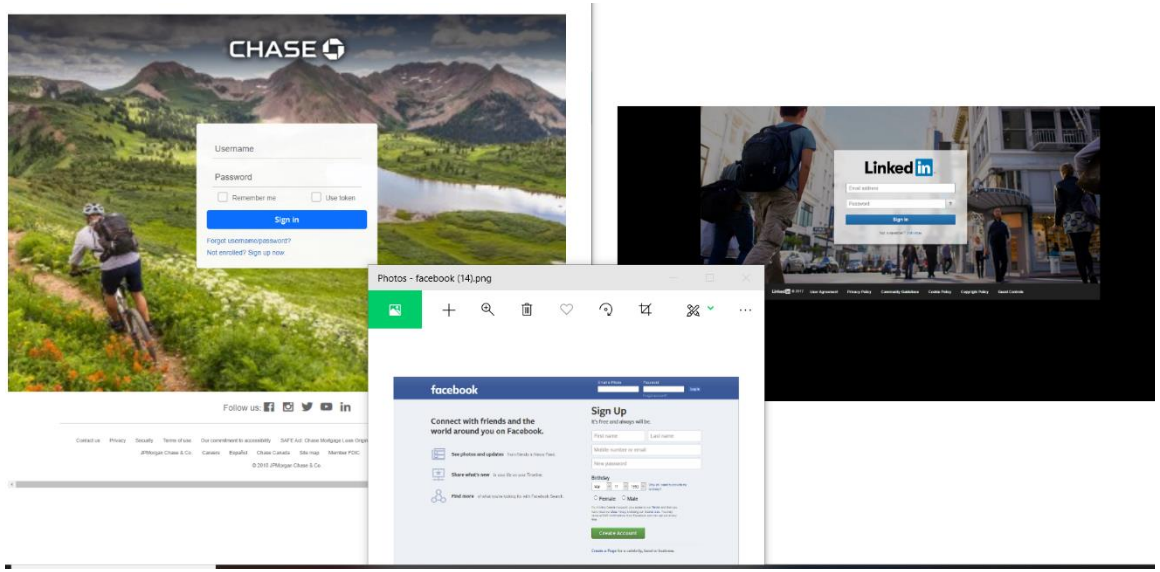
Experimented with two most recent datasets.

- Visual phish
  - Contain 9363 screenshots of PhishTank phishing pages that target 155 websites and 1195 phishing pages.
  - Dataset is larger for testing purpose.
- Phish-Iris
  - target 14 websites and a "other" class.

Dataset

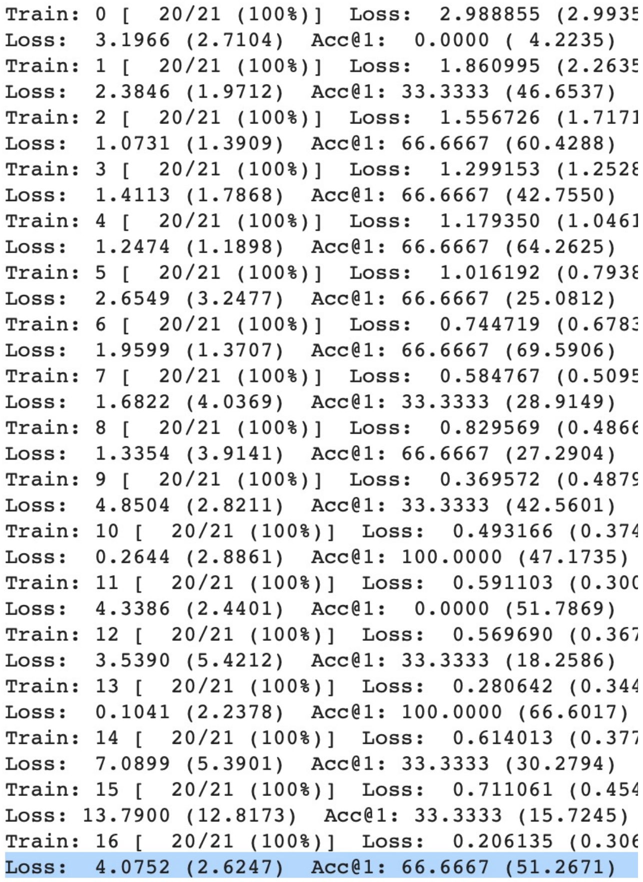


Different screenshots of same website.


CHASE
Username
Password
Sign in
Linked in
Photos - facebook (14).png
facebook
Sign Up
Connect with friends and the world around you on Facebook.

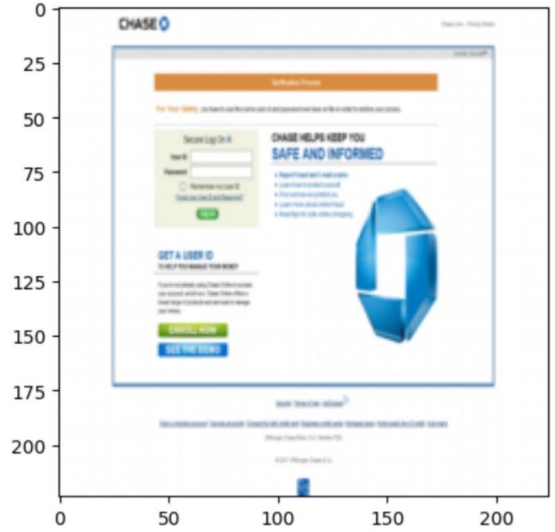
Screenshots of different website.

Accuracy



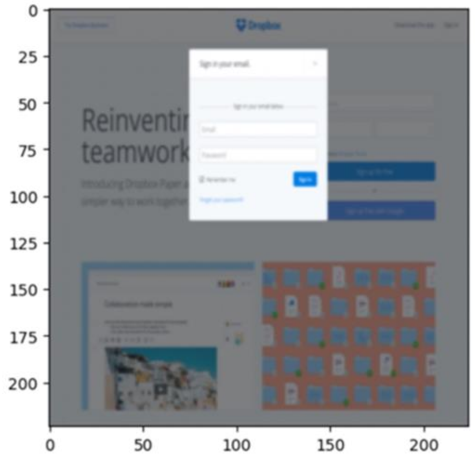
```
Train: 0 [  20/21 (100%)]  Loss:  2.988855 (2.9935
Loss:  3.1966 (2.7104)  Acc@1:  0.0000 ( 4.2235)
Train: 1 [  20/21 (100%)]  Loss:  1.860995 (2.2635
Loss:  2.3846 (1.9712)  Acc@1: 33.3333 (46.6537)
Train: 2 [  20/21 (100%)]  Loss:  1.556726 (1.7171
Loss:  1.0731 (1.3909)  Acc@1: 66.6667 (60.4288)
Train: 3 [  20/21 (100%)]  Loss:  1.299153 (1.2528
Loss:  1.4113 (1.7868)  Acc@1: 66.6667 (42.7550)
Train: 4 [  20/21 (100%)]  Loss:  1.179350 (1.0461
Loss:  1.2474 (1.1898)  Acc@1: 66.6667 (64.2625)
Train: 5 [  20/21 (100%)]  Loss:  1.016192 (0.7938
Loss:  2.6549 (3.2477)  Acc@1: 66.6667 (25.0812)
Train: 6 [  20/21 (100%)]  Loss:  0.744719 (0.6783
Loss:  1.9599 (1.3707)  Acc@1: 66.6667 (69.5906)
Train: 7 [  20/21 (100%)]  Loss:  0.584767 (0.5095
Loss:  1.6822 (4.0369)  Acc@1: 33.3333 (28.9149)
Train: 8 [  20/21 (100%)]  Loss:  0.829569 (0.4866
Loss:  1.3354 (3.9141)  Acc@1: 66.6667 (27.2904)
Train: 9 [  20/21 (100%)]  Loss:  0.369572 (0.4879
Loss:  4.8504 (2.8211)  Acc@1: 33.3333 (42.5601)
Train: 10 [  20/21 (100%)]  Loss:  0.493166 (0.374
Loss:  0.2644 (2.8861)  Acc@1: 100.0000 (47.1735)
Train: 11 [  20/21 (100%)]  Loss:  0.591103 (0.300
Loss:  4.3386 (2.4401)  Acc@1:  0.0000 (51.7869)
Train: 12 [  20/21 (100%)]  Loss:  0.569690 (0.367
Loss:  3.5390 (5.4212)  Acc@1: 33.3333 (18.2586)
Train: 13 [  20/21 (100%)]  Loss:  0.280642 (0.344
Loss:  0.1041 (2.2378)  Acc@1: 100.0000 (66.6017)
Train: 14 [  20/21 (100%)]  Loss:  0.614013 (0.377
Loss:  7.0899 (5.3901)  Acc@1: 33.3333 (30.2794)
Train: 15 [  20/21 (100%)]  Loss:  0.711061 (0.454
Loss: 13.7900 (12.8173)  Acc@1: 33.3333 (15.7245)
Train: 16 [  20/21 (100%)]  Loss:  0.206135 (0.306
Loss:  4.0752 (2.6247)  Acc@1: 66.6667 (51.2671)
```

Maximum accuracy reached – 66%



```
tensor([[ -7.4808,  -0.3093,  -5.7512, -11.0117, -10.9400,  24.4226,  -6.0523,
           5.1337,   1.8349,  -2.9479,  -5.2662,   2.3314,  -7.7054,  -6.5015,
           0.3103]], device='cuda:0', grad_fn=<SqueezeBackward1>)
Predicted label:  5
Real Label:  5
{'adobe': 0, 'alibaba': 1, 'amazon': 2, 'apple': 3, 'boa': 4, 'chase': 5, 'dhl': 6, 'dropbox': 7, 'facebook': 8,
```

Predicted correct

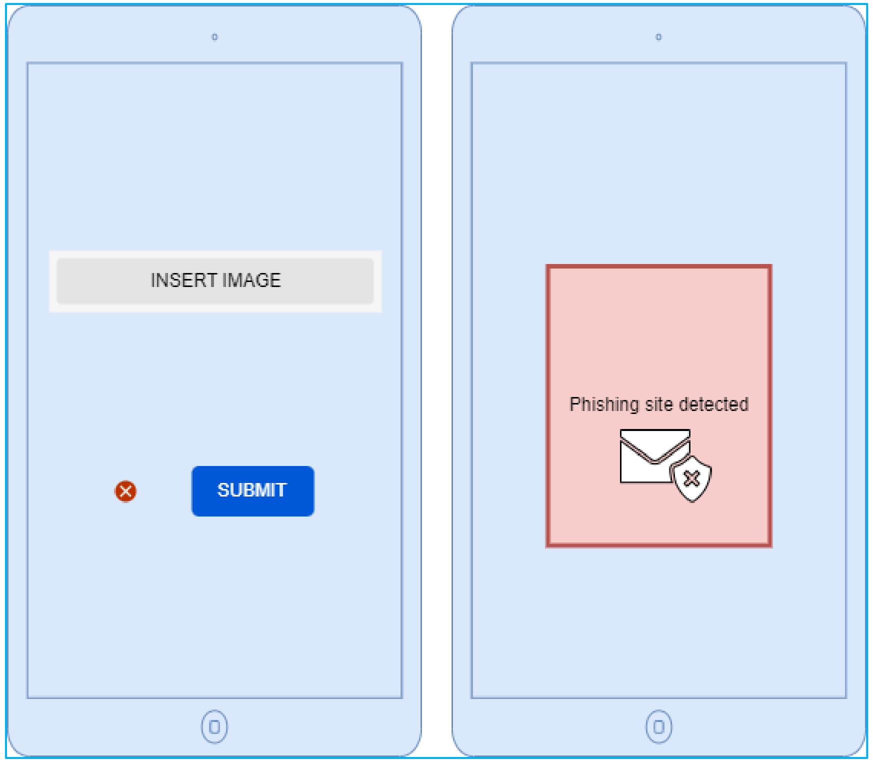


```
tensor([[-0.7453, -4.0790, -4.9918,  2.2352, -5.8290, -2.5973, -5.5398, -1.3433,
          1.0433,  2.8031,  1.0518,  2.5130,  9.9339, -4.1337, -4.7532]],
       device='cuda:0', grad_fn=<SqueezeBackward1>)
Predicted label:  12
Real Label:  7
{'adobe': 0, 'alibaba': 1, 'amazon': 2, 'apple': 3, 'boa': 4, 'chase': 5, 'dhl': 6, 'dropbox': 7, 'facebook': 8,
```

Predicted wrong

Future work

- Use image augmentation techniques to improve accuracy.
- Do testing using visual Phish net dataset.
- Optimize the model to be deployed on mobile devices.
- Make the mobile application and integrate the model to the mobile application.



REFERENCES

[1] Aya Hashim∗Razan Medani, Dr.Tahani Abdalla Attia, "Defences Against web Application Attacks and Detecting Phishing Links Using Machine Learning," in 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Sudan, 2020.

[2] "PHISHING ACTIVITY TRENDS REPORT 3rd Quarter," APWG, 2022.

[3] Dr. Moulana Mohammed,K. Koteswara Prasanth,S. Venkata Sai Subhash , "PHISHING DETECTION USING MACHINE LEARNING ALGORITHMS," in Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022), India, 2022.

[4] A. Lakshmanarao , P.Surya Prabhakara Rao,M M Bala Krishna, "Phishing website detection using novel machine learning fusion approach," in Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021), India, 2021.

[5] Surbhi Gupta,Abhishek Singhal ,Akanksha Kapoor, "A Literature Survey on Social Engineering Attacks:Phishing Attack," in International Conference on Computing, Communication and Automation, India, 2016.

[6] Ankit Kumar Jain and B. B. Gupta, "Phishing Detection: Analysis of Visual Similarity Based Approaches," WILEY, p. 2017, 2017.

[7] R. Dhamija, J. D. Tygar, and M. A. Hearst, "Why phishing works," in SIGCHI Conference on Human, 2006.

[8] Z. Fan, "Detecting and Classifying Phishing Websites by Machine Learning," in 2021 3rd International Conference on Applied Machine Learning (ICAML), china, 2021.

[9] Malak Aljabri ,Samiha Mirza , "Phishing Attacks Detection using Machine Learning and Deep Learning Models," in 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA) , Saudi Arabia, 2022.

[10] "Phishing Website Detection Using Random Forest and Support Vector Machine: A Comparison," in 2nd International Conference on Artificial Intelligence and Data Sciences (AiDAS), Malaysia, 2021.

[11] Jaydeep Solanki, Rupesh G. Vaishnav, "Website Phishing Detection using Heuristic Based Approach," International Research Journal of Engineering and Technology (IRJET), vol. 03, no. 05, 2016.

[12] Eric Medvet,Engin Kirda,Christopher Kruegel, "Visual-Similarity-Based Phishing Detection," in SecureComm 2008 , Turkey, 2008.

[13] Igino Corona1,2, Battista Biggio1,2, Matteo Contini2Luca Piras1,2, Roberto Corda2Mauro, Guido Mureddu2, "DeltaPhish: Detecting Phishing Webpages in Compromised Websites∗," in ESORICS 2017., Italy, 2017.

[14] Sahar Abdelnabi,Katharina Krombholz,Mario Fritz, "VisualPhishNet: Zero-Day Phishing Website Detection by Visual Similarity," 2020.

[15] U. Saeed, "Visual similarity-based phishing detection using deep learning," Journal of Electronic Imaging, vol. 31, no. 5, 2022.

[16] Padmalochan Panda 1,†, Alekha Kumar Mishra 1,† and Deepak Puthal , "A Novel Logo Identification Technique for Logo-Based Phishing Detection in Cyber-Physical Systems," Future Internet, vol. 14, no. 8, 2022.

[17] Saad Al-Ahmadi1 Yasser Alharbi, "DEEP LEARNING TECHNIQUE FOR WEB PHISHING DETECTION COMBINED URL FEATURES AND VISUAL SIMILARITY," International jpurnal of computer networks abd comunications(IJCNC), vol. 12, no. 5, 2020.

[18] Rundong Yang,Kangfeng Zheng, Bin Wu,Chunhua Wu,Xiujuan Wang, "Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning," sensors, 2021.

[19] "Phishing Detection: Analysis of Visual Similarity Based Approaches," WILEY, vol. 2017, 2017.

[20] Kai Han1,2∗ Yunhe Wang2∗ Jianyuan Guo2 Yehui Tang2,3 Enhua Wu1,4, "Vision GNN: An Image is Worth Graph of Nodes".

IT19966236 | MANDIRA PABASARI L.

BSc in Information Technology Specialization in Cyber Security

Detecting Phishing sites using website feature analysis

Website feature analysis

Involves examining and evaluating various characteristics and components of a website.

It focuses on extracting meaningful information from elements such as URL structures, domain names, content, scripting, metadata, visual design, and form handling.

Aims to understand the structure, behavior, and functionality of a website to identify patterns and indicators of potential threats or fraudulent activities.

Crucial for developing algorithms, models, and techniques to detect and classify phishing attacks.

It helps identify specific features associated with phishing, such as abnormal URL patterns, mismatched domain names, suspicious form handling, and unauthorized scripts.

Machine learning algorithms, data mining techniques, and rule-based approaches are used to process and analyze large amounts of data effectively.[1]

Objective:

The objective is to develop a robust accurate method for detecting phishing attacks by leveraging website features.

Sub-Objectives:

Real-Time Detection

Model Optimization

User-Friendly Interface

Abnormal Based Features:

Request URL
URL of Anchor
Links in <Meta>, <Script>, and <Link> tags
Server Form Handler (SFH)
Submitting Information to Email
Abnormal URL

HTML and JavaScript based Features

Website Forwarding
Status Bar Customization
Disabling Right Click
Using Pop-up Window
IFrame Redirection

Domain based Features:

Age of Domain
DNS Record
Website Traffic
PageRank
Google Index
Number of Links Pointing to Page
Statistical-Reports Based Feature

Current Progress

Utilized four machine learning algorithms, namely K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Random Forest, and Decision Tree, for website phishing classification.

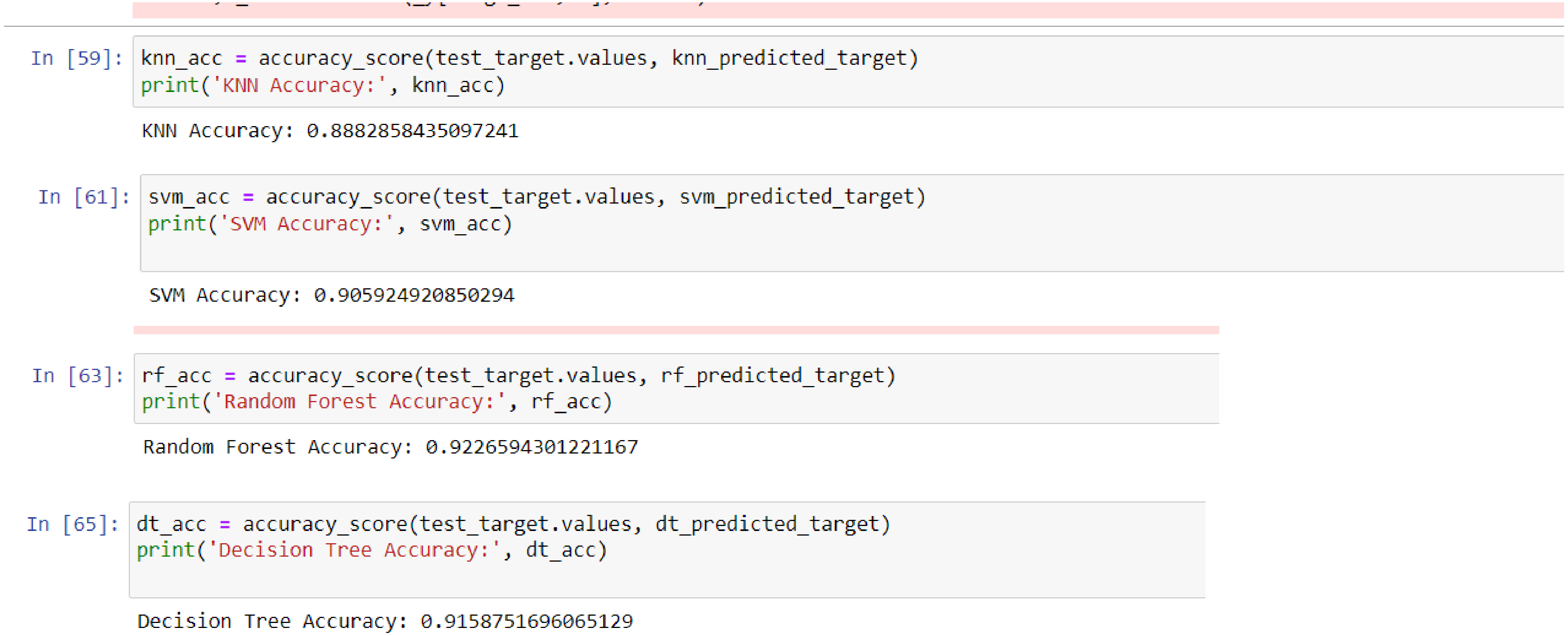
Trained each model using the training data and the corresponding target labels.

Evaluated the performance of each model by predicting the target labels for the testing data.

Calculated the accuracy score for each model using the predicted labels and the actual target labels.

Selected the model with the highest accuracy score as the final model.

Trained models



```
In [59]: knn_acc = accuracy_score(test_target.values, knn_predicted_target)
         print('KNN Accuracy:', knn_acc)

         KNN Accuracy: 0.8882858435097241

In [61]: svm_acc = accuracy_score(test_target.values, svm_predicted_target)
         print('SVM Accuracy:', svm_acc)

         SVM Accuracy: 0.905924920850294

In [63]: rf_acc = accuracy_score(test_target.values, rf_predicted_target)
         print('Random Forest Accuracy:', rf_acc)

         Random Forest Accuracy: 0.9226594301221167

In [65]: dt_acc = accuracy_score(test_target.values, dt_predicted_target)
         print('Decision Tree Accuracy:', dt_acc)

         Decision Tree Accuracy: 0.9158751696065129
```

Future Plans

1

Research and select a suitable browser extension framework, such as Chrome Extensions or Firefox Add-ons, to build the phishing detection extension.

2

Design and develop the user interface (UI) for the extension, ensuring it is intuitive and user-friendly.

3

Implement the necessary functionality to integrate the machine learning models into the extension, enabling real-time phishing detection.

References

[1] "PHISHING ACTIVITY TRENDS REPORT," APWG, 2022.

[2] "PHISHING ACTIVITY TRENDS REPORT 3rd Quarter 2022," APWG.

[3] Samaneh Mahdavifar, Nasim Maleki, Arash Habibi Lashkari, Matt Broda, Amir H. Razavi, "Classifying Malicious Domains using DNS Traffic Analysis," 2021.

[4] Wesam Fadheel , Steve Carr, Wassnaa Al-Mawee, "On Phishing: Proposing a Traffic Behavior-Based Model to Detect, Prevent, and Classify Webpage Suspicious and Malicious Activities".

[5] Ankit Kumar Jain, B. B. Gupta, "Comparative Analysis of Features Based Machine Learning Approaches for Phishing Detection".

[6] Wesam Fadheel, Wassnaa Al-Mawee, Steve Carr, "On Phishing: URL Lexical and Network Traffic Features Analysis and Knowledge Extraction using Machine Learning Algorithms (A Comparison Study)".

[7] Syifa Maliah Rachmawati, Dong-Seong Kim, and Jae-Min Lee, "Machine Learning Algorithm in Network Traffic Classification".

[8] Kai Lei†,‡, Qiuai Fu†,‡, Jiake Ni†, Feiyang Wang†, Min Yang¶, Kuai Xu§, "Detecting Malicious Domains with Behavioral Modeling and Graph Embedding".

[9] Rami M. Mohammad, Fadi Thabtah,Lee McCluskey, "Phishing Website Features".

IT20050108 | S. P. J. YAPA

BSc (Hons) Degree in Information Technology (Specialization in Cyber Security)

SLIIT
FACULTY OF COMPUTING

COMPONENT 3 - PHISHING EMAIL DETECTION WITH SENTIMENT ANALYSIS

WHAT IS PHISHING ?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

EMAIL PHISHING

A phishing email is a fraudulent message sent by cybercriminals who attempt to deceive recipients into revealing sensitive information, such as usernames, passwords, credit card numbers, or personal details. The attackers disguise themselves as a trustworthy entity, such as a bank, an online service provider, a government agency, or a well-known company, in order to trick recipients into believing that the email is legitimate.

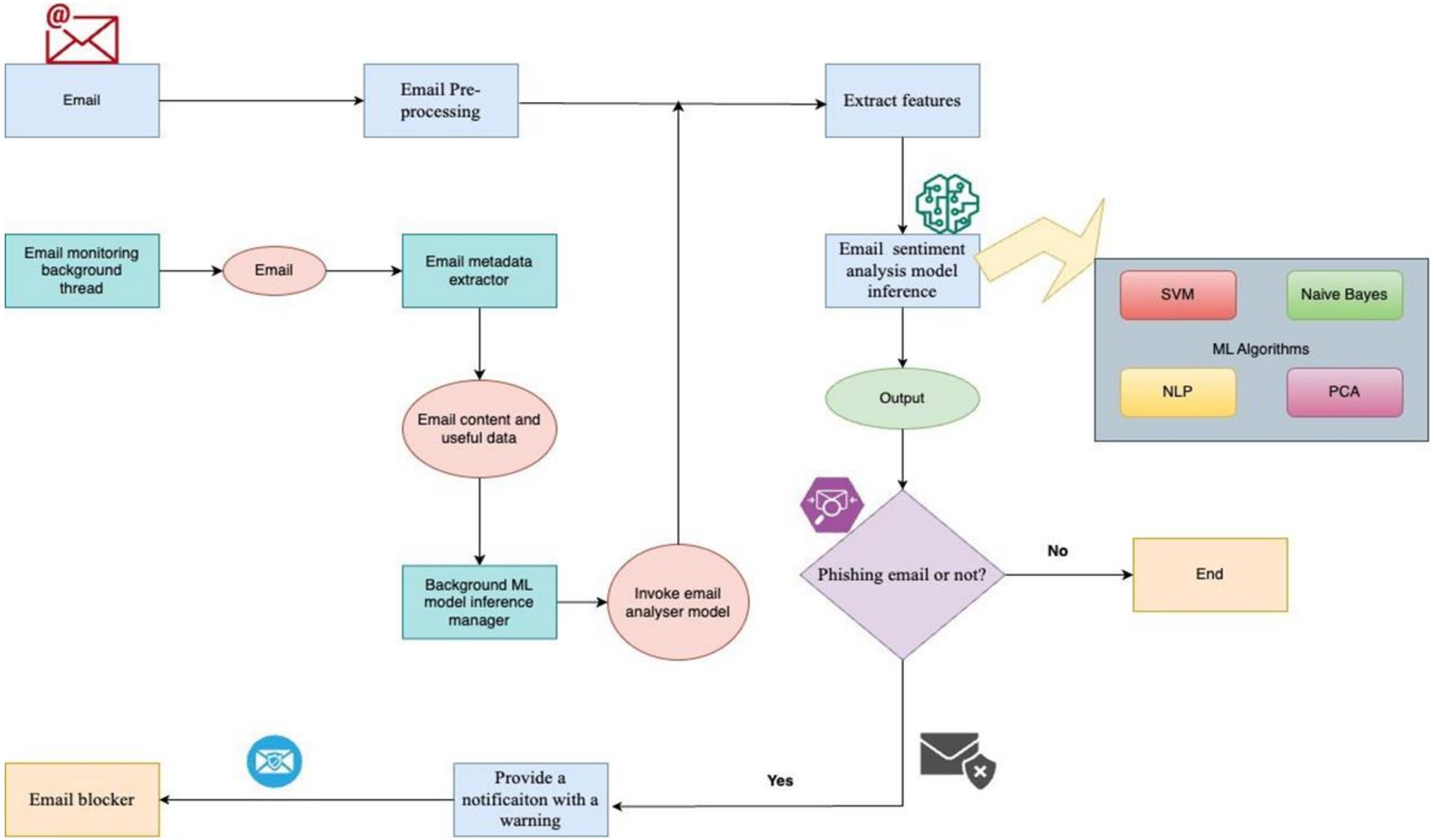
SENTIMENT ANALYSIS

Sentiment analysis, also known as opinion mining, is a natural language processing (NLP) technique used to determine and extract the sentiment or emotion expressed in a piece of text. It aims to understand whether a given text expresses a positive, negative, or neutral sentiment.

RESEARCH PROBLEM

- How to use datasets that have large number of features
- Detect phishing emails that in multiple languages.
- How to use sentiment analysis for detect phishing emails.
- How to make the email blocker to auto block the phishing email sender

SYSTEM DIAGRAM


Email
Email Pre-processing
Extract features
Email monitoring background thread
Email
Email metadata extractor
Email sentiment analysis model inference
SVM
Naive Bayes
ML Algorithms
NLP
PCA
Output
Email content and useful data
Phishing email or not?
No
End
Background ML model inference manager
Invoke email analyser model
Yes
Email blocker
Provide a notificaiton with a warning

SLIIT
FACULTY OF COMPUTING

OBJECTIVES

- ❖ Detect emotion of the text using sentiment analysis.
- ❖ Improve the model to detect multiple languages.
- ❖ Make an email blocker to auto block the phishing email sender.
- ❖ Integrate the developed models to a mobile application.

REQUIREMENTS

Software Requirements

VS Code
Jupiter Notebook
Google CoLab

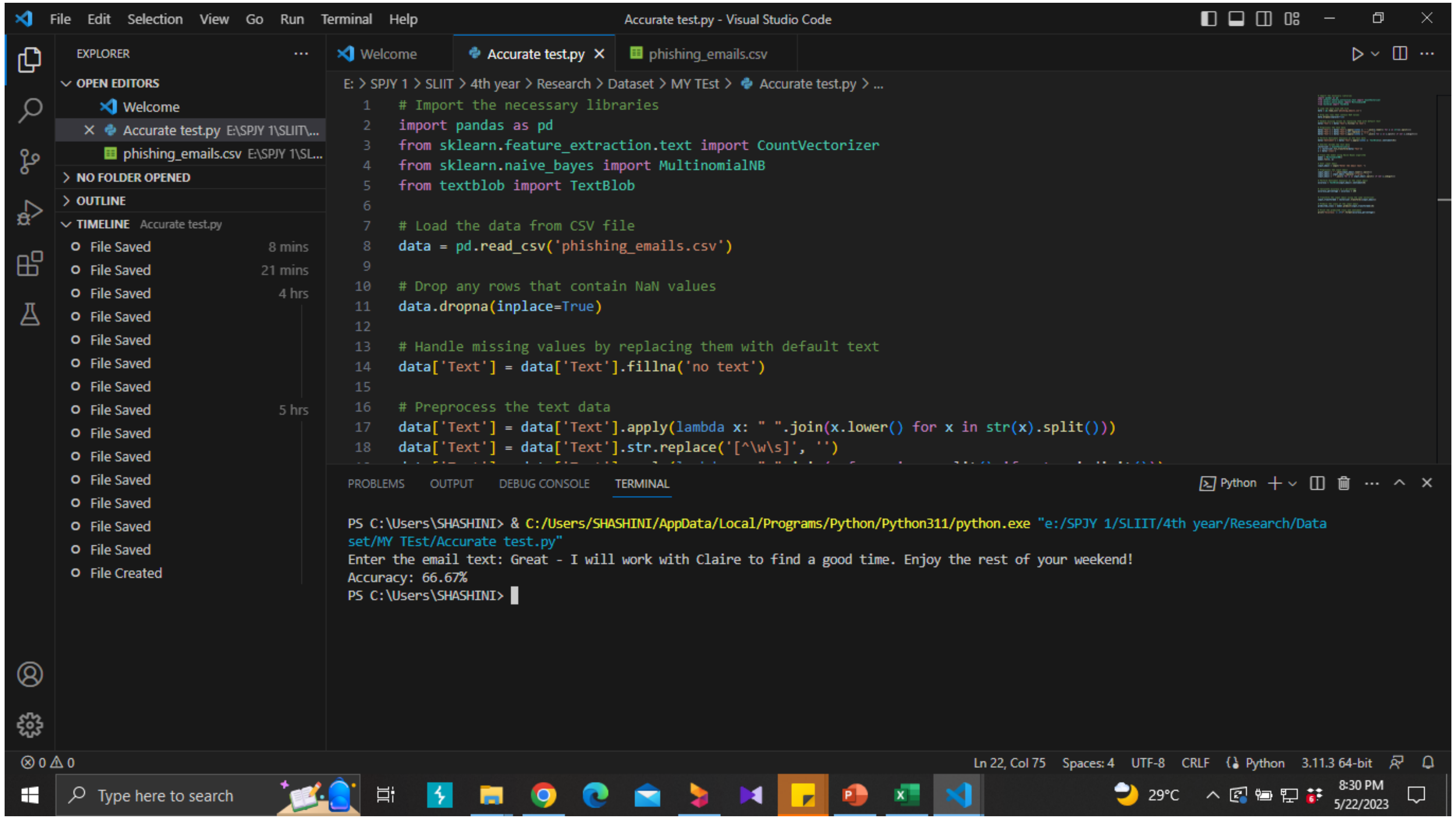
Algorithms

Naive Bayes
Random Forest
Natural Language Processing (NLP)

Techniques

Machine Learning
Sentiment Analysis
Model Training
One hot encoding

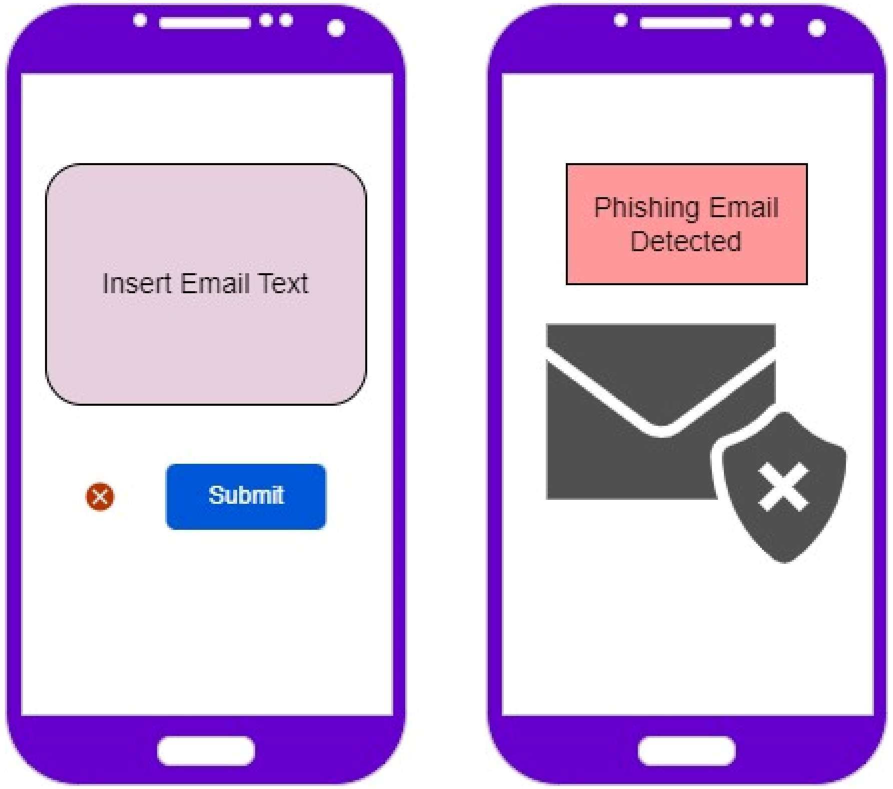
CURRENT PROGRESS



```python
# Import the necessary libraries
import pandas as pd
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.naive_bayes import MultinomialNB
from textblob import TextBlob

# Load the data from CSV file
data = pd.read_csv('phishing_emails.csv')

# Drop any rows that contain NaN values
data.dropna(inplace=True)

# Handle missing values by replacing them with default text
data['Text'] = data['Text'].fillna('no text')

# Preprocess the text data
data['Text'] = data['Text'].apply(lambda x: " ".join(x.lower() for x in str(x).split()))
data['Text'] = data['Text'].str.replace('[^\w\s]', '')
```

```
PS C:\Users\SHASHINI> & C:/Users/SHASHINI/AppData/Local/Programs/Python/Python311/python.exe "e:/SPJY 1/SLIIT/4th year/Research/Data
set/MY TEst/Accurate test.py"
Enter the email text: Great - I will work with Claire to find a good time. Enjoy the rest of your weekend!
Accuracy: 66.67%
PS C:\Users\SHASHINI> 
```

FUTURE WORK



REFERENCES

[1] Tanusree Sharma, Priscilla Ferronato, and Masooda Bashir, Phishing Email Detection Method: Leveraging Data Across Different Organizations
[2] Duo Pan, Ellen Poplavska, Yichen Yu, Susan Strauss, Shomir Wilson, A Multilingual Comparison of Email Scams, 2020
[3] Enaitz ezpeleta, iñaki velez de mendiz abal, josé maría gómez hidalgo, urko zurutuza , Novel email spam detection method using sentiment analysis and personality recognition, 14 January 2020
[4] Tanusree Sharma and Masooda Bashir, An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited, 2020
[5] Sikha Bagui, Debarghya Nandi, Subhash Bagui and Robert Jamie White, Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding, 2021
[6] Ala Mughaid, Shadi AlZu'bi, Adnan Hnaif, Salah Taamneh, Asma Alnajjar, Esraa Abu Elsoud, An intelligent cyber security phishing detection system using deep learning techniques, 14 May 2022
[7] C.J. Hutto, Eric Gilbert, VADER: A Parsimonious Rule-based Model for Sentiment Analysis of Social Media Text
[8] Said salloum, tarek gaber, sunil vadera, and khaled shaalan, A systematic literature review on phishing email detection using natural language processing techniques, 2022
[9] Srishti Rawal, Bhuvan Rawal, Aakhila Shaheen, Shubham Malik, Phishing Detection in E-mails using Machine Learning, 2017
[10] Rakesh Verma and Nabil Hossain, Semantic Feature Selection for Text with Application to Phishing Email Detection
[11] Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding - Sikha Bagui, Debarghya Nandi, Subhash Bagui and Robert Jamie White 2021

IT20222468 |I.S.S. Perera

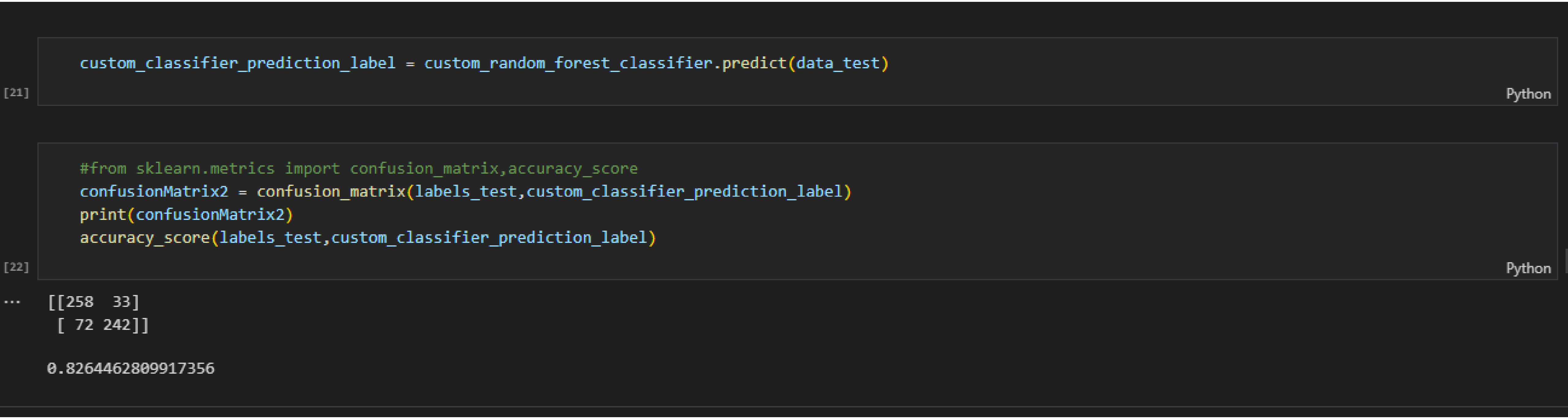
BSc (Hons) Degree in Information Technology (specialization in Cyber Security)

Research Problem

How to detect phishing web sites using machine learning URL based

Objectives

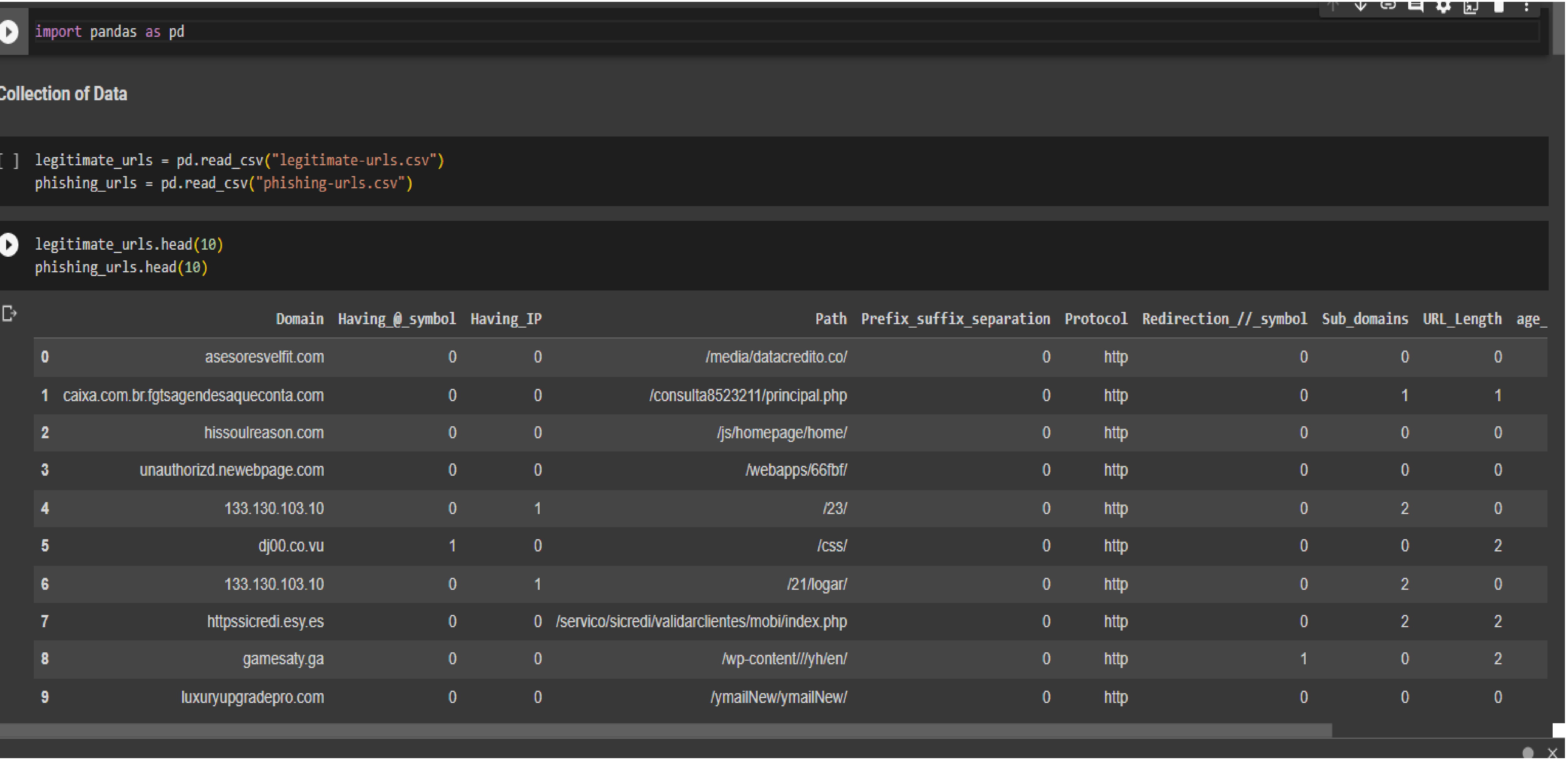
- Investigate the effectiveness of different URL features for phishing website detection. ✓
- Evaluate the performance of different machine learning algorithms for phishing website detection using URL features. ✓
- Design an optimized machine learning model that can achieve high accuracy and efficiency in detecting phishing websites using URL features. ✓
- Compare the performance of the proposed model with existing state-of-the-art phishing website detection methods.
- Made URL blocker to block the Pshing URLs



```
custom_classifier_prediction_label = custom_random_forest_classifier.predict(data_test)
```

```
#from sklearn.metrics import confusion_matrix,accuracy_score
confusionMatrix2 = confusion_matrix(labels_test,custom_classifier_prediction_label)
print(confusionMatrix2)
accuracy_score(labels_test,custom_classifier_prediction_label)
```

```
[[258  33]
 [ 72 242]]

0.8264462809917356
```



```python
import pandas as pd
```

Collection of Data

```python
legitimate_urls = pd.read_csv("legitimate-urls.csv")
phishing_urls = pd.read_csv("phishing-urls.csv")
```

```python
legitimate_urls.head(10)
phishing_urls.head(10)
```

	Domain	Having_@_symbol	Having_IP	Path	Prefix_suffix_separation	Protocol	Redirection_//_symbol	Sub_domains	URL_Length	age_
0	asesoresvelfit.com	0	0	/media/datacredito.co/	0	http	0	0	0	
1	caixa.com.br.fgtsagendesaqueconta.com	0	0	/consulta8523211/principal.php	0	http	0	1	1	
2	hissoulreason.com	0	0	/js/homepage/home/	0	http	0	0	0	
3	unauthorizd.newebpage.com	0	0	/webapps/66fbf/	0	http	0	0	0	
4	133.130.103.10	0	1	/23/	0	http	0	2	0	
5	dj00.co.vu	1	0	/css/	0	http	0	0	2	
6	133.130.103.10	0	1	/21/logar/	0	http	0	2	0	
7	httpssicredi.esy.es	0	0	/servico/sicredi/validarclientes/mobi/index.php	0	http	0	2	2	
8	gamesaty.ga	0	0	/wp-content///yh/en/	0	http	1	0	2	
9	luxuryupgradepro.com	0	0	/ymailNew/ymailNew/	0	http	0	0	0	

Current progress

Datasets

Experimented with two most recent datasets.

- 1000 phishing
  - Contain1000 phishing URLS.

- Legitimate URLS
  - More than 100 legitimate URLS

REFERENCES

- https://www.trendmicro.com/en_hk/what-is/phishing/types-of-phishing.html. [Online].
- https://www.sciencedirect.com/science/article/pii/S1319157823000034. [Online].
- P. D. a. P. u. C. Extension.
- U. P. D. u. M. Learning.
- M. L. A. E. f. P. U. Classification.
- Machine learning based phishing detection from URLs Koray Sahingoz a, Ebubekir Buber b, Onder Demir b, Banu Diri c
- Phishing Website Detection using Machine Learning Algorithms Rishikesh Mahajan Irfan Siddavatam
- Somaiya Vidyavihar