DETECTING EMAIL-BASED PHISHING WEBSITES USING MACHINE LEARNING

2023-123

Team Members

J.M.Lindamulage

Mandira Pabasari L.

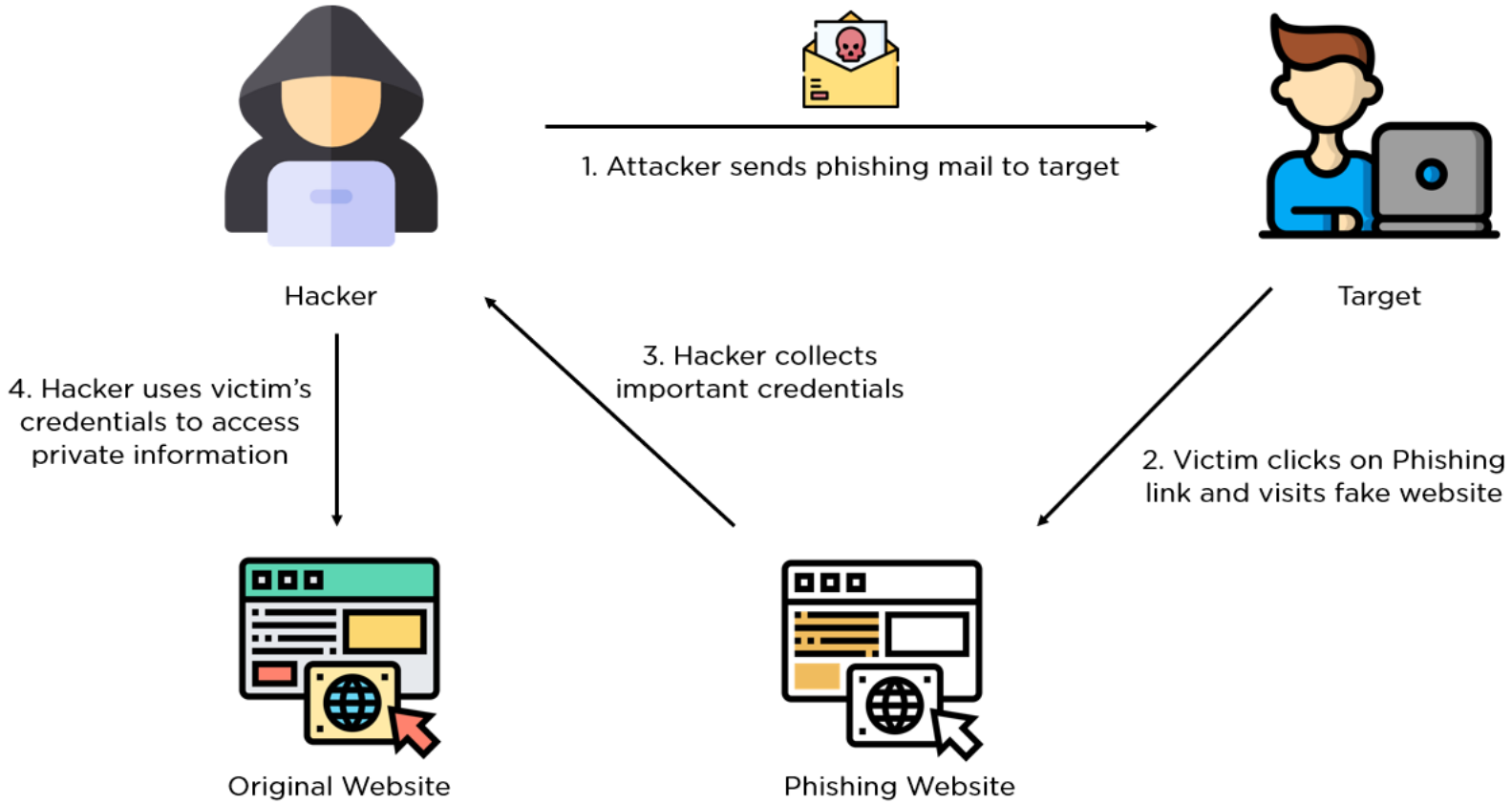
Yapa S.P.J.

Perera I.S.S.

RESEARCH QUESTION

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

Introduction



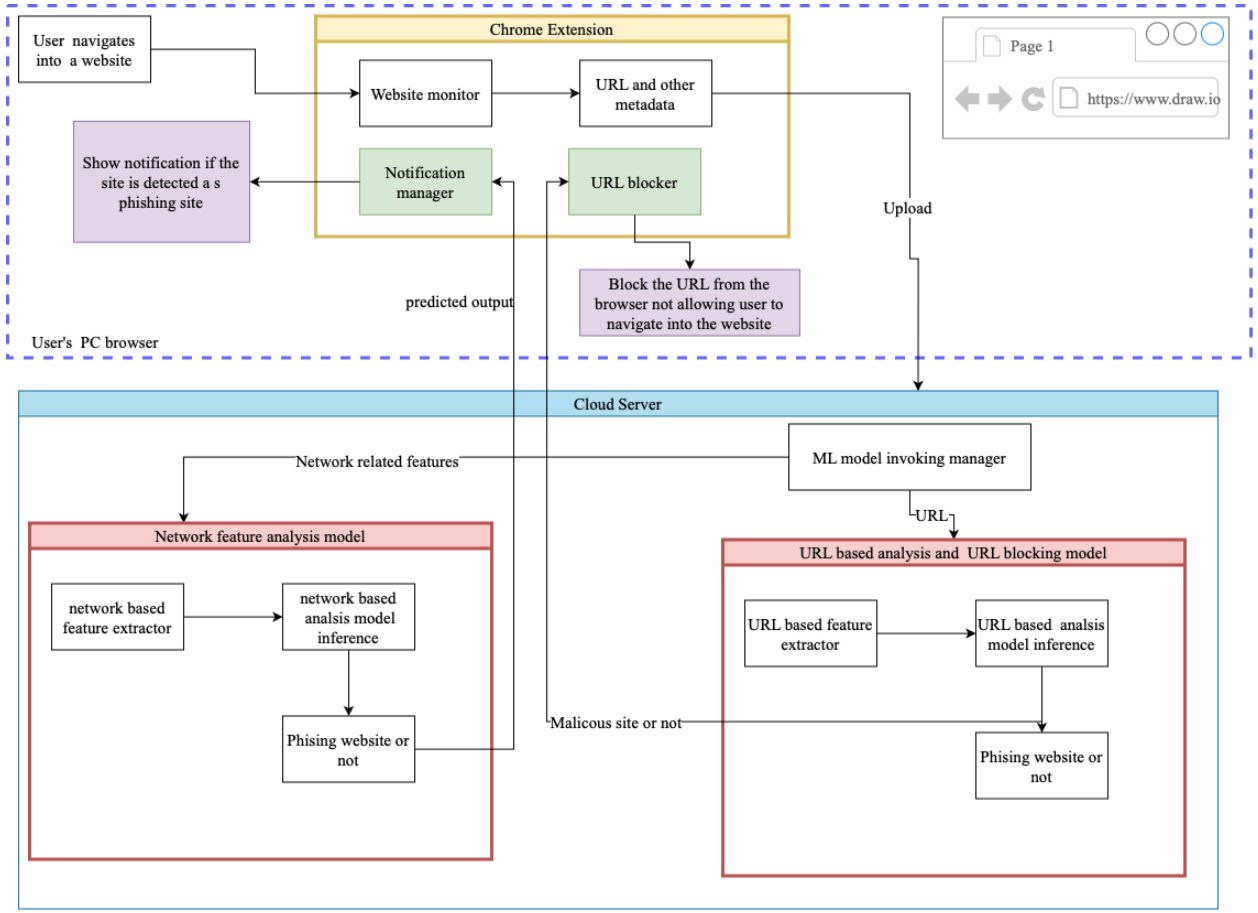
Main Objective

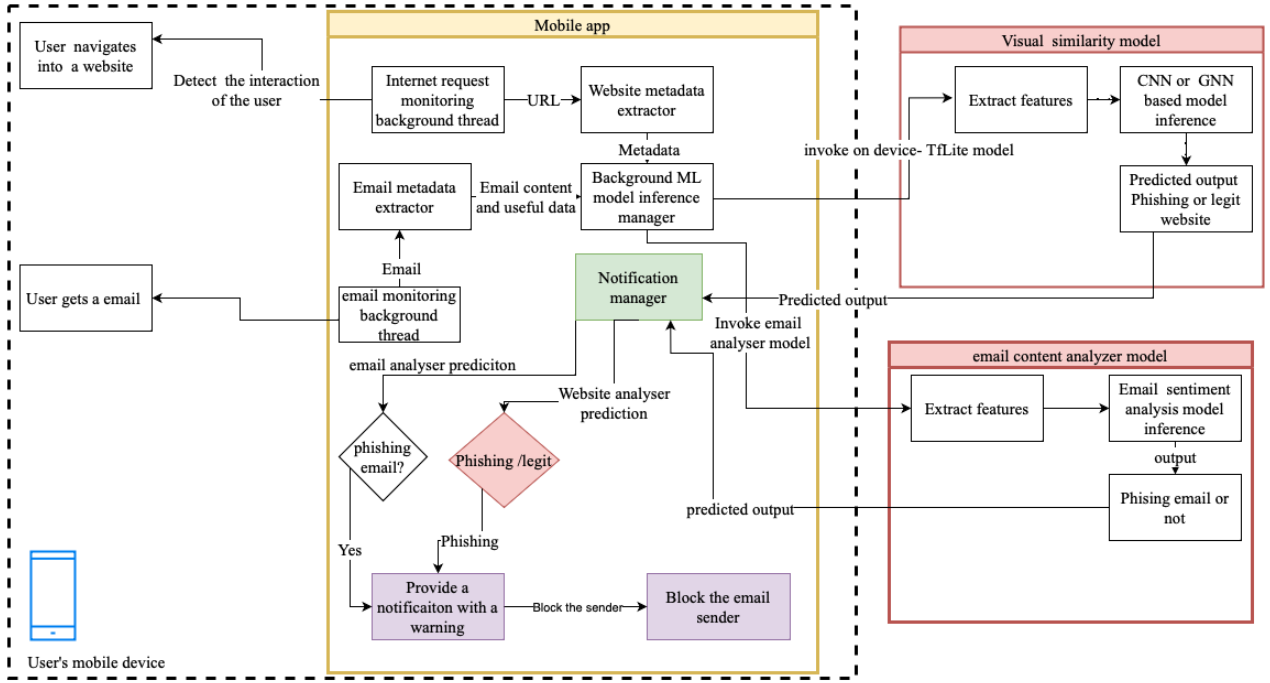
To implement a mobile application and a web extension capable of detecting phishing emails and websites utilizing machine learning and deep learning models.

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.

system diagram





IT20222840 |Judith Malshini L.

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

RESEARCH PROBLEM

How to use visual similarity features of a website to detect if a website is a phishing website or a legitimate website

Objectives

- To utilize Vision GNN for the first time for classifying phishing websites.
  - Vision GNN: An Image is Worth Graph of Nodes(2022)
  - Was trained on ImageNet dataset.
- To optimize the developed model for mobile devices.
- To deploy the deep learning model on android mobile app.

Contributions

Introduced VisionGNN architecture based on Graph neural networks into phishing website classification for the first time

Utilized visual features alone with graph neural network representations for the first time.

Implemented a mobile app to detect phishing websites using a screenshot of the page.

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)

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

Dataset

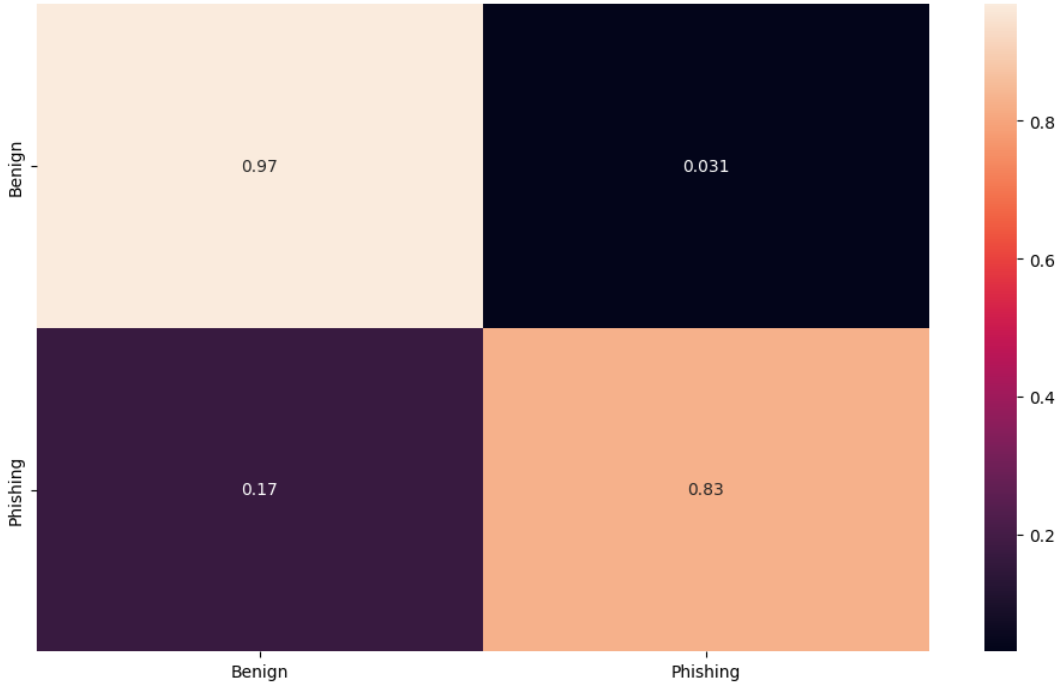
- Visual phish dataset
  - Contain 9363 screenshots of PhishTank phishing pages that target 155 websites and 1195 phishing pages.
- 4072 data were divided into train and test with 20% split.
- Train data-3054
- Test data-1018

Model results

Model	No of parameters(10^6)	Accuracy(100)
Tiny	9.69	93.5
Small	26.23	97.4
Medium	48.50	91.8
Large	91.96	93.5

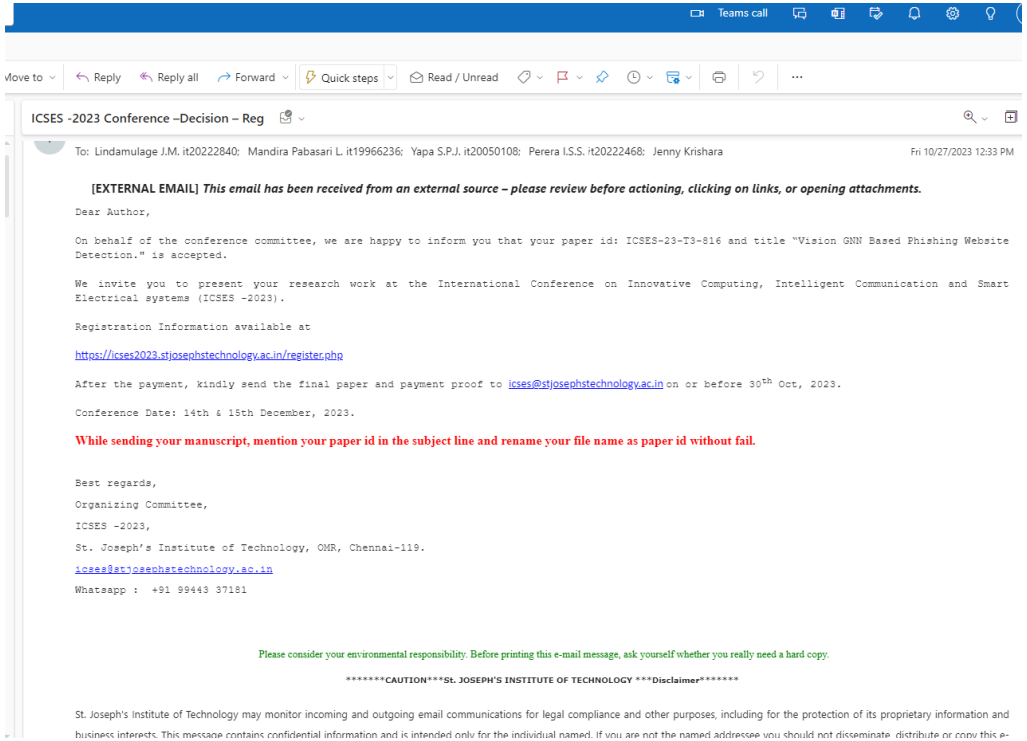
Maxium accuracy 97.4% in small model with 26.23 x 10^6 parameters

83% phishing sites detected
97% beign sites are correctly classified



Vision GNN Based Phishing Website Detection

Paper was accepted for the International Conference on Innovative Computing, Intelligent Communication and Smart Electrical systems (ICSES -2023).
H-Index-10



Teams call

Move to | Reply | Reply all | Forward | Quick steps | Read / Unread

ICSES -2023 Conference –Decision – Reg

To: Lindamulage J.M. it20222840; Mandira Pabasari L. it19966236; Yapa S.P.J. it20050108; Perera I.S.S. it20222468; Jenny Krishara

Fri 10/27/2023 12:33 PM

[EXTERNAL EMAIL] ***This email has been received from an external source – please review before actioning, clicking on links, or opening attachments.***

Dear Author,

On behalf of the conference committee, we are happy to inform you that your paper id: ICSES-23-T3-816 and title "Vision GNN Based Phishing Website Detection." is accepted.

We invite you to present your research work at the International Conference on Innovative Computing, Intelligent Communication and Smart Electrical systems (ICSES -2023).

Registration Information available at

https://icses2023.stjosephstechnology.ac.in/register.php

After the payment, kindly send the final paper and payment proof to icses@stjosephstechnology.ac.in on or before 30th Oct, 2023.

Conference Date: 14th & 15th December, 2023.

While sending your manuscript, mention your paper id in the subject line and rename your file name as paper id without fail.

Best regards,

Organizing Committee,

ICSES -2023,

St. Joseph's Institute of Technology, OMR, Chennai-119.

icses@stjosephstechnology.ac.in

Whatsapp : +91 99443 37181

Please consider your environmental responsibility. Before printing this e-mail message, ask yourself whether you really need a hard copy.

*******CAUTION***St. JOSEPH'S INSTITUTE OF TECHNOLOGY ***Disclaimer*******

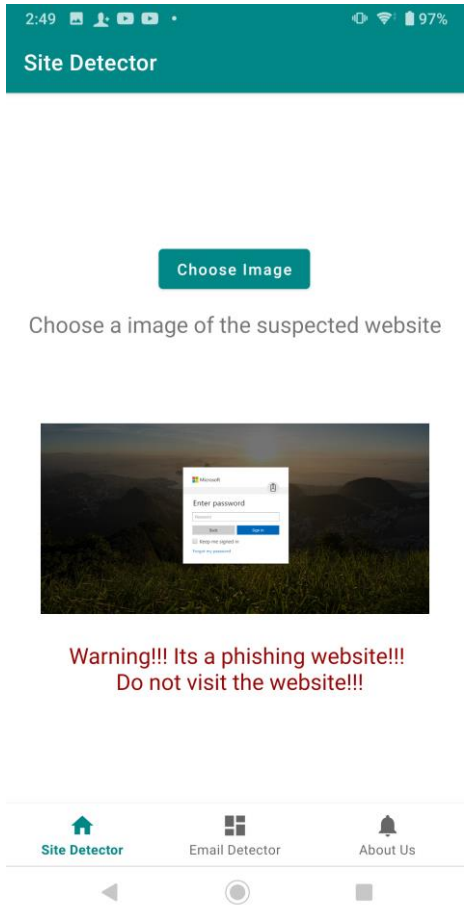
St. Joseph's Institute of Technology may monitor incoming and outgoing email communications for legal compliance and other purposes, including for the protection of its proprietary information and business interests. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-

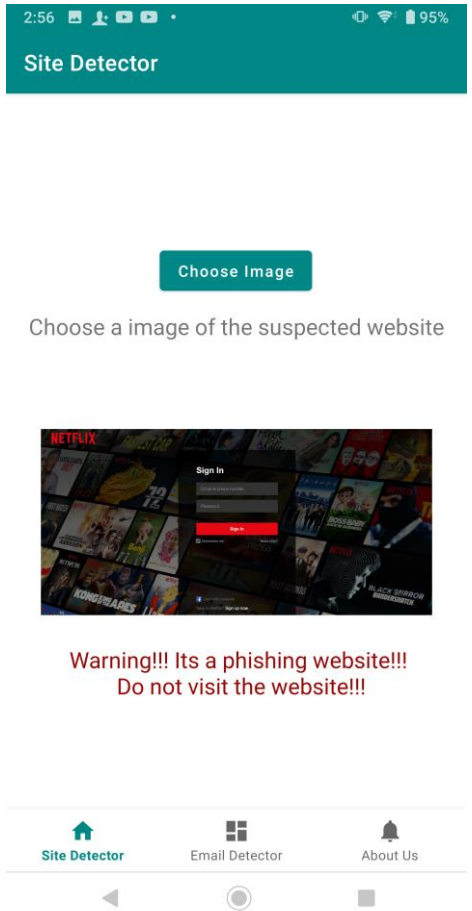
Model mobile app integration

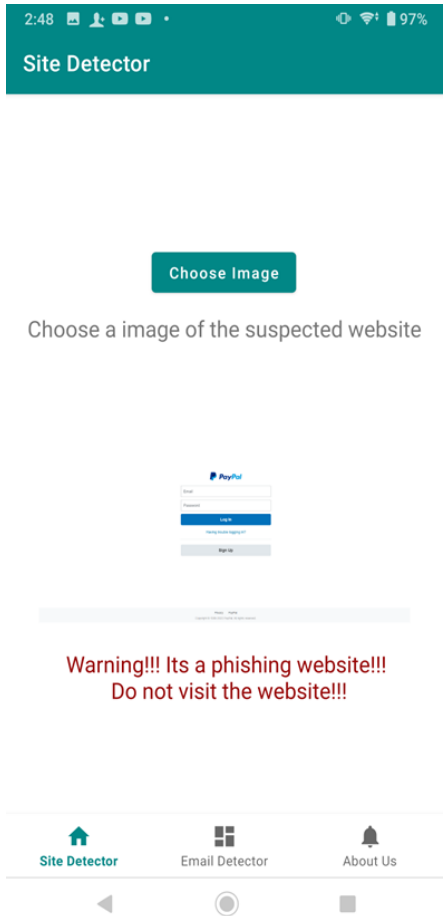
- Optimized model for edge computing using Pytorch mobile
- Converted Pytorch model into pytorch mobile
- Model works on Andorid
- Mobile app works on device without internet
- Advantages:
  - Preserves privacy of the user
  - Saves network bandwidth
  - Low latency

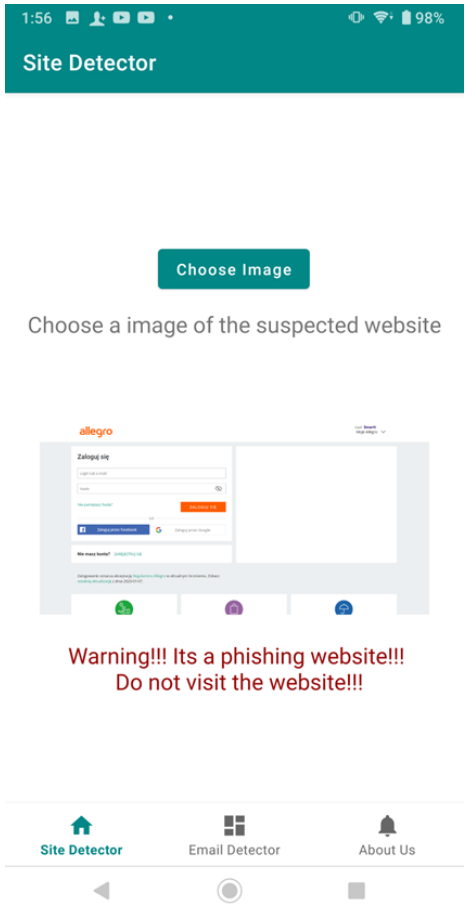
Mobile Application

Output for Phishing Websites

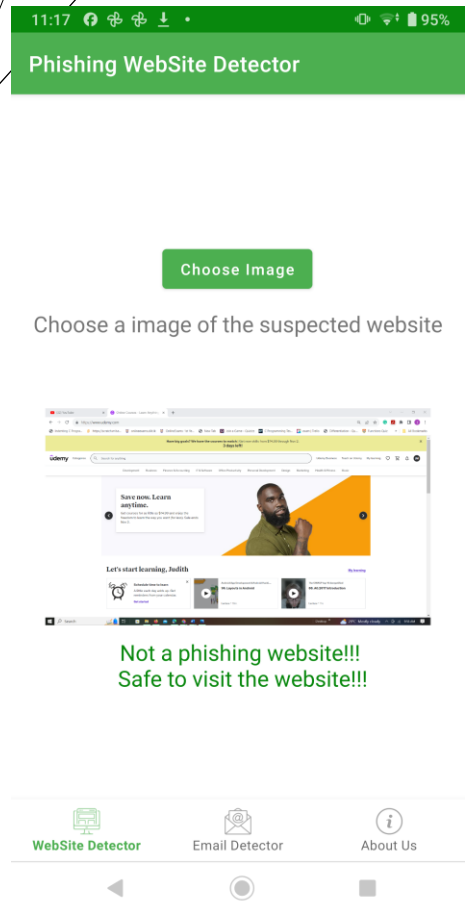


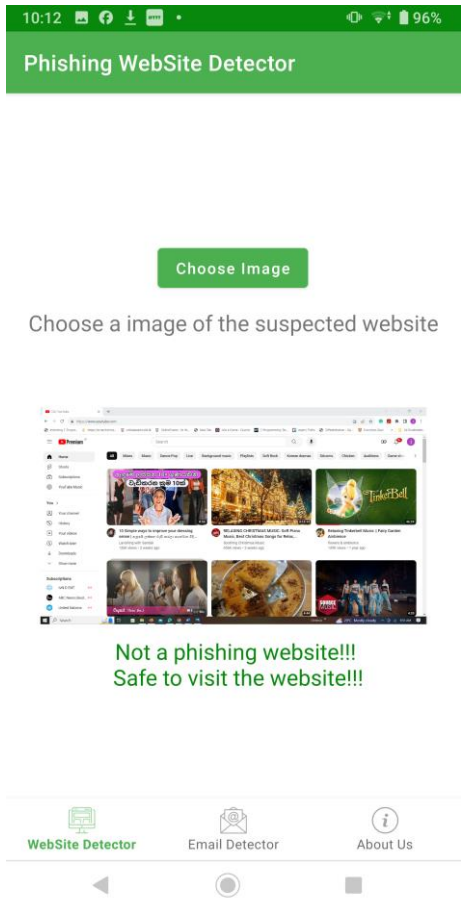


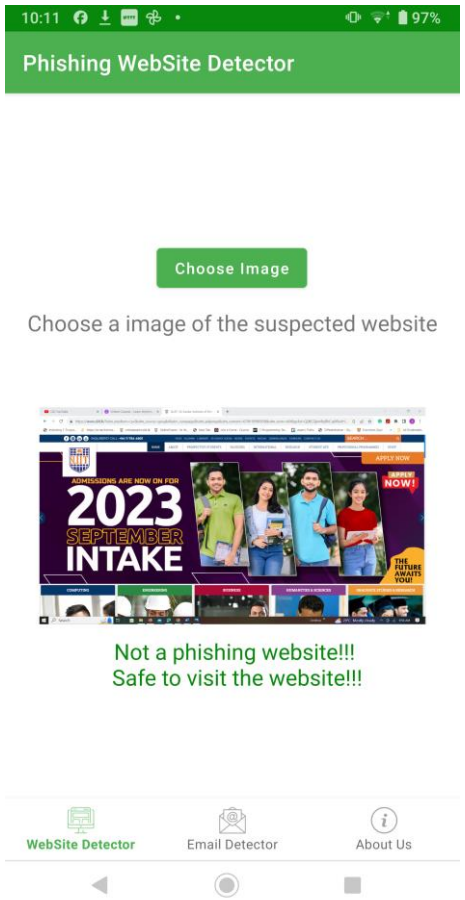


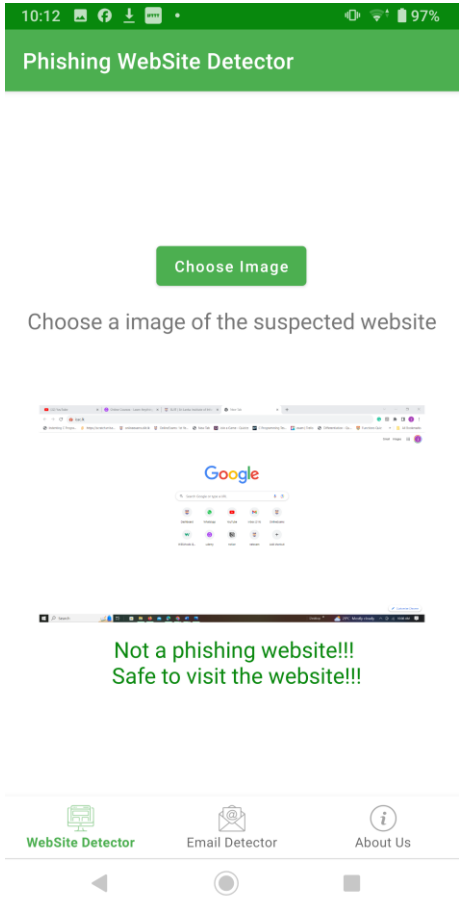


Output for real websites









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".

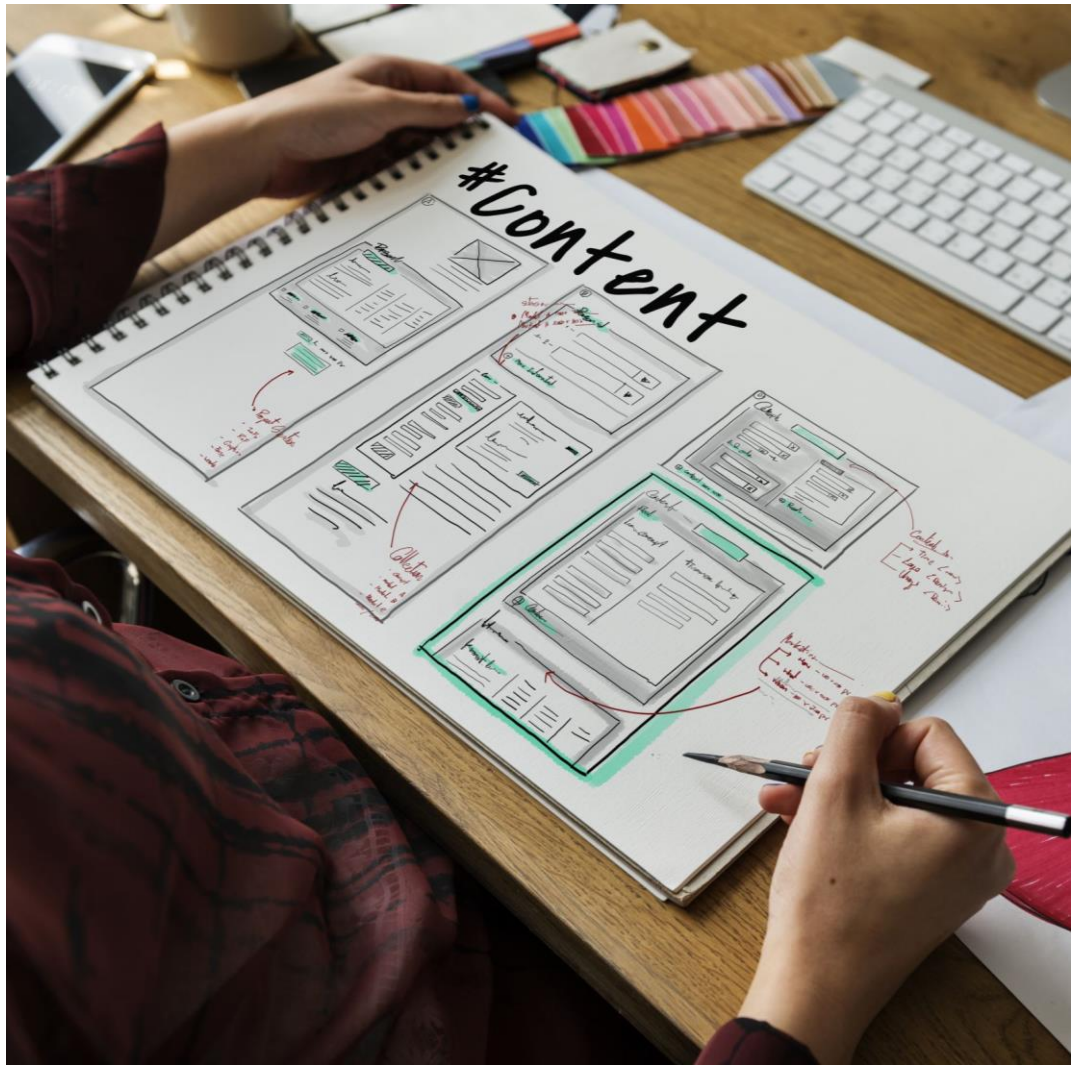
Phishing detection using website features

SLIIT FACULTY OF COMPUTING

IT19966236 | Mandira Pabasari L. | 2023-123

Research problem

- How to use features of a website to detect if a website is a phishing website or a legitimatewebsite



objectives

Emphasize website features, HTML and JavaScript attributes, and abnormal online behavior indicators.

Real time phishing detection.

Website features

- Many individual components that make a website easy to navigate, functional and valuable to users.
- Features can be divided into,
  - Address bar based features
  - Abnormal based features
  - HTML and JavaScript based features
  - Domain based features

```
Running random forests...
Accuracy = 87.43%
[[1173  255]
 [ 162 1727]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity
1173    162     255     1727    0.82
1727    255     162     1173    0.91
F1 Score: 0.8922758977008526
Runtime: 0.17 seconds
```

```
Running neural networks...
Accuracy = 87.40%
[[1172  256]
 [ 162 1727]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity
1172    162     256     1727    0.82
1727    256     162     1172    0.91
F1 Score: 0.8920454545454545
Runtime: 35.22 seconds
```

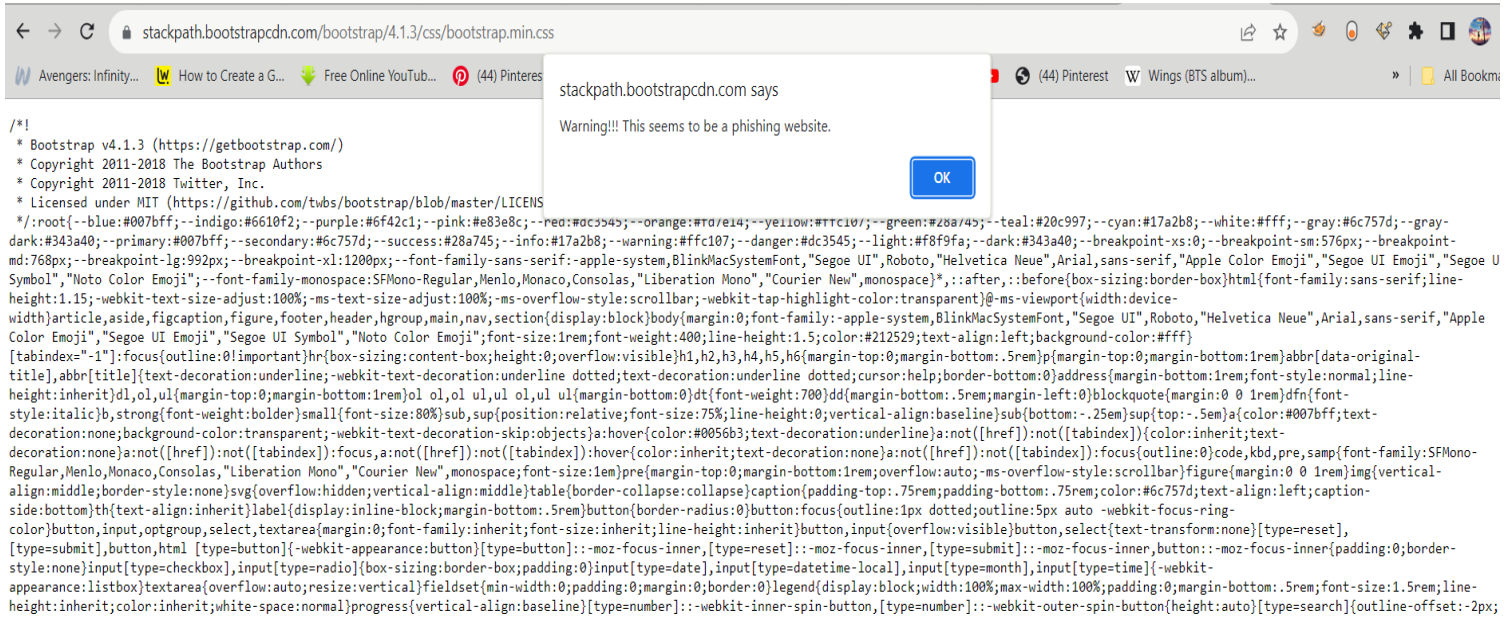
```
Running support vector machines...
Accuracy = 87.37%
[[1174  254]
 [ 165 1724]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity     Specifici
1174    165     254     1724    0.82            0.91
1724    254     165     1174    0.91            0.82
F1 Score: 0.8916472717869149
Runtime: 2.60 seconds
Total Runtime: 38.59 seconds
```

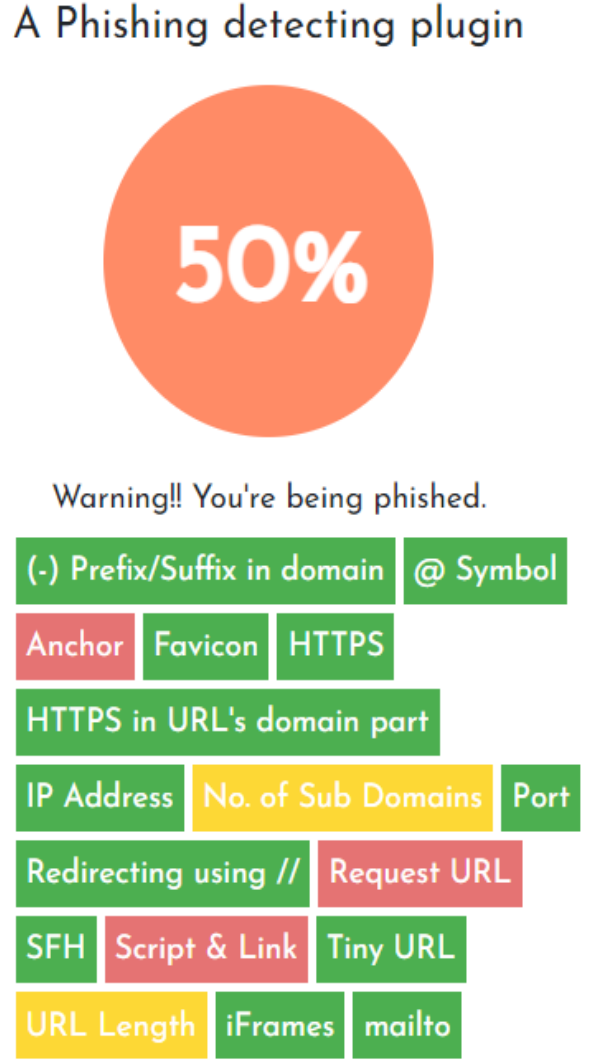
Model Selection

Model integration with Plugin

Model Training:	A machine learning model was trained to identify phishing websites.
Model Integration:	The trained model was integrated into a Chrome extension.
User Interaction:	When a user visits a website, the extension silently checks it for suspicious signs.
Data Transmission:	The extension sends these signs to the model for analysis.
Classification:	The model processes the signs and classifies the website as safe, potentially risky, or dangerous.

Results


stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css
stackpath.bootstrapcdn.com says
Warning!!! This seems to be a phishing website.
OK
/*!
* Bootstrap v4.1.3 (https://getbootstrap.com/)
* Copyright 2011-2018 The Bootstrap Authors
* Copyright 2011-2018 Twitter, Inc.
* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENS
/:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace},::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-ms-overflow-style:scrollbar;-webkit-tap-highlight-color:transparent}@-ms-viewport{width:device-width}article,aside,figcaption,figure,footer,header,hgroup,main,nav,section{display:block}body{margin:0;font-family:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";font-size:1rem;font-weight:400;line-height:1.5;color:#212529;text-align:left;background-color:#fff}
[tabindex="-1"]:focus{outline:0!important}hr{box-sizing:content-box;height:0;overflow:visible}h1,h2,h3,h4,h5,h6{margin-top:0;margin-bottom:.5rem}p{margin-top:0;margin-bottom:1rem}abbr[data-original-title],abbr[title]{text-decoration:underline;-webkit-text-decoration:underline dotted;text-decoration:underline dotted;cursor:help;border-bottom:0}address{margin-bottom:1rem;font-style:normal;line-height:inherit}dl,ol,ul{margin-top:0;margin-bottom:1rem}ol ol,ol ul,ul ol,ul ul{margin-bottom:0}dt{font-weight:700}dd{margin-bottom:.5rem;margin-left:0}blockquote{margin:0 0 1rem}dfn{font-style:italic}b,strong{font-weight:bolder}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sub{bottom:-.25em}sup{top:-.5em}a{color:#007bff;text-decoration:none;background-color:transparent;-webkit-text-decoration-skip:objects}a:hover{color:#0056b3;text-decoration:underline}a:not([href]):not([tabindex]){color:inherit;text-decoration:none}a:not([href]):not([tabindex]):focus,a:not([href]):not([tabindex]):hover{color:inherit;text-decoration:none}a:not([href]):not([tabindex]):focus{outline:0}code,kbd,pre,samp{font-family:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace;font-size:1em}pre{margin-top:0;margin-bottom:1rem;overflow:auto;-ms-overflow-style:scrollbar}figure{margin:0 0 1rem}img{vertical-align:middle;border-style:none}svg{overflow:hidden;vertical-align:middle}table{border-collapse:collapse}caption{padding-top:.75rem;padding-bottom:.75rem;color:#6c757d;text-align:left;caption-side:bottom}th{text-align:inherit}label{display:inline-block;margin-bottom:.5rem}button{border-radius:0}button:focus{outline:1px dotted;outline:5px auto -webkit-focus-ring-color}button,input,optgroup,select,textarea{margin:0;font-family:inherit;font-size:inherit;line-height:inherit}button,input{overflow:visible}button,select{text-transform:none}[type=reset],[type=submit],button,html [type=button]{-webkit-appearance:button}[type=button]::-moz-focus-inner,[type=reset]::-moz-focus-inner,[type=submit]::-moz-focus-inner,button::-moz-focus-inner{padding:0;border-style:none}input[type=checkbox],input[type=radio]{box-sizing:border-box;padding:0}input[type=date],input[type=datetime-local],input[type=month],input[type=time]{-webkit-appearance:listbox}textarea{overflow:auto;resize:vertical}fieldset{min-width:0;padding:0;margin:0;border:0}legend{display:block;width:100%;max-width:100%;padding:0;margin-bottom:.5rem;font-size:1.5rem;line-height:inherit;color:inherit;white-space:normal}progress{vertical-align:baseline}[type=number]::-webkit-inner-spin-button,[type=number]::-webkit-outer-spin-button{height:auto}[type=search]{outline-offset:-2px;


A Phishing detecting plugin
50%
Warning!! You're being phished.
(-) Prefix/Suffix in domain
@ Symbol
Anchor
Favicon
HTTPS
HTTPS in URL's domain part
IP Address
No. of Sub Domains
Port
Redirecting using //
Request URL
SFH
Script & Link
Tiny URL
URL Length
iFrames
mailto

Thank You

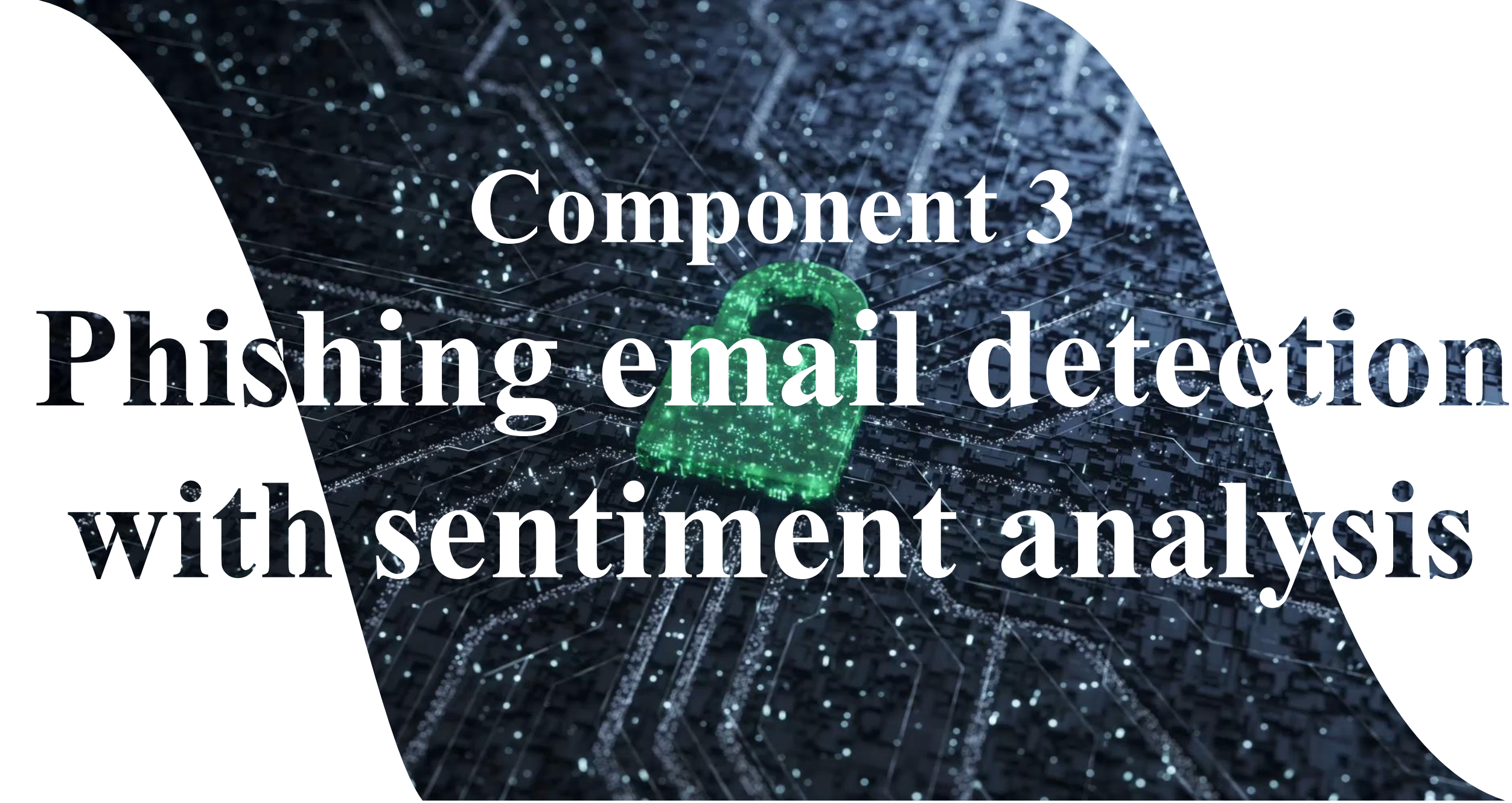
SLIIT
FACULTY OF COMPUTING

IT19966236 | Mandira Pabasari L. | 2023-123

IT20050108 | S. P. J. YAPA

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

SLIIT
FACULTY OF COMPUTING



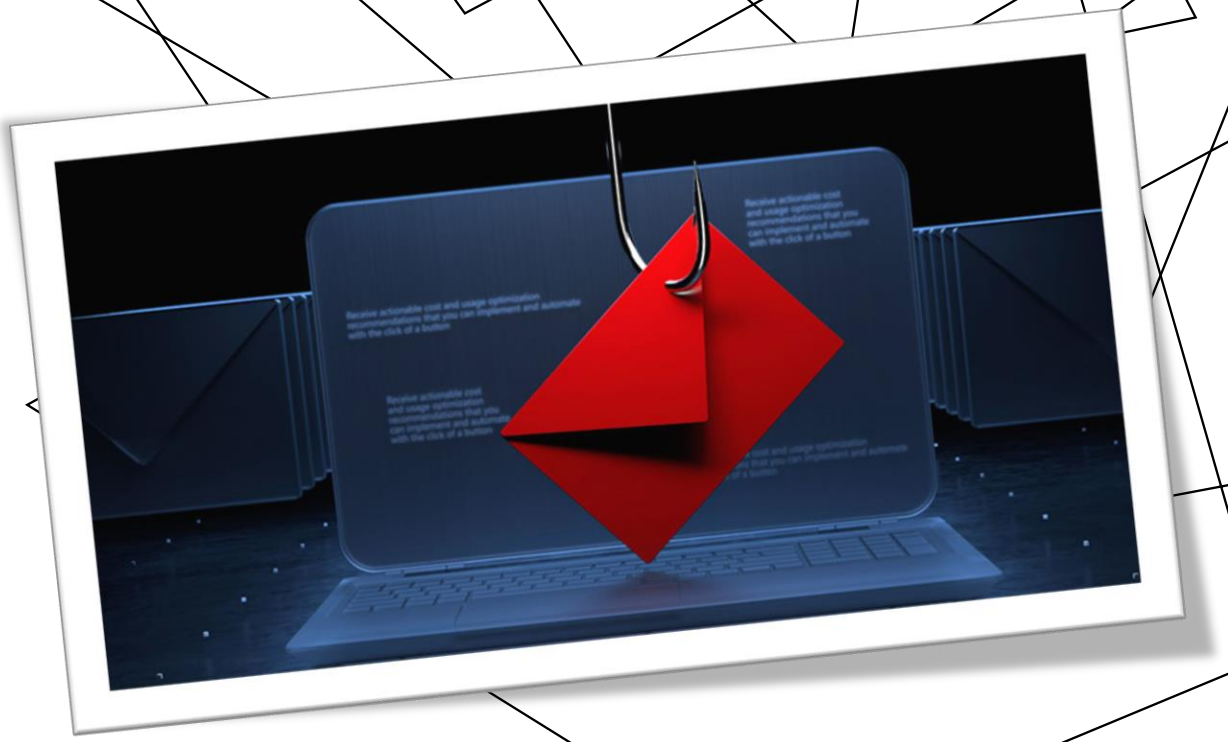
Component 3

Phishing email detection with sentiment analysis

Sentiment Analysis

- *Natural Language Processing (NLP) Technique*

- *Positive*
- *Negative*
- *Neutral sentiment*



Research Problem

- ***How to address the issue of imbalanced datasets, which can affect the accuracy of the model***
- ***Using Large dataset to train the model***
- ***How to use sentiment analysis for detect phishing emails.***
- ***Using Naive Bayes algorithm to train the model***

Objectives

- *Detect emotion of the text using sentiment analysis.*
- *Improve the model to detect the text phishing or not.*
- *Display a warning message when detect a phishing email.*
- *Integrate the developed model to a mobile application.*

Requirements

❑ *Techniques*

Machine Learning
Sentiment Analysis
Model Training

❑ *Software Requirements*

VS Code
Android Studio

❑ *Algorithms*

Naive Bayes (BernoulliNB)
Natural Language Processing (NLP)

Accuracy

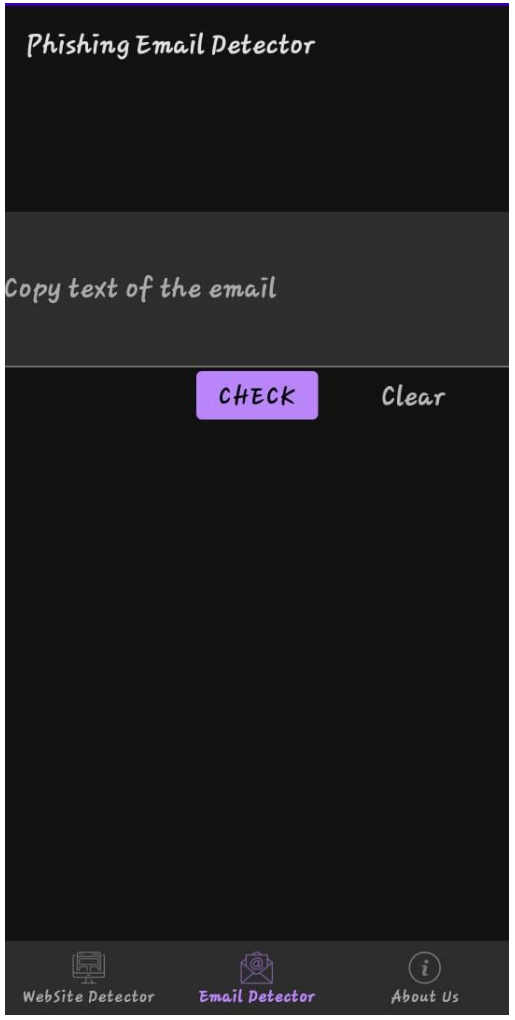
Evaluation

```
    print('confusion matrics :')
    print(confusion_matrix(y_test, y_predict), end='\n\n')

    print('accuracy ',accuracy_score(y_test, y_predict))
```

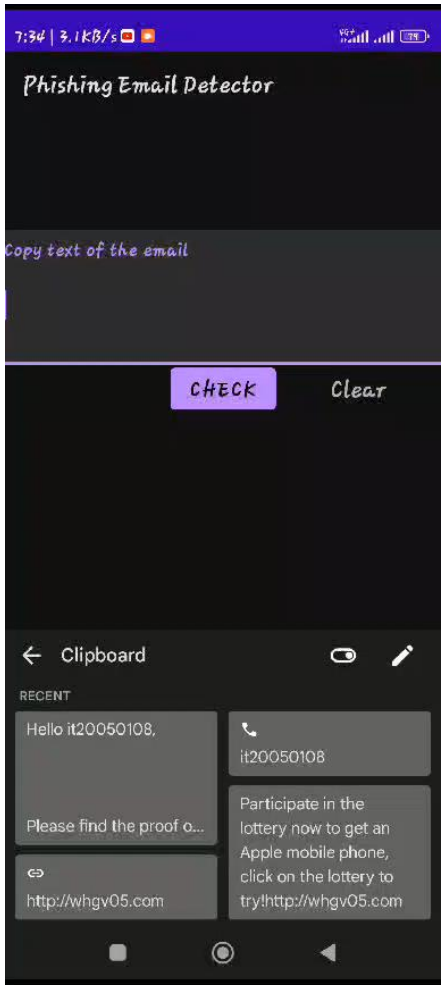
[47] ✓ 0.2s Python

```
confusion matrics :
[[1584   29]
 [ 105 2667]]

accuracy  0.9694412770809578
```

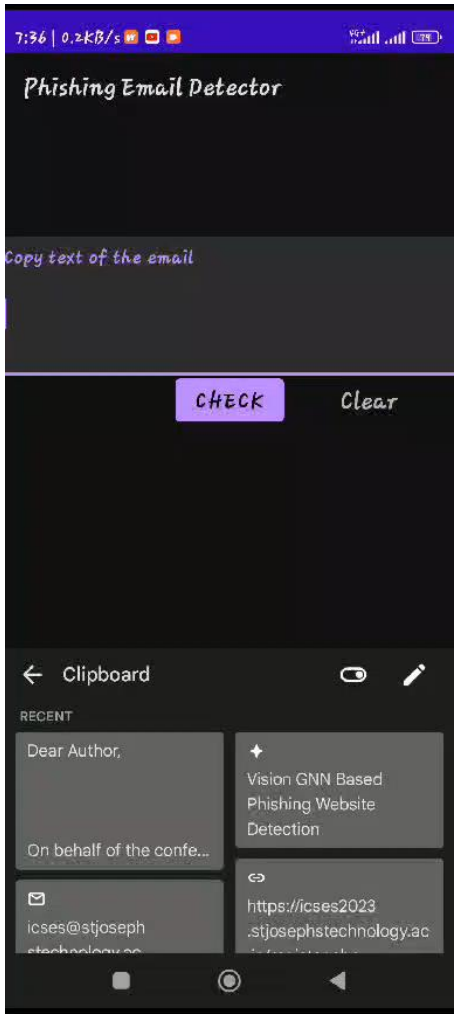
Mobile Application



Output(Phishing)



Output(Not Phishing)



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

[12] D. N. S. B. a. R. J. W. Sikha Bagui, "Machine Learning and Deep Learning for Phishing Email," Journal of Computer Science, 2021.

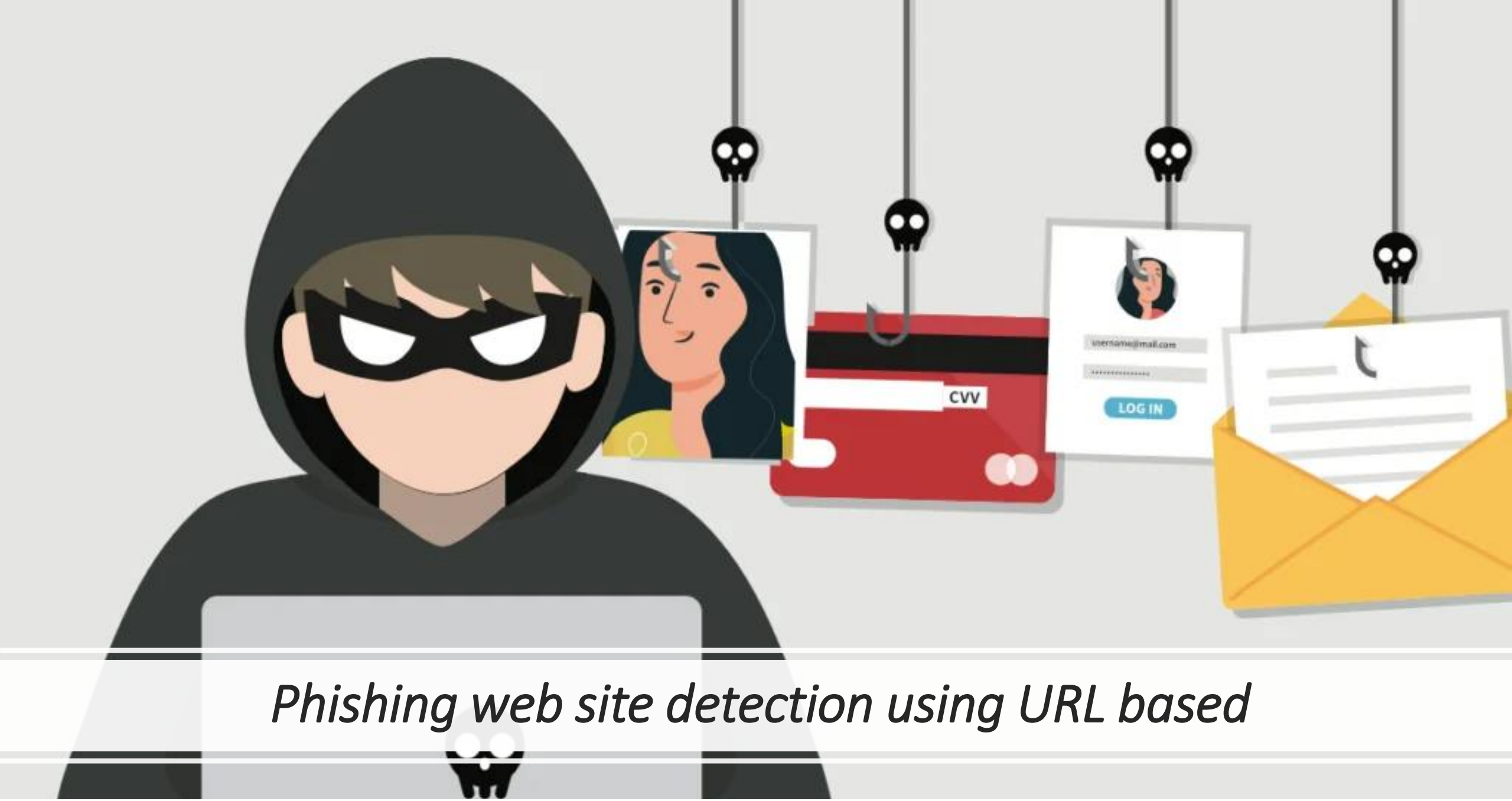
Thank You

SLIIT
FACULTY OF COMPUTING

IT20222468 | I.S.S.Perera

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

SLIIT
FACULTY OF COMPUTING



Phishing web site detection using URL based

Research problem

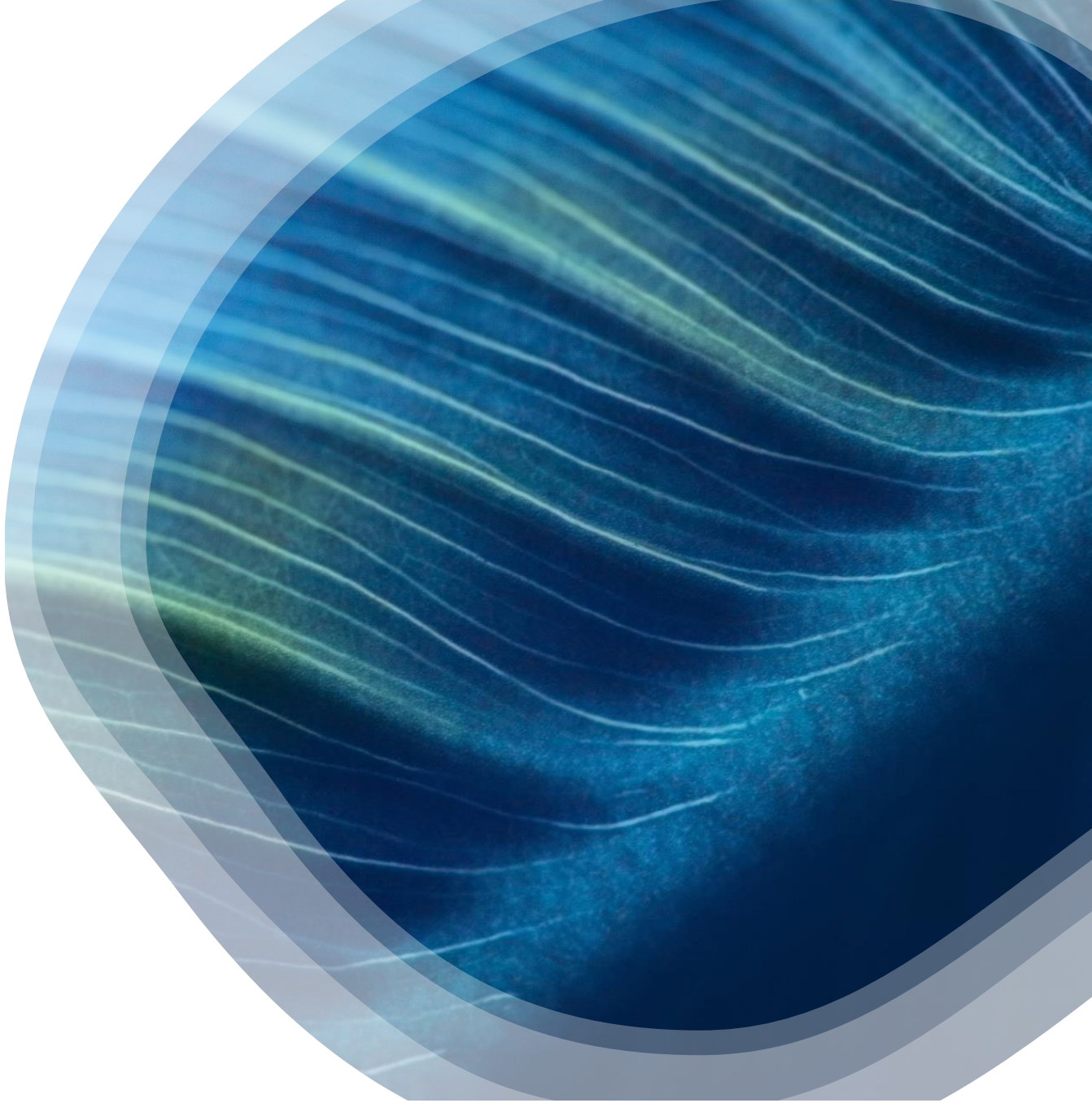
How Effective Are Machine Learning Algorithms in Detecting Phishing Websites Based on URL Features?

objectives

Creating extension for check URLS

URL blocker

Pop up message for user



URL features

- URL-based analysis is a fundamental aspect of today's digital landscape, empowering us to navigate the online world with greater security, efficiency, and confidence.
- Features can be IP Address,URL Length,Tiny URL,@ Symbol,Redirecting using //,(-) Prefix/Suffix in domain,No. of Sub Domains,HTTPS,Favicon,Using Non-Standard Port,HTTPS in URL's domain part

```
Running random forests...
Accuracy = 87.43%
[[1173  255]
 [ 162 1727]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity
1173    162     255     1727    0.82
1727    255     162     1173    0.91
F1 Score: 0.8922758977008526
Runtime: 0.17 seconds
```

```
Running neural networks...
Accuracy = 87.40%
[[1172  256]
 [ 162 1727]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity
1172    162     256     1727    0.82
1727    256     162     1172    0.91
F1 Score: 0.8920454545454545
Runtime: 35.22 seconds
```

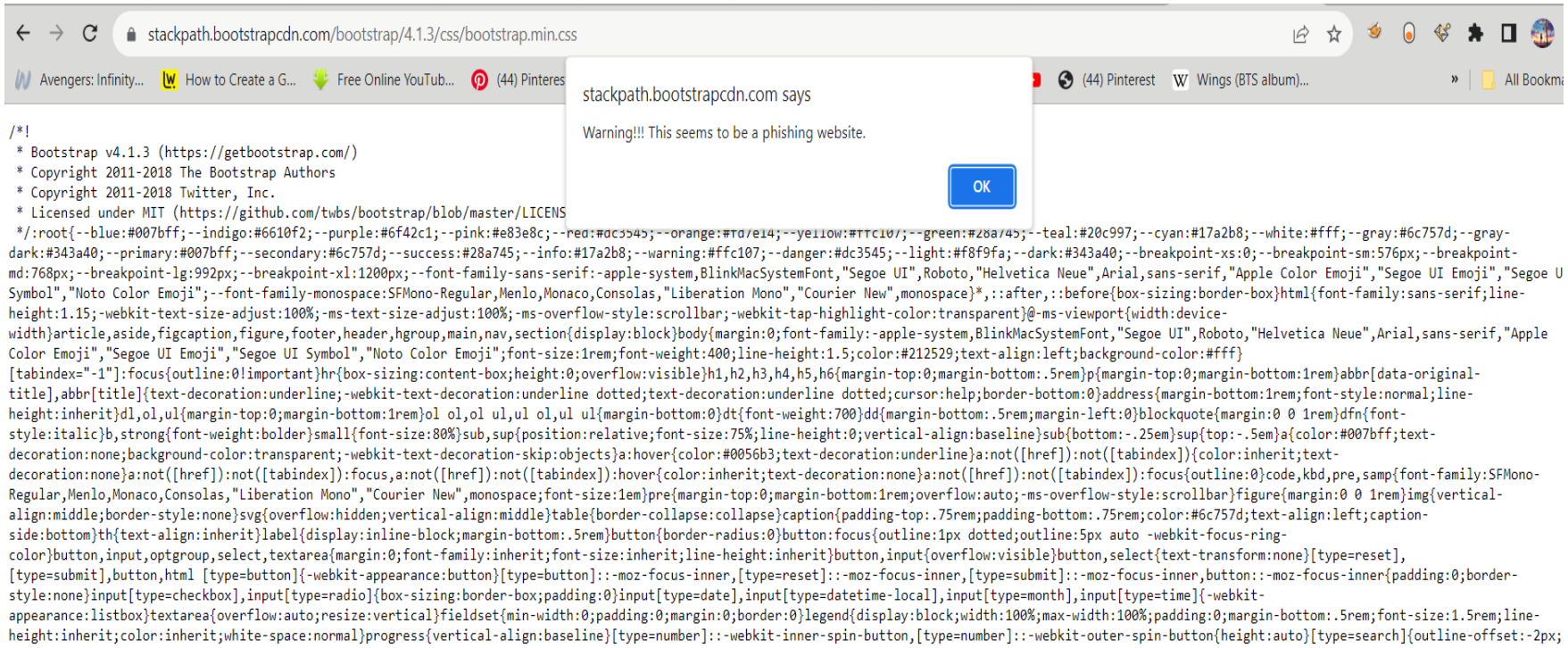
```
Running support vector machines...
Accuracy = 87.37%
[[1174  254]
 [ 165 1724]]
Confusion Matrix Shape: (2, 2)
TP      FP      FN      TN      Sensitivity     Specifici
1174    165     254     1724    0.82            0.91
1724    254     165     1174    0.91            0.82
F1 Score: 0.8916472717869149
Runtime: 2.60 seconds
Total Runtime: 38.59 seconds
```

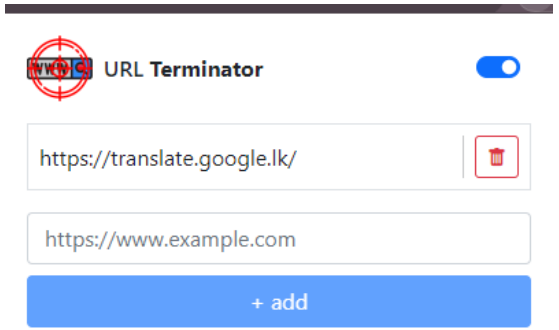
Model Selection

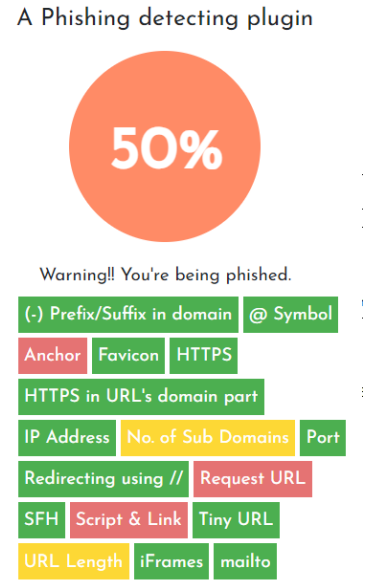
Model integration with Plugin

Model Training:	A machine learning model was trained to identify phishing websites.
Model Integration:	The trained model was integrated into a Chrome extension.
User Interaction:	When a user visits a website, the extension silently checks it for suspicious signs.
Data Transmission:	The extension sends these signs to the model for analysis.
Classification:	The model processes the signs and classifies the website as safe, potentially risky, or dangerous.

Results


stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css
stackpath.bootstrapcdn.com says
Warning!!! This seems to be a phishing website.
OK
/*!
* Bootstrap v4.1.3 (https://getbootstrap.com/)
* Copyright 2011-2018 The Bootstrap Authors
* Copyright 2011-2018 Twitter, Inc.
* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENS
/:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace},::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-ms-overflow-style:scrollbar;-webkit-tap-highlight-color:transparent}@-ms-viewport{width:device-width}article,aside,figcaption,figure,footer,header,hgroup,main,nav,section{display:block}body{margin:0;font-family:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";font-size:1rem;font-weight:400;line-height:1.5;color:#212529;text-align:left;background-color:#fff}
[tabindex="-1"]:focus{outline:0!important}hr{box-sizing:content-box;height:0;overflow:visible}h1,h2,h3,h4,h5,h6{margin-top:0;margin-bottom:.5rem}p{margin-top:0;margin-bottom:1rem}abbr[data-original-title],abbr[title]{text-decoration:underline;-webkit-text-decoration:underline dotted;text-decoration:underline dotted;cursor:help;border-bottom:0}address{margin-bottom:1rem;font-style:normal;line-height:inherit}dl,ol,ul{margin-top:0;margin-bottom:1rem}ol ol,ol ul,ul ol,ul ul{margin-bottom:0}dt{font-weight:700}dd{margin-bottom:.5rem;margin-left:0}blockquote{margin:0 0 1rem}dfn{font-style:italic}b,strong{font-weight:bolder}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sub{bottom:-.25em}sup{top:-.5em}a{color:#007bff;text-decoration:none;background-color:transparent;-webkit-text-decoration-skip:objects}a:hover{color:#0056b3;text-decoration:underline}a:not([href]):not([tabindex]){color:inherit;text-decoration:none}a:not([href]):not([tabindex]):focus,a:not([href]):not([tabindex]):hover{color:inherit;text-decoration:none}a:not([href]):not([tabindex]):focus{outline:0}code,kbd,pre,samp{font-family:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace;font-size:1em}pre{margin-top:0;margin-bottom:1rem;overflow:auto;-ms-overflow-style:scrollbar}figure{margin:0 0 1rem}img{vertical-align:middle;border-style:none}svg{overflow:hidden;vertical-align:middle}table{border-collapse:collapse}caption{padding-top:.75rem;padding-bottom:.75rem;color:#6c757d;text-align:left;caption-side:bottom}th{text-align:inherit}label{display:inline-block;margin-bottom:.5rem}button{border-radius:0}button:focus{outline:1px dotted;outline:5px auto -webkit-focus-ring-color}button,input,optgroup,select,textarea{margin:0;font-family:inherit;font-size:inherit;line-height:inherit}button,input{overflow:visible}button,select{text-transform:none}[type=reset],[type=submit],button,html [type=button]{-webkit-appearance:button}[type=button]::-moz-focus-inner,[type=reset]::-moz-focus-inner,[type=submit]::-moz-focus-inner,button::-moz-focus-inner{padding:0;border-style:none}input[type=checkbox],input[type=radio]{box-sizing:border-box;padding:0}input[type=date],input[type=datetime-local],input[type=month],input[type=time]{-webkit-appearance:listbox}textarea{overflow:auto;resize:vertical}fieldset{min-width:0;padding:0;margin:0;border:0}legend{display:block;width:100%;max-width:100%;padding:0;margin-bottom:.5rem;font-size:1.5rem;line-height:inherit;color:inherit;white-space:normal}progress{vertical-align:baseline}[type=number]::-webkit-inner-spin-button,[type=number]::-webkit-outer-spin-button{height:auto}[type=search]{outline-offset:-2px;


URL Terminator
https://translate.google.lk/
https://www.example.com
+ add


A Phishing detecting plugin
50%
Warning!! You're being phished.
(-) Prefix/Suffix in domain
@ Symbol
Anchor
Favicon
HTTPS
HTTPS in URL's domain part
IP Address
No. of Sub Domains
Port
Redirecting using //
Request URL
SFH
Script & Link
Tiny URL
URL Length
iFrames
mailto

Thank You