DETECTION OF PHISHING ATTACKS USING DEEP LEARNING

Zainab Fatima[1], F. S Amal arif[2],Amena kausar[3], Dr. Syed Asadullah hussaini[4]
[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.
[4]Associate Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

Abstract: In the current digital landscape, several web sites cater to diverse objectives, including data dissemination, advertising, social interaction, and more. However, there are certain online sites that engage in criminal activities or phishing. Phishing refers to the act of gathering confidential information from someone, including financial data and personal details. This activity has the potential to endanger customers. Phishing Websites are online websites that engage in phishing operations. The identification of phishing sites is a well studied field that is crucial for browsers, online apps, and other software. Several technologies, including data mining and text mining, have been explored to identify phishing websites. Most prior research is centered on text-based frameworks that utilize web page text data and employ text mining methods to evaluate phishing data. The primary objective of this study was to investigate methods that rely on attributes to identify phishing websites. This study used contemporary methodologies to incorporate Machine Learning and Deep Learning algorithms into features-based methods. The primary objective of this study is to design an appropriate categorization model for accurately predicting phishing websites.

Keywords: URL, CNN, DNS, HTTP.

INTRODUCTION

A phishing assault is a method used to illicitly get a user's personal information, including their login, password, credit card details, and other pertinent data. The incidence of phishing attacks is rising in tandem with economic development. Phishing often involves the use of emails or websites to illicitly obtain information [3]. The phishing websites closely mimic the appearance of the real websites in order to deceive and ensnare people. The Antiphishing Work Group[4] finds a significant increase in phishing activities. Phishers strategically focus on specific individuals and launch their attacks using emails, texts, or phone calls[3]. Figure 1 displays the quantity of identified phishing websites in the year 2018. Phishing may occur via several methods. Deceptive phishing is a method in which an attacker pretends to be an organization in order to fraudulently get information from individuals. Detection of such attacks may be achieved by examining the URL and distinguishing the fraudulent links from legitimate ones. Spear phishing is a deliberate and focused cyber assault carried out by email, in which the attackers specifically target an individual or organization. They gather information on the victim from social networking platforms such as LinkedIn. The assailant manipulates the data pertaining to the intended victim and carries out the assault via electronic mail. Pharming is a kind of cyber assault that involves cache poisoning of the Domain Name System (DNS). The assailant modifies the IP address associated with the DNS and sends visitors to a malevolent website. Dropbox Phishing is a kind of cyber assault in which the perpetrators aim to get unauthorized access to the data of Dropbox users. They do this by creating a fraudulent sign-in page for Dropbox, which may be hosted on the actual Dropbox platform, in order to obtain the users' login credentials. Google Docs phishing is a kind of cyber assault that is comparable to Dropbox phishing. The objective of the attackers is to get unauthorized access to Google Drive and its associated documents. This particular attack occurred in 2015. In addition to hosting a false login page, the Google website also provided an SSL certificate to ensure a safe connection. Despite the use of anti-phishing procedures, phishing assaults persist for the following reasons. Initially, consumers exhibit a preference for using mobile phones rather than desktop computers for browsing the internet and checking emails[8]. They have a higher probability of accessing phishing websites that have not yet been identified by the anti-phishing websites. Furthermore, people refrain from using or uninstalling the anti-phishing programs on their mobile devices due to concerns about energy consumption and memory use. Furthermore, the existing antiphishing solutions exhibit subpar performance in terms of detection. According to reports, mobile users are three times more inclined to provide their information on phishing websites compared to desktop users[9]. Figure 2 displays the industries that are most often targeted by phishing attacks. The attackers mostly focused on targeting payment systems, although there has been a significant rise in assaults against Software as a Service (SaaS) in 2018. The objective of the attackers is to illicitly acquire the confidential information by launching assaults on Software as a Service (SaaS) or webmail platforms. The proposed Web Content Phishing Attack Detector (WC-PAD) accurately identifies assaults specifically designed for website phishing.

Existing System

Phishing breaches the principles of Confidentiality, Integrity, and Availability. Several changing ways are being developed to identify phishing assaults, but, they remain feasible and pose a significant hazard to individuals. Detecting phishing websites using hardware devices yields excellent accuracy, but it is a costly option. Therefore, software-based alternatives are favored. Blacklist and whitelist are used for very accurate phishing detection. However, they need regular list maintenance, since it is necessary to manually update the list of URLs for phishing websites. Therefore, in order to address the problems associated with human list updates, the present technique involves the use of automated detection methods such as machine learning and heuristic approaches. A multitude of machine learning algorithms use either web structure or online content-based methodologies to detect phishing URLs.

Proposed Methodology

This study presents a comparative analysis and prediction method for phishing websites, using two modeling techniques: Machine Learning and Deep Learning. An architectural diagram was used to illustrate the suggested strategy for this system, as seen in Figure 1. The main goals of this suggested technique are to determine the optimal and most precise classification model for predicting phishing websites.

The classification study included the use of two machine learning models, namely Naïve Bayes and Support Vector Machine, as well as two deep learning models, namely the Neural Networks method and Convolutional Neural Network. The Phishing Websites Features Dataset (Rami, 2015) was used for feature-based categorization. This dataset considers website attributes such as URL length, the count of symbols like '.', '//', HTTP or HTTPS authenticator, and so on. This system is specifically created with a prediction model for identifying phishing websites, based on the categorization analysis.

IJESR

IJESR

SYSTEM DESIGNING

SYSTEM DESIGN

UML DIAGRAMS

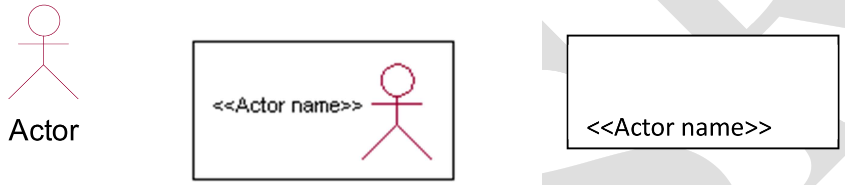
The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

Global Use Case Diagrams:

Identification of actors:

Actor: Actor represents the role a user plays with respect to the system. An actor interacts with, but has no control over the use cases.

Graphical representation:



DEEP LEARNING-BASED METHODS

In this section, we examined contemporary deep learning methods used for detecting phishing websites. Bu and Cho [11] created a deep autoencoder model for identifying zero-day phishing attempts and achieved an accuracy of 97.34%. Character-level characteristics were extracted from URL strings and tests were conducted on three distinct datasets obtained from Phish Storm [2], ISCX-URL-2016 [12], and Phish Tank [13]. The experimental findings were evaluated using receiver-operating characteristic curve analysis and N-fold cross-validation. Upon comparing the root mean square error (RMSE) in the reconstruction phase of both authentic URLs and phishing URLs, it was observed that the RMSE exhibited a significant rise for the phishing URL. Somesha et al. [14] proposed the use of deep learning models to identify phishing websites. They achieved this by using 10 specific elements retrieved from HTML and a third-party service. The researchers conducted a comparative analysis of three deep learning models and determined the weights of 18 characteristics. The empirical findings revealed that the Long Short-Term Memory (LSTM) model had a peak accuracy of 99.57%. However, they just used a single published dataset including 3526 cases. The dataset is evidently insufficient for training deep learning models. The high accuracy rate shown in the experimental findings might perhaps be attributed to the imbalanced distribution and limited variety of the test data.

Adebowale et al. [15] used a combination of the convolutional neural network (CNN) and long short-term memory (LSTM) algorithm to accurately categorize phishing websites. The hybrid classifier achieved a 93.28% accuracy and had an average calculation time of 25 seconds by using image, frame, and text information. The URLs were gathered from Phish Tank and Common Crawl, and picture characteristics were retrieved from the URLs. The picture characteristics are used as input for the offline Convolutional Neural Network (CNN) model, while the text features are sent to the Long Short-Term Memory (LSTM) classifier. The key aspect of this method is to integrate the attributes of images and written content. Nevertheless, based on the experimental findings, there is still scope for enhancing the accuracy rate, and the computation time is too lengthy to fulfill the demands of real-time predictive goods.

FRAMEWORKS AND SYSTEMS

The primary function for identifying potential phishing attempts on a website is a prediction engine that relies on machine learning. The responsiveness of the predictive service is the paramount metric for assessing the viability of this real-time system.

Atimorathanna et al. [16] presented an anti-phishing system that includes a web browser extension, an e-mail detection plug-in, filters, and a phishing detection server based on machine learning. The browser extension is used to get the present URL, record a visual representation of the webpage, and retain the user's browsing history as a profile on the client-side. The server employs the following procedures primarily to identify phishing links: (1) utilizing third-party services' blacklist and whitelist to filter newly generated URLs; (2) employing a machine learning model that relies on 13 characteristics to forecast whether a URL is a phishing link; (3) utilizing computer vision technology to detect website logos and compare the similarity of web page screenshots. The essay utilizes a logo detector to accurately identify 20 prominent online banks and a selection of frequently seen website logos.

The authors curated and constructed their own database specifically for training the logo identification algorithm, achieving a precision rate over 95%. The similarity of the two screenshots is compared using the OpenCV package in Python. The URL analyzer's trial findings indicated that the Random Forest classifier attained the greatest accuracy rate of 96.257%. The system is a fully functional online real-time detection system for phishing that employs many techniques to efficiently safeguard users from attacks. Nevertheless, there is scope for enhancing the performance of the machine learning model, and the logo classifier's ability to recognize logos is limited.

Maurya et al. [17] developed an anti-phishing solution that includes a web browser plugin. The browser plugin acquires the current URL instantaneously and extracts characteristics based on the DOM structure. It then identifies the presence of potential phishing attempts and alerts the user accordingly. The detection service is comprised of three distinct stages: whitelist matching, blacklist filtering, and prediction using a machine learning model. In the prediction step, the URL that qualifies as a phishing link is identified based on its character-level properties. For instance, the web page lacks hyperlinks and the number of linkages to external domain names above a certain threshold. These criteria are susceptible to attacks, and there is a high probability of misidentifying typical URLs. Furthermore, the author enhances precision by amalgamating three fundamental classification models.

Shah et al. [18] introduced a browser plugin that use machine learning to identify phishing URLs. The Random Forest model was trained using the UCI dataset, which consists of 11,055 instances and 30 normalized features. Hence, it is necessary to extract characteristics from the current URL string in a real-time setting. The writers of the paper identified 16 traits that are independent of third-party services. The experimental findings indicate an accuracy rate of 89.6%, suggesting significant potential for improvement.

.

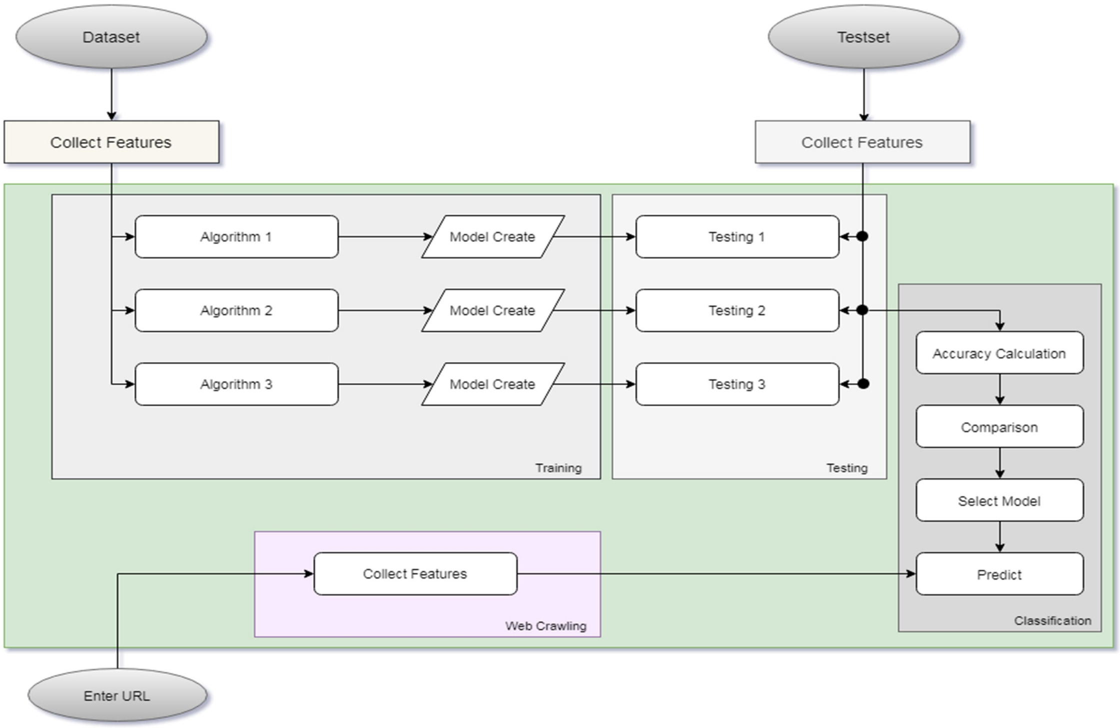
PROTOTYPE IMPLEMENTATION

The prototype implementation of the complete system is partitioned into three autonomous apps. The browser extension is autonomously packed and uploaded to the Chrome browser in accordance with the extension development specifications of the Chrome browser. It will undergo a review process and be published by the Chrome platform. The construction of Chrome browser plug-ins involves the use of three online front-end programming languages: HTML, JavaScript, and CSS. The data collecting application is built using Python as the primary programming language. It utilizes scheduled tasks to effectively handle the collection duties for each data source. One of the tools utilized is Phish Tank, which extracts information from web sites by using a widely popular software program called Beautiful Soup.

An application has been developed that combines model training, prediction services, and the official website for the product. This application utilizes Python as its main programming language and incorporates Flask as the web framework. Model training is also controlled by scheduled tasks. Once the training is finished, the key performance indicators are promptly recorded in the MySQL database, and the model is stored in the system. The prediction service is a RESTful API that offers customers the ability to acquire real-time detection results via POST queries. The primary purpose of the official website is to receive and assess suspected phishing links reported by users using a combination of human and automated verification processes in order to establish the level of risk associated with the links.

IMPLEMENTATION

Flow chart

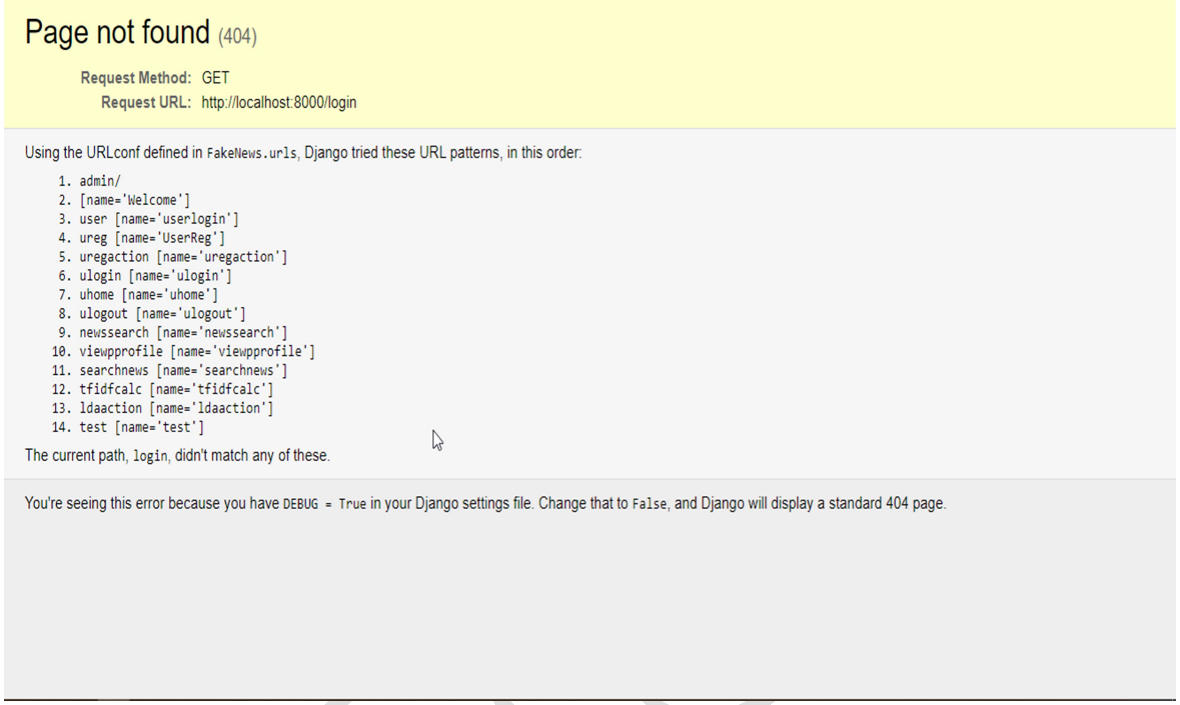


TESTING

Integration Testing

URL Mismatch Error

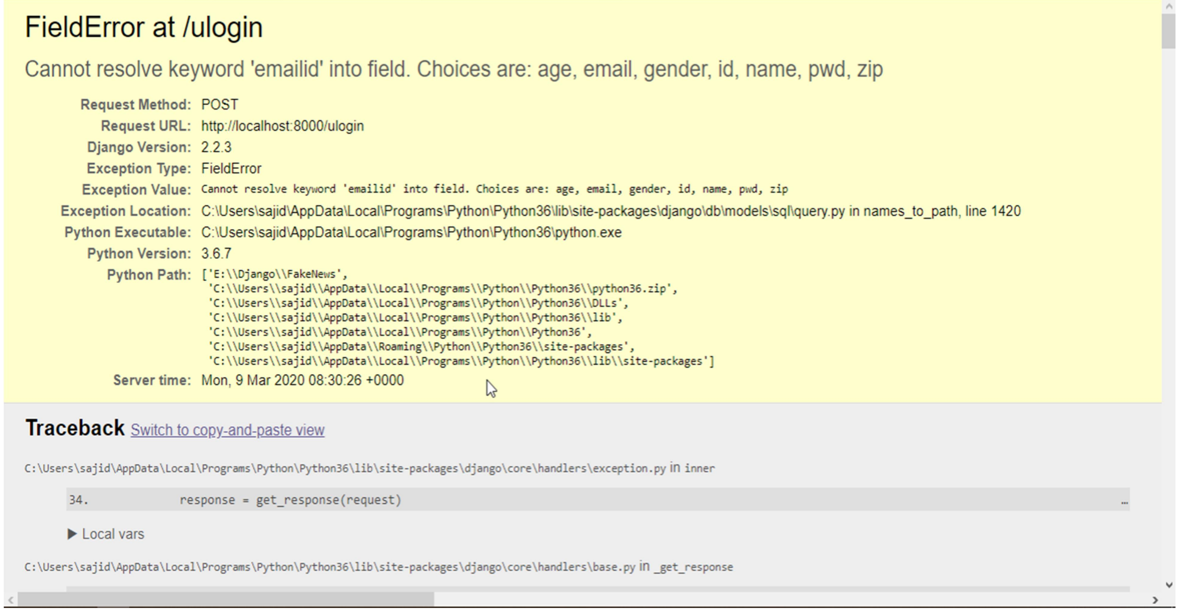
When we give URL like localhost:8000/login and if it's not match in urls.py files, we can get this error.



```
Page not found (404)

    Request Method:  GET
       Request URL:  http://localhost:8000/login

Using the URLconf defined in FakeNews.urls, Django tried these URL patterns, in this order:

     1. admin/
     2. [name='Welcome']
     3. user [name='userlogin']
     4. ureg [name='UserReg']
     5. uregaction [name='uregaction']
     6. ulogin [name='ulogin']
     7. uhome [name='uhome']
     8. ulogout [name='ulogout']
     9. newssearch [name='newssearch']
    10. viewpprofile [name='viewpprofile']
    11. searchnews [name='searchnews']
    12. tfidfcalc [name='tfidfcalc']
    13. ldaaction [name='ldaaction']
    14. test [name='test']

The current path, login, didn't match any of these.

You're seeing this error because you have DEBUG = True in your Django settings file. Change that to False, and Django will display a standard 404 page.
```

Field Error

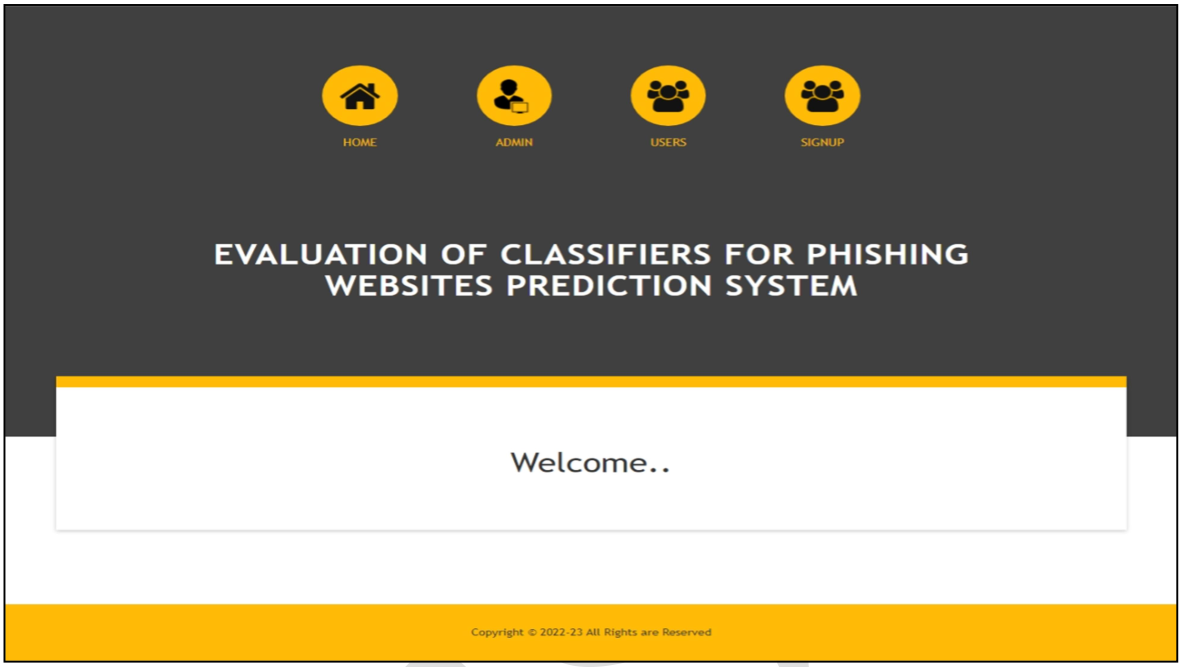
Database field mismatch from model. Given keyword 'emailid' into field. expected: age, email, gender, id, name, pwd, zip.



```
FieldError at /ulogin
Cannot resolve keyword 'emailid' into field. Choices are: age, email, gender, id, name, pwd, zip

    Request Method:  POST
       Request URL:  http://localhost:8000/ulogin
    Django Version:  2.2.3
    Exception Type:  FieldError
   Exception Value:  Cannot resolve keyword 'emailid' into field. Choices are: age, email, gender, id, name, pwd, zip
Exception Location:  C:\Users\sajid\AppData\Local\Programs\Python\Python36\lib\site-packages\django\db\models\sql\query.py in names_to_path, line 1420
 Python Executable:  C:\Users\sajid\AppData\Local\Programs\Python\Python36\python.exe
    Python Version:  3.6.7
       Python Path:  ['E:\\Django\\FakeNews',
                      'C:\\Users\\sajid\\AppData\\Local\\Programs\\Python\\Python36\\python36.zip',
                      'C:\\Users\\sajid\\AppData\\Local\\Programs\\Python\\Python36\\DLLs',
                      'C:\\Users\\sajid\\AppData\\Local\\Programs\\Python\\Python36\\lib',
                      'C:\\Users\\sajid\\AppData\\Local\\Programs\\Python\\Python36',
                      'C:\\Users\\sajid\\AppData\\Roaming\\Python\\Python36\\site-packages',
                      'C:\\Users\\sajid\\AppData\\Local\\Programs\\Python\\Python36\\lib\\site-packages']
       Server time:  Mon, 9 Mar 2020 08:30:26 +0000

Traceback Switch to copy-and-paste view

C:\Users\sajid\AppData\Local\Programs\Python\Python36\lib\site-packages\django\core\handlers\exception.py in inner

    34.            response = get_response(request)                                                   …

    ▶ Local vars

C:\Users\sajid\AppData\Local\Programs\Python\Python36\lib\site-packages\django\core\handlers\base.py in _get_response
```

RESULTS

Homepage



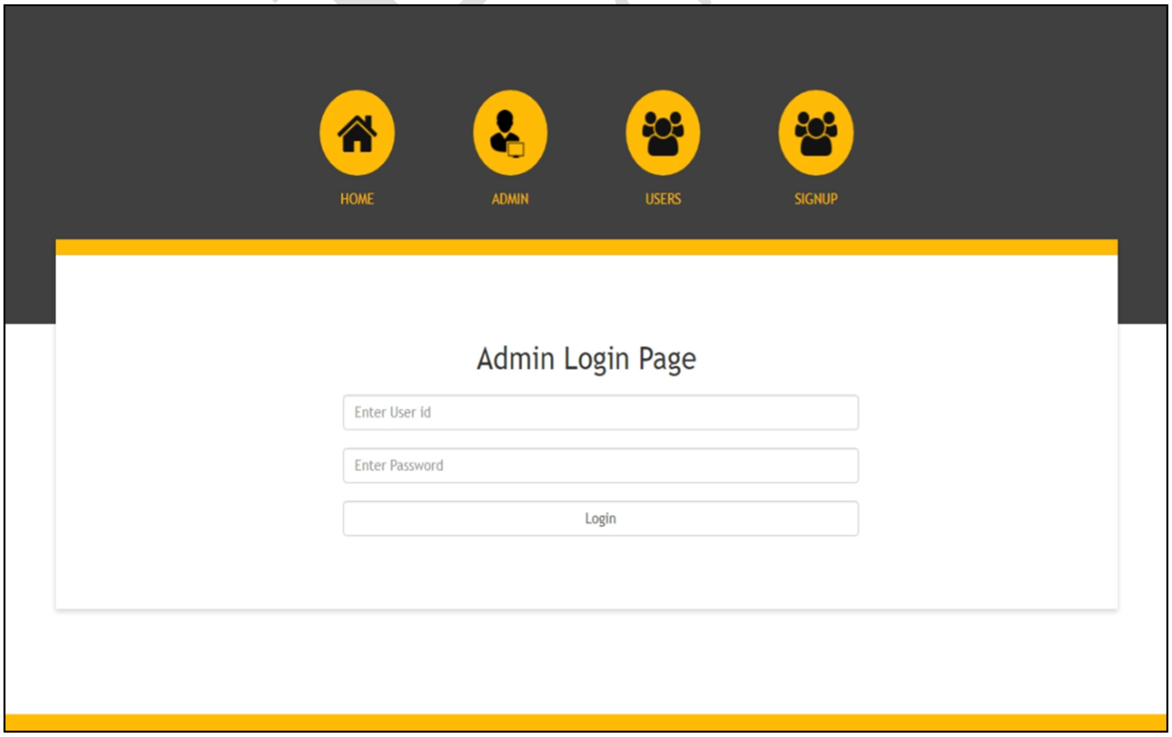
EVALUATION OF CLASSIFIERS FOR PHISHING WEBSITES PREDICTION SYSTEM

Welcome..

Copyright © 2022-23 All Rights are Reserved

Figure: Homepage

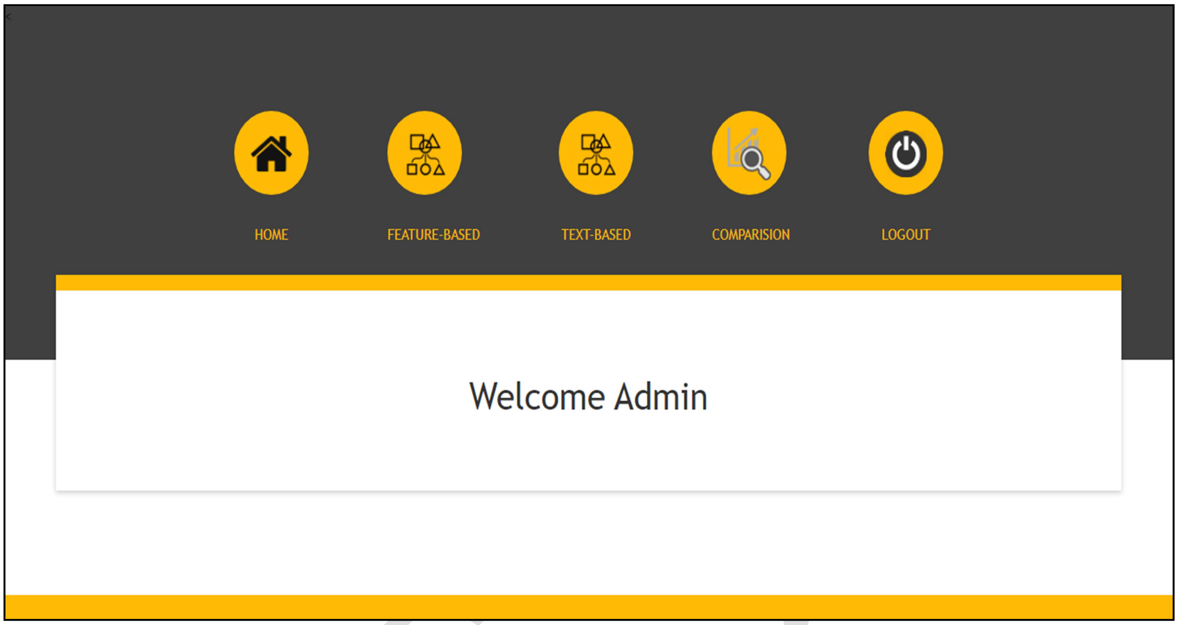
Login module of the admin



Admin Login Page

Figure : Login module of the admin

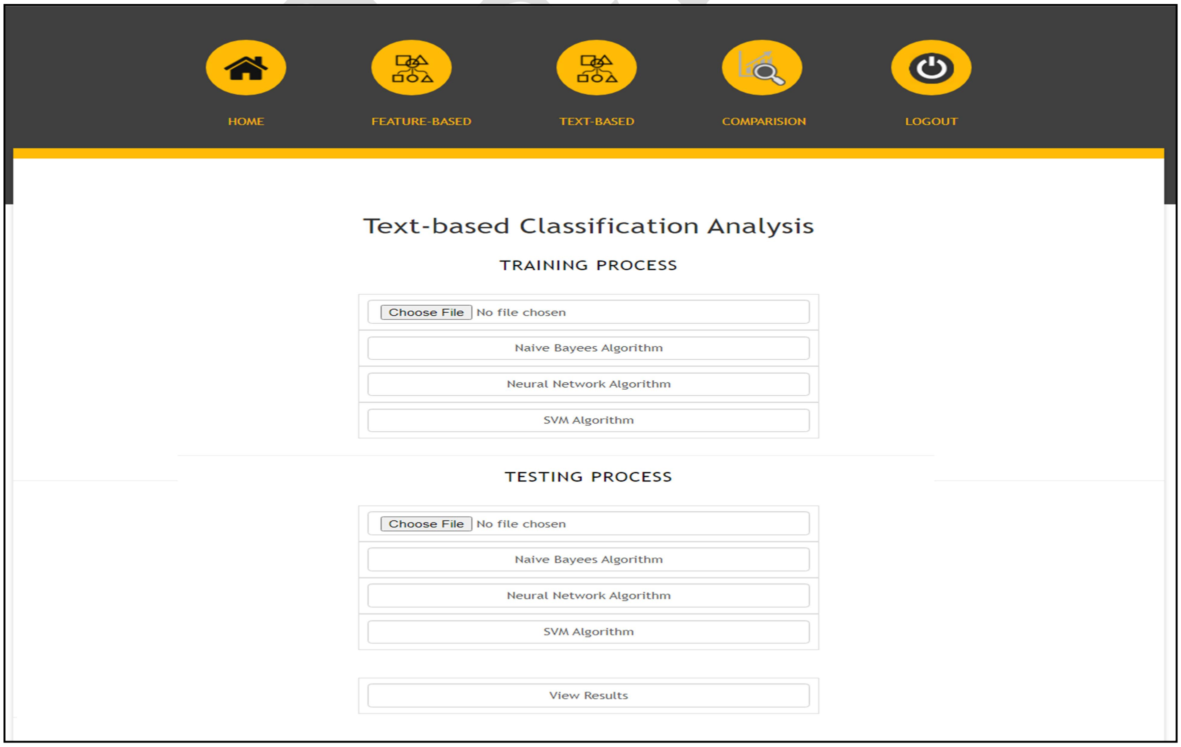
Homepage of the admin



Welcome Admin

Figure : Homepage of the admin

Text-based classification analysis page



Text-based Classification Analysis

TRAINING PROCESS

TESTING PROCESS

Figure : Feature-based classification analysis page

Login module of the users

This page is for verifying the users' with this login option. As shown in figure 6.9, this page collect login details of the user.

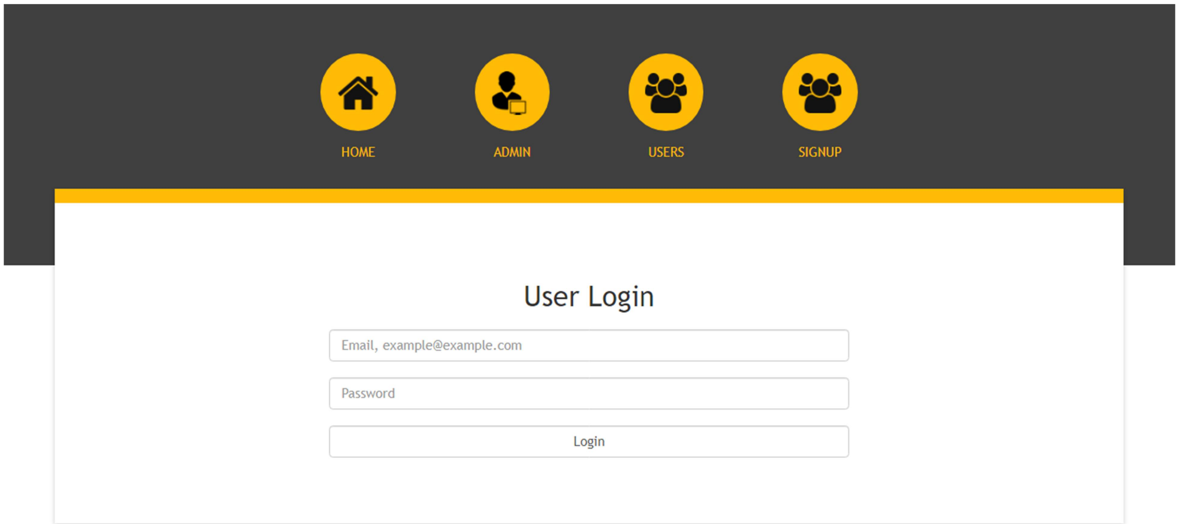
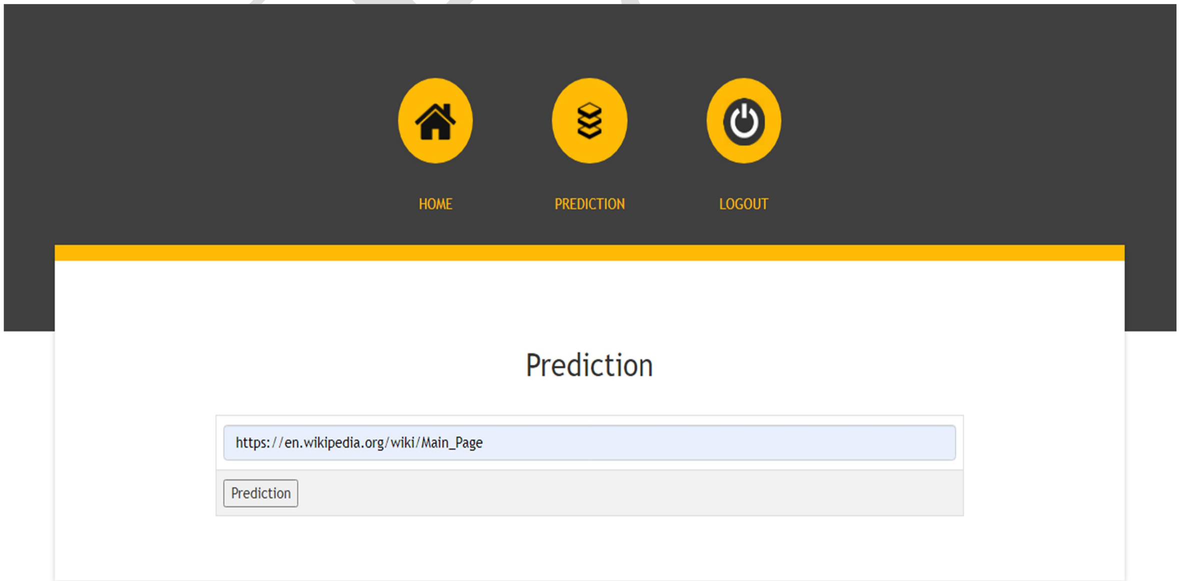


Figure : Login module of the users

User prediction page

As shown in figure , this page is for entering the real-time websites URLs for prediction. With a high degree of accuracy, the machine learning module can determine whether a website is legitimate or a phishing site for given website.



https://en.wikipedia.org/wiki/Main_Page

Figure : User prediction page

CONCLUSIONS AND FUTURE WORK

Phishing is the act of acquiring confidential information from customers, which may potentially put users at risk. Phishing site detection is a well studied field and a need for browsers, online apps, and other software. Most studies used text mining and data mining techniques. Prior research has used text-based frameworks that are constructed using textual data extracted from websites. This research primarily examined text-based and feature-based classification analysis approaches in order to identify the most effective model for predicting phishing websites. The research used naive Bayes, support vector machine, and neural networks as machine learning methodologies. These algorithms were executed on two distinct datasets, one consisting of text-based data and the other consisting of features-based data. The neural network technique outperformed other classification methods in terms of accuracy for both analyses. This study also achieved precision in classifying real-time websites based on manually labeled data. The feature-based neural networks model outperformed the text-based neural networks model in these findings.Explore advanced categorization methods, such as Convolutional Neural Networks (CNN) and R-CNN, for predicting phishing websites.

References

1. Sahingoz, Ozgur & Buber, Ebubekir & Demir, Onder & Diri, Banu. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications. 117. 345-357.
2. Bohacik, Jan & Skula, Ivan & Zábovský, Michal. (2020). Data Mining-Based Phishing Detection. 27-30. 10.15439/2020F140.
3. Jain, Ankit & Gupta, B B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. EURASIP Journal on Information Security. 2016. 10.1186/s13635-016-0034-3.
4. Aljofey, Ali & Jiang, Qingshan & Rasool, Abdur & Chen, Hui & Liu, Wenyin & Qu, Qiang & Wang, Yang. (2022). An effective detection approach for phishing websites using URL and HTML features. Scientific Reports. 12. 8842. 10.1038/s41598-022-10841-5.
5. Rami Mustafa A Mohammad, Phishing Websites Data Set, 2015, [Online] Available at: https://archive.ics.uci.edu/ml/datasets/phishing+websites#. Last Accessed 1st Sep, 2022.
6. Alex Liddle, Dataset of Malicious and Benign Webpages, 2020, [Online] Available at: https://www.kaggle.com/code/alexliddle/semi-supervised-machine-learning-99-accuracy/data. Last Accessed 2nd, May, 2022.
7. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
8. Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.
9. Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
10. Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)

11. Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022
12. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
13. Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
14. M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978-981-10-3874-7_3 Dec (2016)
15. Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017
16. Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
17. Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
18. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
19. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
20. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
21. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.
22. Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
23. Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017

IJESR

24. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;
25. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
26. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021
27. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
28. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
29. .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
30. Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
31. Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)
32. Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)
33. Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
34. Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016
35. Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
36. Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)

IJESR