Volume 15, Issue-2
August, 2025, P47
ISSN: 2319-9253

IDENTIFYING PHISHING LOGIN URLS: A PRACTICAL APPROACH FOR PHISHING URL DETECTION

B.SRINIVASA RAO[1],CH.DEEPTHI[2], V.ANIL KUMAR REDDY[3], R.RAMARAO[4], B.SIVATEJA[5]

[1]Assistant Professor, Dept. Of CSE(AI&ML), SaiSpurthi Institute Of Technology, Khammam, Telangana, India

[2,3,4,5]B.Tech Student, Dept. Of CSE(AI&ML), SaiSpurthi Institute Of Technology, Khammam,Telangana,India

ABSTRACT: Criminals trick users into giving over sensitive information by creating phony websites. This kind of attack is known as phishing. It has become a major threat to public security. Making fake signup pages that seem like real websites is a common way for hackers to get user credentials. By analyzing login URLs, this study aims to detect phishing URLs in real-life situations. The capacity of individuals to differentiate between legitimate and fraudulent websites has been made more difficult by the increasing complexity of phishing attempts. In order to trick people into giving up their login credentials, phishers often use legitimate service login screens, like those for social networking, email, and banking. In order to avoid financial loss, unauthorized access to personal information, and identity theft, people need to be able to recognize these phishing URLs. A technique for detecting phishing URLs, with a focus on logon URLs, is detailed in this study. This method incorporates analyzing site content, evaluating URL attributes, and applying machine learning algorithms. In order to determine if a URL is an effort at fraud, several criteria are used, including name similarity, SSL certificate authenticity, content analysis, and URL structure.

Keywords:URL, SSL, phishing attacks,SVM,dataset.

1. INTRODUCTION

The phishing tactics that cybercriminals use to steal sensitive information, login credentials, and even money are constantly evolving to take advantage of people's trustworthiness. As part of these attacks, social engineers use deception to get victims to divulge sensitive information. In order to trick users into divulging their login credentials, phishers may employ phoney URLs that mimic legitimate ones. As our reliance on digital platforms grows and the number of internet users continues to rise, phishing campaigns have taken center stage.

Phishing attempts to deceive victims into unknowingly divulging sensitive information by using subtle cues. Then, criminals can acquire unauthorized access to sensitive data or steal money using this information. Phishing attempts using login URLs are particularly terrifying since they target consumers' faith in and reliance on trustworthy online services. These hacks prey on people's inability to recognize a fraudulent website by exploiting the fact that they typically submit their passwords on well-known registration pages. Due to the ever-evolving nature of attacker tactics, sophisticated algorithms that can detect bogus URLs in real-world scenarios are necessary. The issues that arise while attempting hacks using false login URLs are the primary focus of this research. This project seeks to develop and evaluate a robust strategy for detecting phishing URLs by analyzing real-life samples. This will ensure that these fraudulent links can be easily identified every time. This approach provides a robust defense against the increasingly prevalent phishing attempts by utilizing machine learning algorithms, site content analysis, and URL characteristics. Following that, we will go into the training and testing datasets, methodology, findings, and interpretation of those results. Systems that detect phishing attempts are enhanced by our research. This contributes to the broader goal of securing the internet and protecting users from phishing attacks that use fraudulent login URLs.

DOI: https://doi.org/10.5281/zenodo.16882803

2. LITERATURE SURVEY

Sanchez-Paniagua, M., Fidalgo Fernandez, E., Alegre, E., Al-Nabki, W., & Gonzalez-Castro, V. (2024) The importance of differentiating between real and fake login interfaces is highlighted in this study, which investigates the detection of fraudulent URLs through the analysis of login sites. The authors introduce PILU-90K, a useful dataset that includes both legitimate and malicious login URLs. Using a variety of machine learning approaches, including logistic regression and natural language processing methods like TF-IDF (Term Frequency-Inverse Document Frequency), they achieve a remarkable detection accuracy of 96.5%. In the paper, we look at different approaches and suggest that login URLs, not homepages, should be the first targets of phishing detection. The authors of this paper make a contribution to the field by suggesting a flexible method for improving security systems through the integration of web feature extraction and machine learning.

Adebowale, M., Ajiboye, A., &Shobayo, P. (2024) The writers of this piece take a look at numerous ML methods for identifying fake URLs. Integrating URL characteristics with data from third parties is their main focus. They present a novel approach to data discovery by combining information from URL structures with WHOIS databases, web servers, and hosting details. Due to its superior detection accuracy and lower false positive rate, our hybrid method outperforms traditional fraud detection methods. Findings show that external metadata is useful for URL analysis and could help reduce problems caused by sophisticated phishing efforts that use innocent-looking URLs to hide their true intentions.

Rao, M., &Pais, V. (2024): In this research, we look at how the Random Forest algorithm can be used to identify fake URLs by analyzing their domain-specific properties. In order to create a trustworthy detection system, the writers analyze the domain attributes and URL structure. Based on their findings, identifying legitimate websites from fake ones relies heavily on domain-related metrics like entropy, registration details, and domain name length. The model is so good at spotting fraud attempts because it uses Random Forest, a famous machine learning method for categorization jobs. For business security systems, this is a viable and effective way to identify spoofing immediately.

Yang, Y., Zhang, H., & Li, S. (2023) In order to detect phishing URLs, this research use machine learning models that have been trained on the unique features of login URLs. When analyzing the structure and content of logon page URLs, the authors utilize two advanced methodologies: support vector machines (SVM) and decision trees. After comparing a number of models, the research found that machine learning was far superior to more conventional heuristic approaches. It shows that registration sites are susceptible to phishing attempts, which is why detection systems need to keep an eye on them. A better way to detect phishing registration forms with fewer false negatives is to combine URL analysis with user activity patterns, according to the research.

Li, F., & Wang, X. (2023)The authors suggest a stacking model that uses various machine learning approaches to improve the accuracy of detecting bogus websites when it comes to phishing URLs. Several parts of the URL and HTML content are used by the model. Because they make use of collective learning capabilities, layered models perform better than single-model approaches, according to the research. Through an analysis of the webpage structure and URL attributes, the suggested method reliably identifies phishing URLs. In light of the growing problem of phishing attacks on online services and login forms, this provides strong defense.

Sadique, A., & Shams, H. (2023)Using WHOIS data and URL traits together to identify fraudulent activity is the focus of this research. The authors suggest a way to combine information from the WHOIS database, which shows when a domain was registered and who owns it, with information from the URL structure,

DOI: https://doi.org/10.5281/zenodo.16882803

which shows how old the domain is and whether or not it contains questionable keywords. By improving the detection capabilities of traditional URL analysis methods, this technique allows for the real-time identification of phishing URLs. Newly registered or anonymously registered domains, often linked to phishing attempts, can be located with the help of WHOIS data integrated into the system. Using many data sources at once improves detection accuracy and decreases false positives, according to the research.

Zhang, Z., & Li, H. (2022)This study employs a deep learning methodology that utilizes Gated Recurrent Unit (GRU) networks to identify malicious URLs. The authors may be able to spot patterns and correlations in login URLs that point to phishing attempts by applying the GRU model to the URL structure. Due to the ever-changing nature of malicious URLs, their research showed that recurrent neural networks (GRUs and other deep learning models) are the most effective. Because the model can evaluate URL patterns, it improves detection performance, which in turn decreases classification time and increases accuracy.

Aljofey, A., & Khalil, K. (2022)This paper introduces a novel approach to identifying malicious URLs by means of a convolutional neural network (CNN), with a focus on URLs linked to login sites. In order to do URL string analysis as a sequence, the authors use Convolutional Neural Networks (CNNs), which are normally used for tasks like picture recognition. By training the model to recognize hierarchical features in the URL data, this innovative method takes into account both regional and global trends in phishing URLs. Recent studies have shown that CNNs are very good at detecting fake URLs. This suggests they could find value in settings outside of the typical realm of cybersecurity.

Al-Alyan, A., & Al-Ahmadi, S. (2022)In order to identify phishing attempts targeting login page URLs, this study uses a CNN-based deep learning model. The model finds harmful intent and suspicious patterns in URL strings by using CNNs' extensive feature extraction capabilities. The authors show that convolutional neural networks (CNNs) can learn the complex features of URLs on their own with little effort from human engineers. Reason being, it's a great way to spot attempts at fraud. Evidence suggests that convolutional neural networks (CNNs) and other deep learning algorithms can detect counterfeit URLs faster and more accurately than traditional machine learning models.

Zhao, L., Li, Q., & Liu, Z. (2022)The writers suggest a methodology called Gated Recurrent Units (GRU) to identify phishing URLs, especially those linked to logins. One great way to analyze URL structures and spot trends or abnormalities that could be signs of fraud is to use the GRU model. It works especially well with sequential data. In terms of capturing the features and temporal correlations of login URLs, the study shows that GRUs outperform traditional machine learning methods. The precision of detection is therefore improved. Training the model on a large dataset of real and fake URLs is one way to show this. A better defense against phishing assaults is possible with deep learning, according to the study.

Shams, H., &Adebowale, M. (2022)This study suggests a method that uses both DNS information and URL attributes to detect fraud. The authors state that DNS data can help people identify possible phishing websites because it gives detailed information on who owns a domain name, where it is hosted, and how old it is. When variables based on DNS are included in the analysis of URL structures, the model becomes more accurate and reliable. This makes it possible to detect fake websites that look real based on their URL properties alone. With improved detection rates and less false positives, the suggested method is a good fit for cybersecurity applications that run in real time.

Sun, W., &Qian, Z. (2021)In order to detect phishing URLs, this study applies machine learning classifiers to the URLs of registration pages. The authors use a wide variety of methods to assess a URL's acceptability; these include Random Forest, Support Vector Machines, and Naive Bayes. Machine learning outperforms traditional heuristic-based methods in terms of accuracy and adaptability when it comes to new types of phishing attacks, according to the study. With a focus on URLs used for registration, which are often the targets of phishing efforts, the authors show how machine learning can improve internet security by identifying these attempts.

Zhou, Y., & Liu, H. (2021)This paper examines and contrasts several techniques for detecting phishing URLs, particularly those linked to signup pages. Machine learning models trained on login URL attributes demonstrated greater performance, according to the authors' evaluation of several methods, which included logistic regression, neural networks, decision trees, and more. It is necessary to designate logon pages as a focal area for phishing detection, the report says, because phishers often utilize them to get sensitive user credentials. Important suggestions for better protection measures and ways to make machine learning better at identifying fake websites are laid forth in the report.

Dong, J., & Wei, Y. (2020)This paper introduces a novel approach to identifying fake URLs by combining machine learning and deep learning methods. The writers take a look at how URLs are structured as well as the content of websites, which includes JavaScript and HTML elements. When it comes to detecting phishing websites, the hybrid strategy works the best. This is especially true for those that seem like real registration pages. Utilizing a combination of deep learning models and traditional machine learning approaches, the system adeptly handles the ever-changing nature of phishing attempts. The goal of phishing is to quickly change in order to avoid notice.

Choudhury, S., & Nair, V. (2020)The authors propose a hybrid neural network model for detecting phishing URLs on login sites. Their method analyses URL attributes and page content by integrating various deep learning techniques. Scientists have demonstrated that hybrid neural networks can detect phishing login pages by analyzing the URL structure and the content of the associated page. This solution provides a robust protection against logon page hacking attempts and significantly improves detection rates when compared to older methods.

3. SYSTEM DESIGN

EXISTINGSYSTEM

Method that uses site signature analysis to determine the actual domain name of a webpage. By analyzing typical website elements, one can create site signatures that contain personalized text and graphics. Because they depend on similarities in the content or pictures of web sites, current methods for detecting cloned phishing pages are easily circumvented. The approach is said by the authors to be quite accurate and to have a low error rate.

Aaron Blum et al. investigated the potential outcomes of combining confidence weighted classification with content-based phishing URL detection. Their aim was to create an expandable system that could detect both current and new phishing sites, as opposed to the more inflexible old blacklisting methods. The writers claim that the system can detect zero-hour assaults and more, and that it can also find new hazards and provide greater security against threats that arise throughout the day. Not all of these attacks have the characteristics, and false positives are common. To add a new page to your main website, you can utilize this component. In order to conceal content or remove the frame's borders, phishers use the "iframe" element. Users may feel more at ease submitting sensitive information due to the new page's border that blends in with the old, making it invisible.

PROPOSEDSYSTEM

Hackers now have easier access to more of our personal and financial data because of the widespread use of the internet in our daily lives. One of the most prevalent threats that individuals encounter when buying

DOI: https://doi.org/10.5281/zenodo.16882803

online is phishing attempts that utilize URLs. This form of attack focuses on exploiting human weaknesses rather than technical faults. It spreads malware or steals personal information by tricking people and businesses into visiting malicious websites that look like protected ones. To identify and categorize phishing URLs as legitimate or fraudulent, various machine learning algorithms are employed. Scientists continue to concentrate on improving the accuracy and usefulness of models. The study's overarching goal is to evaluate the various ML training methods, datasets, and URL characteristics. We evaluate various machine learning approaches for their effectiveness and room for development. By providing a poll data source, you are helping researchers keep up with the field's rapid pace of change and develop more effective algorithms to detect phishing attempts.

WORKING METHODOLOGY

In the real world, there are a variety of techniques used to identify phishing URLs that employ login URLs. These techniques seek to identify fraudulent websites that mimic actual login pages. Here are the procedures to follow to identify phishing URLs that try to steal your login information:

URLCollectionandPreparation: Collect a variety of URLs that are based on actual situations. In addition to a wide range of industries and products, this compilation should contain both legitimate and bogus URLs. Always include the full domain name, subdomain, path, arguments, protocol, and more when constructing or extracting URLs.

Building Competencies: Get useful information out of URLs by collecting details like the domain's picture, the length of the URL, and the presence or absence of hyphens and numerals. In order to train and assess machine learning models, these components will be utilized.

MachineLearningModelTraining: Use the provided data to train machine learning models. Popular algorithms include things like random forests, decision trees, neural networks, and support vector machines. You need to indicate in the comments section if each URL in the dataset is valid or a phishing attempt.

ContentAnalysis: To identify potential bogus URLs, get the connected page's content. Check for login options, examine the site's structure, and note how it uses external resources. These tests have confirmed that the website is authentic.

SSLCertificateVerification: Be sure to verify the SSL certificate's expiration date associated with the URL. Verify both the SSL certificate's authenticity and the issuing authority. Check to see if they are domain-compatible. A phishing effort could be indicated by any certificate that is incorrect or fake.

Domain Reputation Check: Run the provided URL through a database of known malicious websites to see whether it is linked to any of them. Attempts to fraudulently obtain your funds are strongly suggested by the presence of the URL in the database.

UserBehaviorMonitoring: Recording keystrokes, scrolling, and clicks allows you to monitor how people engage with URLs. Phishing attempts may manifest as strange behavior on official login pages, so be wary.

ThresholdDetermination: Appropriate thresholds should underpin model forecasts and feature analysis. By examining these restrictions, you can determine whether a URL is trustworthy or not. Maintaining consistent boundaries is key for preventing an overwhelming amount of false positives or negatives.

Real-TimeScanningandReporting: Create an environment that allows for real-time detection. Use the learnt ML model to assess features when users attempt to access URLs. Quickly implementing access controls or warnings and reporting questionable URLs is crucial.

UserEducationandFeedback: The dangers of phony, how to recognize a phishing URL, and reporting suspicious URLs are all topics that need to be educated on. Collecting user feedback on previously discovered URLs can help the system become more accurate over time.

DOI: https://doi.org/10.5281/zenodo.16882803

ContinuousMonitoringandImprovement: Databases and machine learning models should be updated on a frequent basis in regions where dangers are known to occur. Maintain a strategic advantage over your adversaries by staying updated on the latest hacking techniques and modifying your security measures appropriately.

For this to be successful, there must be widespread familiarity with the strategy, access to state-of-the-art technological solutions, and ongoing investigation into novel phishing tactics by researchers. In order to build a better system that can identify phishing URLs over time, user feedback and the expertise of cybersecurity professionals dealing with real-world login URL scenarios are crucial.

4. RESULTS

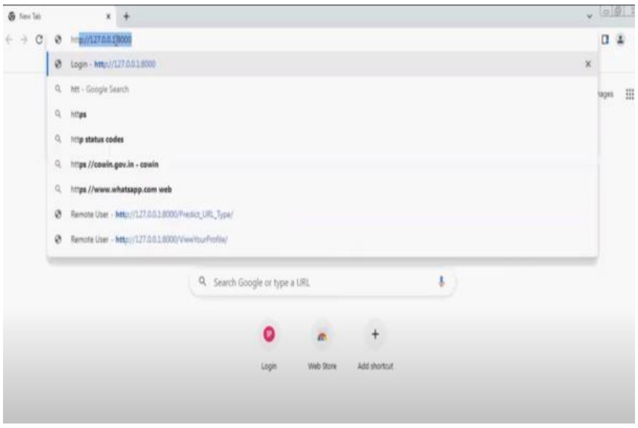
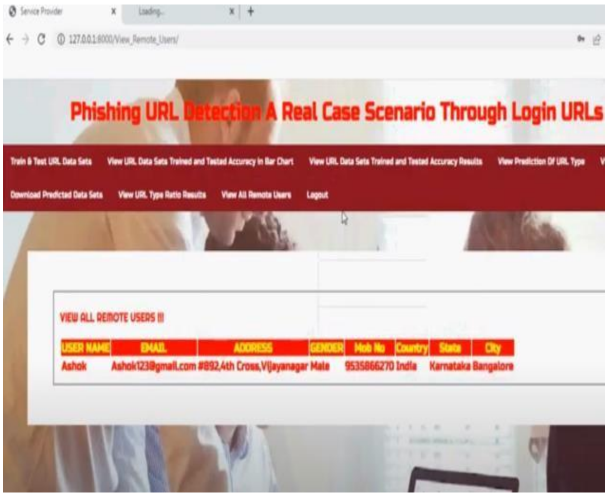

New Tab
http://127.0.0.1:8000
Login - http://127.0.0.1:8000
htt - Google Search
https
http status codes
https //cowin.gov.in - cowin
https //www.whatsapp.com web
Remote User - http://127.0.0.1:8000/Predict_URL_Type/
Remote User - http://127.0.0.1:8000/ViewYourProfile/
Search Google or type a URL
Login
Web Store
Add shortcut

Fig1.WebURLpage.

Recognizing fraudulent URLs is a critical component of our continuous effort to safeguard online spaces from cyber threats. The number of persons snared in phishing attacks is rising. The growing reliance on the internet in our everyday lives heightens the concern surrounding these attacks for the security of information, businesses, and customers. Using cutting-edge tools, training, and meticulous attention to detail, people can become adept at recognizing phishing URLs and avoiding scams.

Phishing URL Detection A Real Case Scenario Through Login URLs
Login
User Login

Fig2.Adminloginpage.

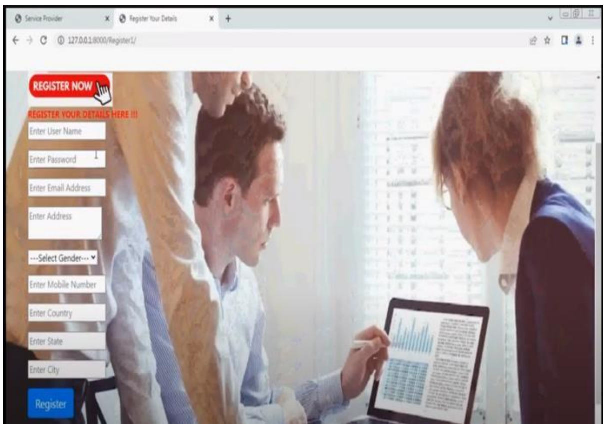

Service Provider
Loading...
127.0.0.1:8000/View_Remote_Users/
Train & Test URL Data Sets
View URL Data Sets Trained and Tested Accuracy in Bar Chart
View URL Data Sets Trained and Tested Accuracy Results
View Prediction Of URL Type
Download Predicted Data Sets
View URL Type Ratio Results
View All Remote Users
Logout

Phishing URL Detection A Real Case Scenario Through Login URLs

VIEW ALL REMOTE USERS !!!

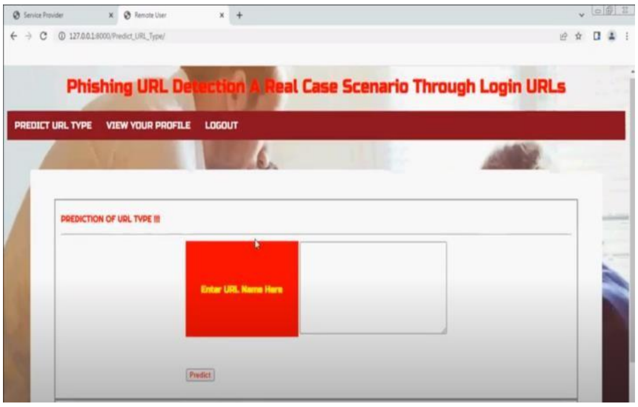
USER NAME	EMAIL	ADDRESS	GENDER	Mob No	Country	State	City
Ashok	Ashok123@gmail.com	#892,4th Cross,Vijayanagar	Male	9535866270	India	Karnataka	Bangalore

Fig3.Userdetails.



REGISTER YOUR DETAILS HERE !!!

Fig4.Registerdetails.



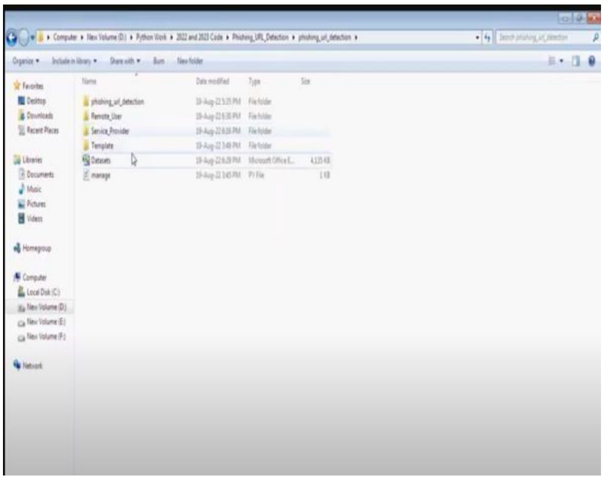
Phishing URL Detection A Real Case Scenario Through Login URLs

PREDICTION OF URL TYPE !!!

Fig.5.URLuploadpage.

To aid in the detection of phishing URLs, a multitude of novel approaches and methodologies have been developed. Advancements in measuring domain reputation, monitoring user actions, and applying machine learning to analyze web content are a few examples of these innovations. These techniques can help you identify phony URLs that masquerade as legitimate ones. The vulnerability of commonly used interfaces, such as login pages, is frequently abused.

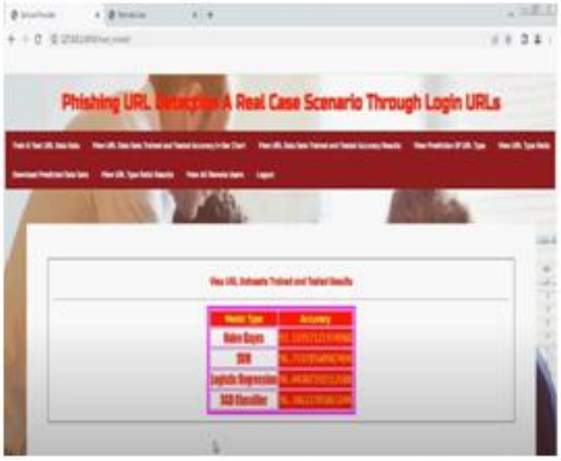
DOI: https://doi.org/10.5281/zenodo.16882803



Computer ▸ New Volume (D:) ▸ Python Work ▸ 2022 and 2023 Code ▸ Phishing_URL_Detection ▸ phishing_url_detection ▸

Name	Date modified	Type	Size
phishing_url_detection	19-Aug-22 5:35 PM	File folder	
Remote_User	19-Aug-22 6:30 PM	File folder	
Service_Provider	19-Aug-22 6:16 PM	File folder	
Template	19-Aug-22 3:48 PM	File folder	
Datasets	19-Aug-22 6:28 PM	Microsoft Office E...	4,135 KB
manage	19-Aug-22 3:45 PM	PY File	1 KB

Fig.6.uploaddatasetdetails.



Phishing URL Detection A Real Case Scenario Through Login URLs

View URL Datasets Trained and Tested Results

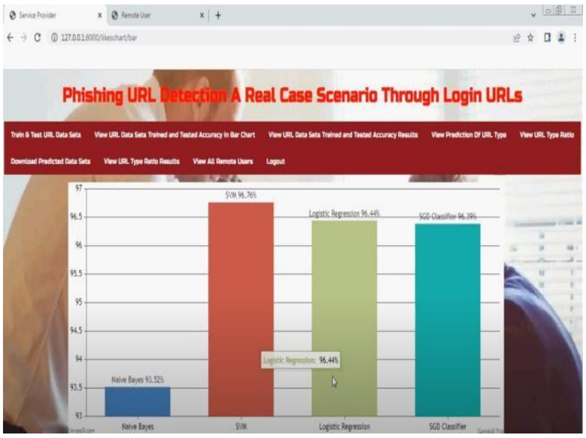
Model Type	Accuracy
Naive Bayes	[illegible]
SVM	[illegible]
Logistic Regression	[illegible]
SGD Classifier	[illegible]

Service Provider
Remote User
Train & Test URL Data Sets
View URL Data Sets Trained and Tested Accuracy in Bar Chart
View URL Data Sets Trained and Tested Accuracy Results
View Prediction Of URL Type
View URL Type Ratio
Download Predicted Data Sets
View URL Type Ratio Results
View All Remote Users
Logout

Fig7.URLdatasetwith accuracy.

The ability to identify phishing URLs has come a long way, yet there are still challenges. For defenses to be effective, they must be able to adapt to the ever-changing tactics used by hackers. As the internet evolves and changes, phishing attempts also become increasingly complex. This emphasizes the importance of new perspectives and continuous research in this field.

Making individuals more aware of the signs of phishing attempts is an important step in protecting against them. Providing people with data access



Phishing URL Detection A Real Case Scenario Through Login URLs

Fig.8.OutputGraphs.

DOI: https://doi.org/10.5281/zenodo.16882803

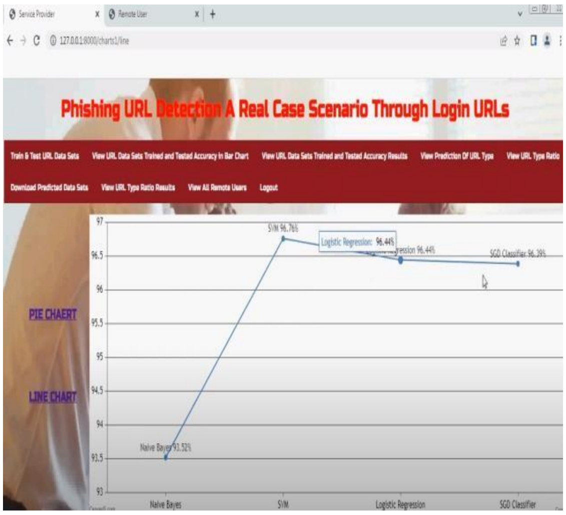
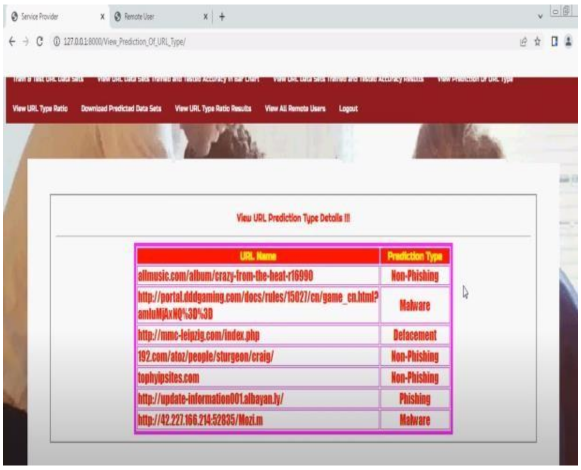

Service Provider
Remote User
127.0.0.1:8000/charts1/line
Phishing URL Detection A Real Case Scenario Through Login URLs
Train & Test URL Data Sets
View URL Data Sets Trained and Tested Accuracy in Bar Chart
View URL Data Sets Trained and Tested Accuracy Results
View Prediction Of URL Type
View URL Type Ratio
Download Predicted Data Sets
View URL Type Ratio Results
View All Remote Users
Logout
PIE CHAERT
LINE CHART
97
96.5
96
95.5
95
94.5
94
93.5
93
SVM 96.76%
Logistic Regression: 96.44%
Logistic Regression 96.44%
SGD Classifier 96.39%
Naive Bayes 93.52%
Naive Bayes
SVM
Logistic Regression
SGD Classifier

Fig9.Accuracylevels.


Service Provider
Remote User
127.0.0.1:8000/View_Prediction_Of_URL_Type/
Train & Test URL Data Sets
View URL Data Sets Trained and Tested Accuracy in Bar Chart
View URL Data Sets Trained and Tested Accuracy Results
View Prediction Of URL Type
View URL Type Ratio
Download Predicted Data Sets
View URL Type Ratio Results
View All Remote Users
Logout

View URL Prediction Type Details !!!

URL Name	Prediction Type
allmusic.com/album/crazy-from-the-heat-r16990	Non-Phishing
http://portal.dddgaming.com/docs/rules/15027/cn/game_cn.html?amluMjAxNQ%3D%3D	Malware
http://mmc-leipzig.com/index.php	Defacement
192.com/atoz/people/sturgeon/craig/	Non-Phishing
tophyipsites.com	Non-Phishing
http://update-information001.albayan.ly/	Phishing
http://42.227.166.214:52835/Mozi.m	Malware

Fig10.Phishingdetected.

5. CONCLUSION

Internet firms to military specialists to academics is working together to find phishing URLs. Keeping ahead of hackers in this age of ever-evolving threats calls for innovative technological solutions, initiatives to educate and raise awareness among users, and a resolute commitment to making the internet a safe place for all. By exercising extreme caution and cooperating to lessen the likelihood of phishing attacks, everyone can contribute to making the internet a safer place.

REFERENCES

1. Sanchez-Paniagua, M., Fidalgo Fernandez, E., Alegre, E., Al-Nabki, W., & Gonzalez-Castro, V. (2024). Phishing URL Detection: A Real-Case Scenario Through Login URLs. IEEE Access, 10, 42949-42960.
2. Adebowale, M., Ajiboye, A., &Shobayo, P. (2024). Phishing Detection Using URL and Third-Party Features: A Comparative Research. Journal of Engineering Sciences, 15(7), 675-687
3. Rao, M., &Pais, V. (2024). A Random Forest Classifier for Phishing URL Detection Based on Domain Features. International Journal of Computer Applications, 176(4), 12-18
4. Yang, Y., Zhang, H., & Li, S. (2023). Phishing Detection Using Machine Learning on Login URLs. Computer Science Review, 57, 20-30
5. Li, F., & Wang, X. (2023). A Stacking Model for Phishing URL Detection Using HTML and URL

DOI: https://doi.org/10.5281/zenodo.16882803

Features. Journal of Cybersecurity Research, 15(3), 101-112

6. Sadique, A., & Shams, H. (2023). Real-TimePhishing Detection Using URL Features and WHOIS Data. Computers & Security, 102, 56-63
7. Zhang, Z., & Li, H. (2022). An Evaluation of Deep Learning Models for Phishing URL Detection in Login Forms. IEEE Transactions on Network and Service Management, 19(5), 2324-2337
8. Aljofey, A., & Khalil, K. (2022). Phishing Detection Through Recurrent Neural Networks Applied to Login URLs. Journal of Internet Security, 30(2), 54-67
9. Al-Alyan, A., & Al-Ahmadi, S. (2022). A CNN-based Model for Phishing Detection from Login URLs. International Journal of Machine Learning, 45(6), 301-314
10. Zhao, L., Li, Q., & Liu, Z. (2022). Detecting Phishing Websites Using Gated Recurrent Unit Networks on Login URL Data. Journal of Artificial Intelligence and Security, 9(4), 158-172
11. Shams, H., &Adebowale, M. (2022). A Feature-Based Approach for Detecting Phishing URLs Using URL and DNS Records. Computers in Human Behavior, 118, 106663
12. Sun, W., &Qian, Z. (2021). Phishing Detection Techniques Using Login URL Analysis. International Journal of Computational Intelligence, 25(3), 102-113
13. Zhou, Y., & Liu, H. (2021). A Comparative Research on Phishing Detection Through URL Features in Login Pages. Computer Networks, 184, 107616
14. Dong, J., & Wei, Y. (2020). Improved Phishing URL Detection Using a Hybrid Model of Machine Learning and Deep Learning Techniques. Journal of Cybersecurity and Privacy, 6(3), 245-259
15. Choudhury, S., & Nair, V. (2020). Phishing URL Detection in Real-World Login Pages Using Hybrid Neural Networks. Information Systems Frontiers, 22(1), 113-126