Phishing detection of websites using machine learning

Dr. S. Deepika
Assistant Professor, Dept of CSE , Sreyas Institute of Engineering and Technology,
Telangana,India.

Alli Vamshi Nandhu
Dept of CSE, Sreyas Institute of Engineering and Technology,
Telangana,India.

Ramavath Teja Sree
Dept of CSE, Sreyas Institute of Engineering and Technology,
Telangana,India.

A pranay Vasanth
Dept of CSE, Sreyas Institute of Engineering and Technology,
Telangana,India.

Vallepu Om Prakash
Dept of CSE, Sreyas Institute of Engineering and Technology,
Telangana,India.

Abstract— **Phishing is a type of fraud where an attacker targets a company or a person in order to get sensitive information such as login credentials or account information via emails or other communication channels. Phishing attacks often leading to significant financial losses and data breaches. This project aims to develop a Chrome extension that can detect phishing websites in real-time, providing users with extra protection while they browse. By using machine learning algorithms, the extension examines various elements of URLs, website content, and metadata to tell apart legitimate sites from malicious ones. We train and test the model using a dataset that includes examples of both phishing and safe websites. We evaluate different machine learning techniques, like Random Forest, Support Vector Machine, and Neural Networks, to find the best approach for detecting phishing sites. The extension works seamlessly with the browser, giving users immediate warnings about suspicious websites. We measure the extension's performance using accuracy, precision, recall, and F1-score. The results show that this machine learning based Chrome extension can greatly improve the detection and prevention of phishing attacks, making online browsing safer for everyone,**

Keywords—phishing, extension, machine learning, random forest, feature extraction.

I. INTRODUCTION

Phishing can be defined as impersonating a valid site to trick users by stealing their personal data comprising usernames, passwords, accounts numbers, national insurance numbers, etc. Phishing frauds might be the most widespread cybercrime used today. There are countless domains where phishing attack can occur like online payment sector, webmail, and financial institution, file hosting or cloud storage and many others. The webmail and online payment sector was embattled by phishing more than in any other industry sector. Phishing can be done through email phishing scams and spear phishing hence user should be aware of the consequences and should not give their 100 percent trust on common security application. Machine Learning is one of the efficient techniques to detect phishing as it removes drawback of existing approach. The objectives which is the

most vital thing in proposed project is to verity the validity of the website by capturing blacklisted URLs. To notify the user on blacklisted website through pop-up while they are trying to access and to notify the user on blacklisted website through email while they are trying to access. This proposed project will allow administrator to add blacklisted URL's in order to alert user during their inquiry. The two scope of project, which is well known as user scope and system scope. User has some responsibility towards the system. The system includes a few standards and policies that requires to be obliged in order to comply the system. The user can be notified if blacklisted website is being accessed. The admin can capture the blacklisted URL's to alert user.

II. LITERATURE SURVEY

In [1], Amani Alswailem Bashayr Alabdullah Norah Alrumayh Dr. Aram Alsedrani, "Detecting Phishing Websites Using Machine Learning", IEEE 2019. The system is based on a machine learning method, particularly supervised learning. Here is selected the Random Forest technique due to its good performance in classification. The focus is to pursue a higher-performance classifier by studying the features of phishing websites and choosing the better combination of them to train the classifier. As a result, the conclusion is the paper is with an accuracy of 98.8.

In [2], safa Alrefaai, Ghina Ozdemir, Afnam Mohamed, Phishing, a cybercriminal's attempted attack, is a social web-engineering attack in which valuable data or personal information might be stolen from either email addresses or websites. There are many methods available to detect phishing, but new ones are being introduced in an attempt to increase detection accuracy and decrease phishing websites ' success to steal information. Phishing is generally detected using Machine Learning methods with different kinds of algorithms. In this study, our aim is to use Machine Learning to detect phishing websites. We used the data from Kaggle consisting of 86 features and 11,430 total URLs, half of them are phishing and half of them are legitimate. We trained our data using Decision Tree (DT), Random Forest (RF), XGBoost, Multilayer Perceptrons, K-Nearest Neighbors, Naive Bayes, AdaBoost, and Gradient Boosting and reached the highest accuracy of 96.6using X G Boost.

In [3], Phishtank was proposed to carry out the inspection once a link has been pasted on the section given. This allow user to keep on track of faked website. They can copy and paste the link in order to identify whether the site that they are going to access is safe or not safe. User can use the website search feature directly or they can use information from PhishTank through its API. A search engine displayed on PhishTank website is to be used as the first method. Using its API will be the second method. API service can be avail by software builder after registering themselves on PhishTank website. Both methods mentioned above do not cost a single penny. The purpose of API's usage is for user who has basis information on software development. Limitation of this project is there was no facility of displaying pop-up and email notification once user had access blacklisted website.

According to [4], PhishZoo was proposed to evaluate a new method for web phishing detection based on profiles of complex sites' appearance and content. PhishZoo makes profiles of sites comprising of the website contents and

images displayed. These profiles are kept in a local folder and are either synchronized against the newly loaded sites at the time of loading or against risky sites for instance, links in email offline. Limitation of this project is there was no facility of displaying pop-up and email notification once user had access blacklisted website.

From [5], A. Lakshmanarao, P. Surya, M Bala Krishna : This thesis collected a dataset of phishing websites from the UCI repository and used various Machine learning techniques, including decision trees, AdaBoost, support vector machines (SVM), and random forests, to analyze selected features (such as web traffic, port, URL length, IP address, and URL_of_Anchor). The most effective model for detecting phishing websites was chosen, and two priority-based algorithms (PA1 and PA2) were proposed. The team utilized a new fusion classifier in conjunction with these algorithms and attained an accuracy rate of 97%. when compared to previous works in phishing website detection.

As stated in [6], Arathi Krishna V, Anusree A, Blessy Jose, Karthika Anilkumar, Ojus Thomas Lee : We have moved most of our financial, work related and other daily activities to the internet, we are exposed to greater risks in the form of cybercrimes. URL based phishing attacks are one of the most common threats to the internet users. In this type of attack, the attacker exploits the human vulnerability rather than software flaws. It targets both individuals and 5 organizations, induces them to click on URLs that look secure, and steal confidential information or inject malware on our system. Different machine learning algorithms are being used for the detection of phishing URLs, that is, to classify a URL as phishing or legitimate. Researchers are constantly trying to improve the performance of existing models and increase their accuracy. In this work we aim to review various machine learning methods used for this purpose, along with datasets and URL features used to train the machine learning models. The performance of different machine learning algorithms and the methods used to increase their accuracy measures are discussed and analysed. The goal is to create a survey resource for researchers to learn the current developments in the field and contribute in making phishing detection models that yield more accurate results.

In [7], M. Aydin and N. Baykal : Throughout this experiment, phishing websites were detected using subset-based feature selection methods based on URL attributes. A dataset comprising both legitimate and phishing URLs was obtained from Google and PhishTank, and multiple features were retrieved from URLs. The usefulness of two classification algorithms—Naive Bayes and Sequential Minimal Optimization (SMO)—for identifying phishing websites was investigated in this study. The results showed that SMO performed better than Naive Bayes for phishing detection, with an accuracy rate of 95.39%. The SMO algorithm also had another benefit in that it made use of more chosen features overall. The accuracy rate of the Naive Bayes method, in contrast, was 88.17% while using the same quantity of chosen features.

In [8], M. Karabatak and T. Mustafa [25]: The objective of this research is to assess the effectiveness of classification algorithms on a condensed dataset of phishing websites obtained from the UCI Machine Learning Repository. The paper investigates how data mining and feature selection

algorithms affect reduced datasets through experiments and analysis, finally selecting the methods that perform the best in terms of classification. According to the results, some classification strategies improve performance while others have the opposite impact. Ineffective classifiers for condensed phishing datasets included Lazy, BayesNet, SGD Multilayer Perceptron, PART, JRip, J48, RandomTree, and RandomForest. However, it was discovered that KStar, LMT, ID3, and R.F.Classifier were efficient. Lazy produced the highest classification accuracy rate of 97.58% on the compressed 27-feature dataset, whereas KStar performed at its best on the same dataset.

According to [9], GoldPhish was proposed to perceive and report phishing sites. This was done by using optical character recognition (OCR) to recite the text from an image of the page precisely from the company logo, grasping the top hierarchical areas from a search engine, and comparing them with the current web site. The forte of the tool lies in the user's capability to recognize famous company logos. A phishing site cannot change a familiar company logo without the phishing target perceiving. Limitation of this project is there was no facility of displaying pop-up and email notification once user had access blacklisted website.

III.PROBLEM STATEMENT

The most frequent type of phishing assault, in which a cybercriminal impersonates a well known institution, domain, or organization to acquire sensitive personal information from the victim, such as login credentials, passwords, bank account information, credit card information, and so on. Emails containing malicious URLs in this sort of phishing email contain a lot of personalization information about the potential victim. To spear phish a "whale," here a top-level executive such as CEO, this sort of phishing targets corporate leaders such as CEOs and top-level management employees. To infect the target, the fraudster or cyber-criminal employs a URL link.

IV.WORK FLOW

The process to detect of phishing websites is as follows:

1. The user opens the chrome browser and enter the url in search bar
2. When the user enters url automatically the machine learning algorithm checks the url .
3. The backend server checks the characteristics of the url .
4. After checking the url its gives the ouput.
5. The user receives a pop up message .

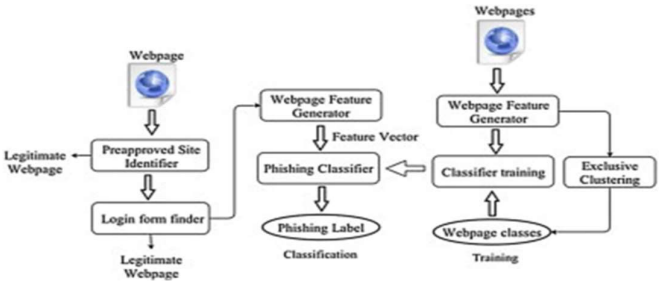

Fig 1: Architecture of the Project

1. Data collection

The process begins with the collection of data from the trusted sources and extracted the relevant features for phishing detection.

2. Machine Learning Model Development

Here choosed a light weighted machine learning models for real-time inferences like random forest and support vector machine and Neural networks for more complex patterns.

3. Chrome Extension Development

The Chrome extension will extract website features, apply the ML model for prediction, and alert the user if the site is classified as phishing and manifest the files and integrate with ML models.

4. Real Time Feature Extraction

For dynamic analysis it extracts the URL's and webpage features and it send the extracted festures to the backend of the system.

5. Output

The extension produces a pop up message that the website is phishing or not.

V.RESULT ANALYSIS

.

Figure 2 illustrates the user interface where the extension found non phishing website.

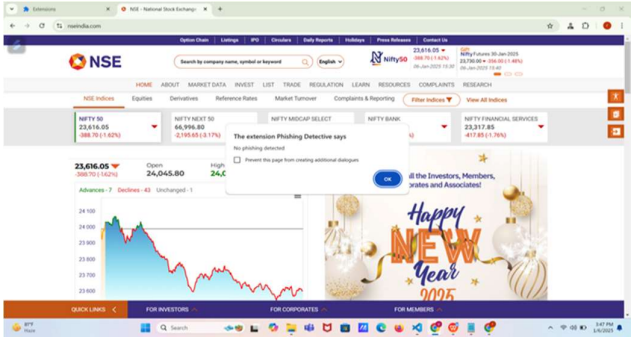

Fig 2: User Interface of Non phishing website

Figure 3 shows the detection of phishing website.

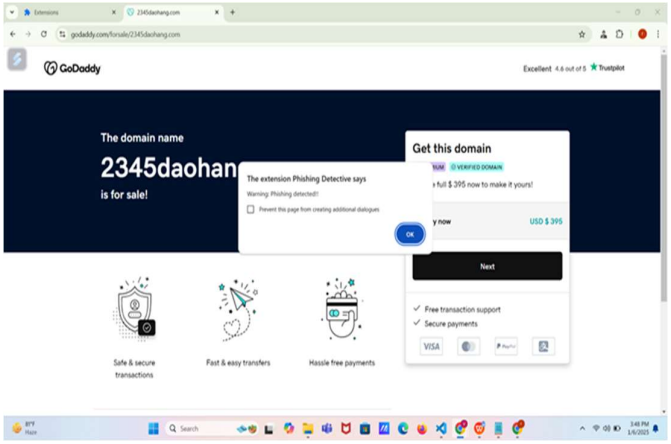

Fig 3: User Interface of detection of phishing website

VI.LIMITATIONS AND FUTURE SCOPE

Machine learning models needs of lots of updated data to stay accurate. If the data is old or in complete, the system might not detect newer phishing attacks and No matter how advanced the detection systems, user behaviour remains a significant weakness. Many users lack awareness or ignore warnings, clicking on suspicious links or entering sensitive information.

Enhancements to the Detection of phishing websites includes integration with other browsers and real-time threat intelligence using block chain technology.

VII.CONCLUSION

The challenges such as evolving phishing tactics and the need for advanced feature extraction present opportunities for further research and refinement. Future enhancements, including broader browser support, real-time threat

intelligence integration, and model optimization, can improve the tool's performance and usability. Overall, this project demonstrates a valuable step toward empowering users with accessible, automated tools to navigate the internet securely.

REFERENCES

[1] Arathi Krishna V, Anusree A, Blessy Jose, Karthika Anilkumar, Ojus Thomas Lee, " phishing detection using machine learning based url analysis".

[2] Safa Alrefaai, Ghina Ozdemir, Afnam Mohamed "Detection of phishing websites using machine learning techniques." Journal of Information Security and Applications.

[3] Kshetri, N. (2019). "Cybersecurity strategies and artificial intelligence." IT Professional, 21(4), 21-27.

[4] A. Lakshmanarao, P. S. P. Rao, and M. B. Krishna, "Phishing website detection using novel machine learning fusion approach," in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021: IEEE, pp. 1164-1169.

[5] M. Aydin and N. Baykal, "Feature extraction and classification phishing websites based on URL," in 2015 IEEE Conference on Communications and Network Security (CNS), 2015: IEEE, pp. 769-770.

[6] M. Karabatak and T. Mustafa, "Performance comparison of classifiers on reduced phishing website dataset," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018: IEEE, pp. 1-5.

[7] Ye Cao, Weili Han, "Anti -phishing based on automated individual whitelist"

[8] 14 Types of Phishing Attacks That IT Administrators Should Watch For [online] (2021)https://www.blog.syscloud.com.

[9] S. A. Anwekar and V. Agrawal, "PHISHING WEBSITE DETECTION USING MACHINE LEARNING ALGORITHMS."