ADScAI
Applied Data Science & Artificial Intelligence Symposium

AN INTELLIGENT BROWSER EXTENSION FOR PHISHING WEBSITE DETECTION USING MACHINE LEARNING MODELS

L.Y. Abeywickrama
Faculty of Information Technology
Horizon Campus
Malabe, Sri Lanka.
lochanaabeywickrama99@gmail.com

T. D. Samarasinghe
Faculty of Information Technology
Horizon Campus
Malabe, Sri Lanka.
thilina.samarasinghe@horizoncampus.edu.lk

Keywords—Phishing detection, Cybersecurity, Browser extension, Random Forest classifier, Machine Learning

I. INTRODUCTION

At present, most daily tasks are completed by websites through digital platforms. As a result, website reliability has become a significant concern in today's digital landscape [1]. Phishing is the most common type of cyberattack in today's digital environment [2]. Phishing comes in different forms, such as spear, email, whaling, and vishing [3]. In recent years, there has been an escalation in phishing attacks. One such attack is URL phishing. A URL is a website address that indicates a website's location on a network and how to access it [3]. Most of the phishers create fake websites that appear as legitimate websites.

To gather insights for my research, a questionnaire was created to assess the current status of phishing attacks in organizations. The responses indicated that phishing attacks most frequently occur within organizations. Hence, I conducted this research to provide a solution to the ongoing phishing attacks targeting websites. The main objective of this study is to develop a browser extension to detect phishing websites. Additionally, this study focuses on determining the key URL features and the most accurate classification algorithm for training the model.

The significance of this study is, it contributes to the increasing need for practical, user-friendly cybersecurity solutions to prevent phishing scams. The current situation highlights the need for advanced security mechanisms to prevent phishing attacks.

II. LITERATURE REVIEW

The literature highlights various machine learning-based approaches for phishing URL detection, focusing on feature extraction and classification techniques. Phishing detection was done using a variety of datasets, such as ISCXURL-2016, Phish Tank, Alexa, and Kaggle. Machine learning models with high classification accuracy included Random Forest, Decision Tree, SVM, and ANN [4],[5],[6]. The existing literature highlights that feature extraction is based on lexical-based features and content-based features [7]. This study is based on the UC Irvine Machine Learning Repository and uses a literature summary table to identify the most important features of the URL.

III. METHODOLOGY

A. Dataset

Data for training the machine learning model was collected from the UC Irvine Machine Learning Repository. The dataset includes 54 URL features and 235,795 URLs, including 100,945 phishing and 134,850 legitimate URLs.

B. Data Analysis

The dataset is pre-processed to handle null values, duplicates, and any invalid values. The used dataset does not contain any missing or duplicate values. However, the dataset contains categorical data and uses LabelEncoder to convert all categorical data into a numerical format. Furthermore, to classify URLs as legitimate or phishing, features were selected based on the correlation analysis results and insights from existing literature: IsHTTPS, HasSocialNet, HasCopyrightInfo, and HasDescription. The dataset is then split into two subsets: training data and testing data. Additionally, this research used three different classification algorithms to train the model using the Sklearn library in Python. They are Decision Tree (DT), Random Forest (RF), and Naive Bayes (NB).

IV. RESULTS AND EVALUATION

The Decision Tree and Random Forest achieved the highest accuracy of 96.52%, and Naive Bayes achieved 78.85%. The cross-validation results for both RF and DT models have a mean of 0.9651 and a standard deviation of ± 0.0010, indicating the highest cross-validation accuracy. Additionally, Hyperparameter Tuning is used to tune the parameters of RF and DT to select the best algorithm to train the model because these two algorithms achieve the same results in model training. The accuracy of the trained models is presented in Fig. 1.

https://doi.org/10.31705/ADScAI.2025.06

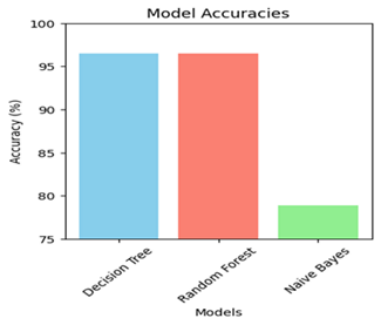

Fig. 1. The accuracy of the classification algorithms

Furthermore, the precision, recall, and F1-score have similar scores for both class 0 (phishing URLs) and class 1 (legitimate URLs), as shown in Table 1.

TABLE I. PERFORMANCE METRICS RESULTS

Algorithms	***Random Forest - RF***	***Decision Tree - DT***
Accuracy	96.52%	96.52%
Precision (0.0)	0.97	0.97
Recall (0.0)	0.94	0.94
F1-Score (0.0)	0.96	0.96
Precision (1.0)	0.96	0.96
Recall (1.0)	0.98	0.98
F1-Score (1.0)	0.97	0.97

However, in choosing the best model training algorithm, Random Forest is selected since it is an ensemble that can combine multiple decision trees by strengthening and improving the performance of the prediction, without compromising any overfitting possibilities.

Finally, a test was conducted to evaluate the performance of the browser extension in real time on 20.lk domain URLs and 20 foreign domain URLs collected from live web sources. The test was conducted to identify whether the extension was able to differentiate between legitimate .lk and foreign domains, and classify phishing and legitimate websites. The extension identified phishing and legitimate sites with 96% accuracy in both domain and dataset testing.

V. CONCLUSION

This study focused on the development of an intelligent browser extension for the detection of phishing websites using machine learning models. Three types of machine learning techniques: Decision Trees, Random Forest, and Naive Bayes, used highly correlated features to train the model: IsHTTPS, HasSocialNet, HasCopyrightInfo, HasDescription. These algorithms have been widely used in phishing detection in previous research work. However, the dataset has some limitations because it consists of more legitimate URLs than phishing URLs; the model would get biased towards the majority class. Therefore, the biased data set may cause the model to perform extremely well on the training set but poorly on unseen, real-world phishing URLs. A balanced dataset with diverse phishing and legitimate URLs will be used to avoid the aforementioned issue in the future. Additionally, the dataset is not updated with recent phishing URLs, which means the model may not detect new attack patterns. Therefore, this browser extension will be integrated with the database to capture new phishing URLs in order to overcome the aforementioned issue. In the future, this browser extension can be further developed in many areas: including some educational resources with the browser extension to create awareness among the users, integrating the browser extension with cybersecurity companies to embed it into larger security solutions, and a faster response time to detect phishing URLs in real-time.

ACKNOWLEDGMENT

I would like to extend my heartfelt gratitude to my research supervisor, Mr. T. D. Samarasinghe, for his exceptional guidance and support in this journey. His vast knowledge, feedback, and encouragement played a crucial role in maintaining the quality and direction of my work. I want to express my gratitude to the faculty lecturers for their insight, considerate critiques, and encouragement that have been so important in completing this research. Finally, I would like to express my deepest gratitude to my family and friends for their endless support, encouragement, and motivation.

REFERENCES

[1] M. Korkmaz, O. K. Sahingoz, and B. Diri, "Detection of Phishing Websites by Using Machine Learning-Based URL Analysis," in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India: IEEE, Jul. 2020, pp. 1–7. doi: 10.1109/ICCCNT49239.2020.9225561.

[2] S. Hossain, D. Sarma, and R. Joyti, "Machine Learning-Based Phishing Attack Detection," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 9, 2020, doi: 10.14569/IJACSA.2020.0110945.

[3] S. H. Ahammad, "Phishing URL detection using machine learning methods," Adv. Eng. Softw., 2022.

[4] I. M. M. Matin and B. Rahardjo, "Malware Detection Using Honeypot and Machine Learning," in 2019 7th International Conference on Cyber and IT Service Management (CITSM), Jakarta, Indonesia: IEEE, Nov. 2019, pp. 1–4. doi: 10.1109/CITSM47753.2019.8965419.

[5] J. T. Martínez Garre, M. Gil Pérez, and A. Ruiz-Martínez, "A novel Machine Learning-based approach for the detection of SSH botnet infection," Future Gener. Comput. Syst., vol. 115, pp. 387–396, Feb. 2021, doi: 10.1016/j.future.2020.09.004.

[6] D. Fraunholz, D. Krohmer, S. D. Anton, and H. Dieter Schotten, "Investigation of cybercrime conducted by abusing weak or default passwords with a medium interaction honeypot," in 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), London, United Kingdom: IEEE, Jun. 2017, pp. 1–7. doi: 10.1109/CyberSecPODS.2017.8074855.

[7] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," Expert Syst. Appl., vol. 117, pp. 345–357, Mar. 2019, doi: 10.1016/j.eswa.2018.09.029.