www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 295-297

e-ISSN : 2583-1062

Impact Factor : 5.725

DETECTING PHISHING WEBSITE AND SPAM CONTENT USING MACHINE LEARNING

Prasad N[1], Anthoni Thomas R[2], Karthikeyan D[3], Pon Pandian P[4], Sekar S[5]

[1]Assistant Professor, Department of Information Technology,
Nandha College of Technology, Perundurai 638 052, Tamilnadu, India.

[2,3,4,5]UG Students - Final Year, Department of Information Technology,
Nandha College of Technology, Perundurai 638 052, Tamilnadu, India.

ABSTRACT

This Project presents a novel approach for Detecting Phishing Websites and Spam Content using Machine Learning algorithms. Specifically, we focus on using the K-Neighbors Classifier algorithm to accurately identify and classify suspicious websites and content. Our proposed approach involves training the model on a large dataset of known Phishing Website and Spam Content, and then using the model to classify new websites and content based on their features and characteristics. We demonstrate the effectiveness of our approach through extensive experimentation and evaluation on a Real-World Dataset. Our results show that our approach is highly effective in detecting and classifying phishing websites and spam content, achieving high accuracy and low false positive rates. Overall, our projects present a promising approach to combatting web phishing attacks using machine learning techniques.

Keywords: Machine Learning, K-Neighbors (KNN) algorithm, dataset, Spam Content, Phishing Website, High Accuracy.

1. INTRODUCTION

Phishing is a type of cyber-attack that uses deceptive emails, websites, or text messages to trick users into providing sensitive information. Web Phishing is a form of cybercrime where criminals attempt to steal sensitive information such as login credentials, credit card details and personal data by discussing themselves as a legitimate entity through a Fake Website or E-mail. Web Phishing is a significant threat to individuals, Businesses and organizations; it can result in identity theft, financial losses and reputational damage. Using Machine Learning Algorithms, it is possible to detect phishing URL's and Text by analyzing the content of the messages, URL's and attachments.

2. Objectives

To develop a system that can automatically identify and classify websites and content that are designed to trick users into providing sensitive information, downloading malware, or taking other harmful actions. This can help to reduce the risk of users falling victim to phishing attacks and protect them from receiving unwanted or harmful messages.

3. LITERATURE SURVEY

Khatod, V., & Jain, P. (2020), this paper proposes a hybrid approach for detecting phishing websites using feature extraction and machine learning. This Model is based on Random Forest and it has 98.3% in Accuracy. Mani et al (2018), the ensemble strategy aided in obtaining a high accuracy score. This Model is based on Random Forest, Naive Bayes, SVM and it has 87.68% in accuracy. Kumar et al (2018), for effective spam identification use both univariate and multivariate distribution across user ratings. This Model is based on Random Forest, Naive Bayes, SVM, K-Nearest Neighbor, Decision tree and it has 76.0% in Accuracy. Watcharenwong, Saikaew (2017), Social features like comments etc., are combined with textual features yields better results. This Model is based on Random Forest and it has 91.3% in accuracy. Dewan, Kumaraguru (2015), automatic identification of spam text is done with 42 features using Machine Learning Techniques. This Model is based on Random Forest and it has 86.9% in Accuracy. Mohammed et al (2013), Instead of using spam trigger words, which may fail; a lexicon-based approach is used to filter the data. This Model is based on Naive Bayes, SVM, K-Nearest Neighbor, Decision tree and it has 85.96% in Accuracy.

4. EXISTING SYSTEM

Existing System is based on the Support Vector Machine and Random Forest Algorithm. Then it was using the Support Vector Machine for its accuracy which is best. Correct classification ratio, F1-score, Matthew's correlation, Classification ratio and False negative ratio and False alarm ratio are used to evaluate the performance of different classifiers.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 295-297

e-ISSN : 2583-1062

Impact Factor : 5.725

5. PROPOSED SYSTEM

In this project, we are using Kneighbors Classifier and SVM algorithm. When we are using the Kneighbors Classifier algorithm then its accuracy is best. In this project, we have provided URL and Phishing website data as input. Then we detect the output whether the provided input is a Phishing website or Not. And also we detect the output whether the text data is Spam or Not.

6. SYSTEM FLOW DIAGRAM

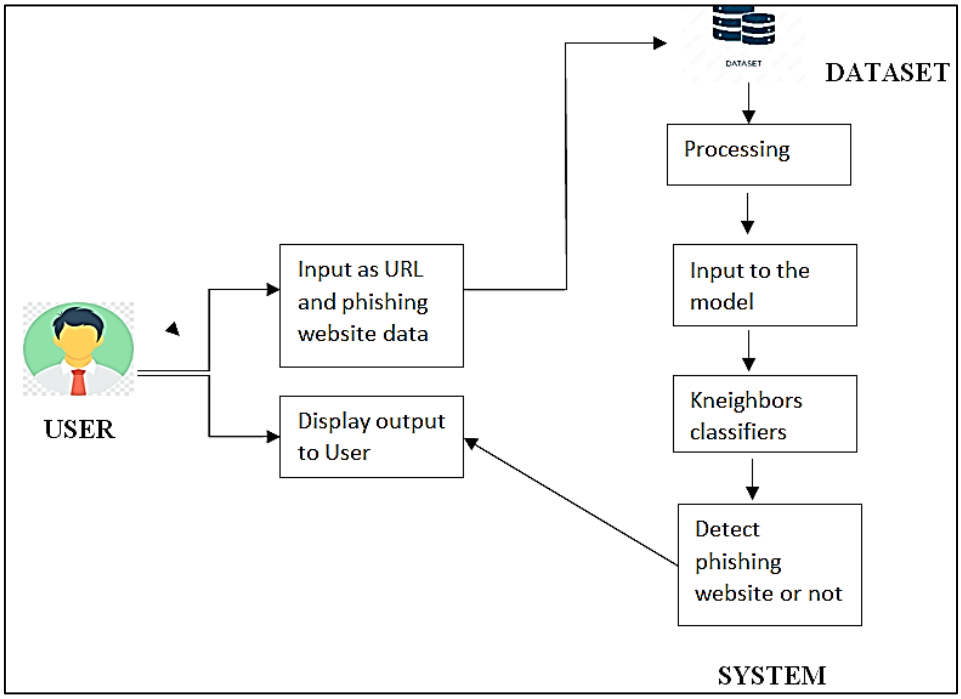

Figure 1. System Flow Diagram

7. METHODOLOGY

7.1 Modules

User Registration and Login, Spam Text Detection, Phishing URL Detection and Chat Bot.

7.1 User Registration and Login

In this module, the user authenticates the website by register and login it. User Registration is required to create new login. In the registration the user have to give username, E-mail id and password. These details are stored into the database. User has to Login after Registering.

7.2 Spam Text Detection

In this module, the user can click the Text detection button for to detect the Spam text or Spam content. After clicking the button, the user can enter the website content or any other message content in the empty dialog box. That message content is accepted to detect as Spam content or Normal sentence.

7.3 Phishing URL Detection

In this module, the user can click the URL detection button for to detect the Phishing website. After clicking the button, the user can enter the website URL or message URL in the empty dialog box. That URL is taken to detect whether it is a phishing website or not.

7.4 Chat Bot

In this module, the user can click the Chat icon for asking queries. After clicking that icon, the user can ask their queries by chatting to that bot.

8. ALGORITHM

K-nearest neighbors (KNN) is a simple and intuitive machine learning algorithm used for classification and regression tasks. It belongs to the family of instance-based learning or lazy learning algorithms. In classification tasks, the goal of KNN is to predict the class of an input data point based on the classes of its neighboring data points. The algorithm uses the distance between data points to determine which points are closest to the input data point. K-nearest neighbors (KNN) algorithm can be used for detecting phishing URLs and spam content using machine learning. The algorithm works by comparing the features of new URLs/content to the features of known phishing URLs/content.

The algorithm then classifies the new URLs/content as either legitimate or phishing/spam based on the similarity of their features.

Step 1: Import the Dataset.

Step 2: Read the Dataset.

Step 3: Extract the data from the dataset for preprocessing.

Step 4: Make predictions for the test dataset.

Step 5: Applying Machine Learning algorithms to the dataset.

Step 6: Predict the best accuracy algorithms form ML algorithm.

9. RESULTS

Machine learning algorithms were imported using the Scikit-learn library. The classifiers were trained on a set of data, and their performance was evaluated using a separate testing set. The accuracy scores of the classifiers were measured to evaluate their effectiveness.

10. CONCLUSIONS

In conclusion, machine learning algorithms, such as K-nearest neighbors(KNN), can be used to detect phishing URL's and Spam Content. These algorithms work by comparing the features of new URL's or content to the features of known phishing URL's or content and classifying them as either legitimate or phishing/spam based on their similarity. However, it's important to note that no machine learning model is 100% accurate, and attackers are constantly evolving their tactics to avoid detection. Therefore, it's essential to use multiple approaches and techniques, including training staff on how to identify phishing and spam, implementing multi-factor authentication, and using email filtering software to reduce the risk of phishing and spam attacks. Overall, machine learning algorithms can provide valuable assistance in detecting phishing and spam, but they should be used in combination with other security measures to create a comprehensive security strategy.

11. REFERENCES

[1] Almeida, T. A., Gómez Hidalgo, J. M., & Yamakami, A. (2011). Contributions to the study of SMS spam filtering: New collection and results. Journal of Machine Learning Research.

[2] Alzahrani, A., & Yoo, P. D. (2021). Deep learning-based phishing detection techniques: A comprehensive review. Journal of Information Processing Systems.

[3] Bilenko, M., & Mooney, R. J. (2003). Adaptive duplicate detection using learnable string similarity measures. In Proceedings of the 6th International Conference on Discovery Science.

[4] Guzella, T. S., & Caminhas, W. M. (2009). A review of machine learning approaches to spam filtering. Expert Systems with Applications.

[5] Kumar, A., Kant, K., & Gupta, B. B. (2018). A machine learning approach for phishing detection using novel features. Expert Systems with Applications.

[6] Li, Y., Li, J., Li, K., & Li, J. (2019). A machine learning-based approach for phishing websites detection. Journal of Intelligent & Fuzzy Systems.

[7] Mani, G. K., Reddy, B. K., & Kumar, G. P. (2018). Hybrid approach for detecting phishing websites using machine learning and rule-based techniques. International Journal of Computer Applications.

[8] Schneider, J., Martinez-Romo, J., & Almeida, T. A. (2017). Toward effective SMS spam filtering: A review of state-of-the-art techniques and trends. IEEE Transactions on Systems, Man and Cybernetics Systems.

[9] Zhang, W., Zhang, H., Hu, B., & Cheng, X. (2017). Deep learning for detecting SMS spam. In 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC).

[10] Zhu, X., & Yao, H. (2019). A phishing detection method based on SVM optimized by particle swarm optimization algorithm. Journal of Ambient Intelligence and Humanized Computing.