PhishSpotter

Table of Contents

1 Motivation

Phishing websites are increasingly common and dangerous, as they trick people into providing sensitive information like passwords and financial details. These sites often look like legitimate ones, making it hard for users to detect the threat. As online transactions grow, detecting these phishing sites becomes more critical for protecting users. Our motivation is to create a solution that can keep up with the constantly changing nature of phishing websites. By using machine learning algorithms, we aim to build a model that can accurately detect phishing websites and help improve online security [1].

This project will develop a machine learning model that takes 30 features, such as URL structure and domain information, as input. The model will output a binary classification: 1 for legitimate websites and -1 for phishing websites. This process is illustrated in Figure 1.

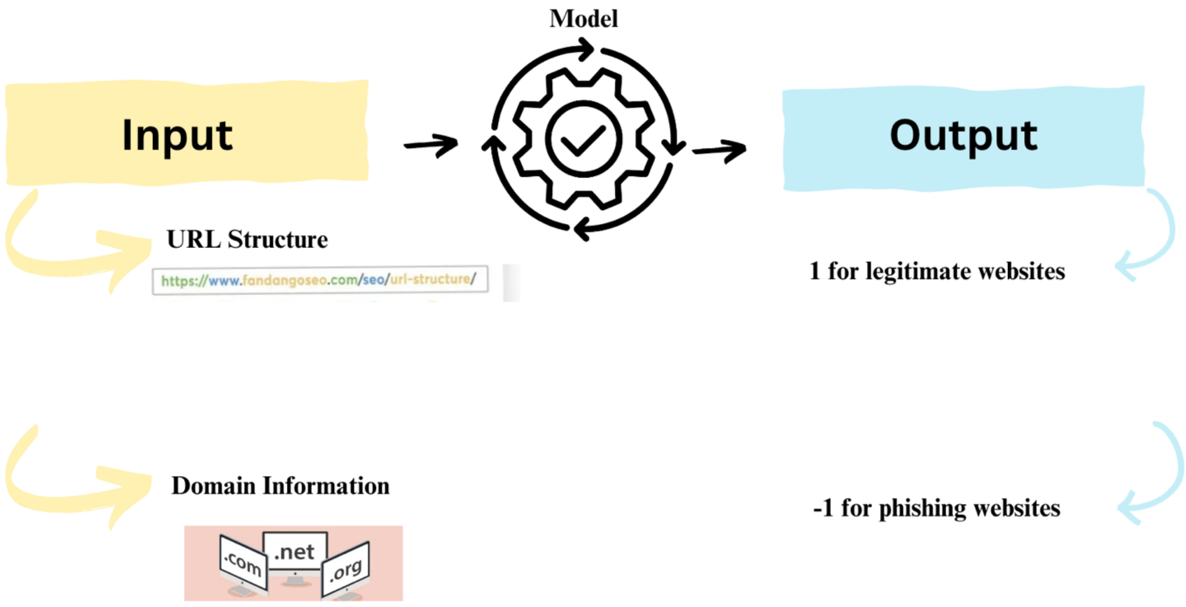

Figure 1.An illustration of the task

2 Background

As techehnology evolves, phishing attacks are becoming common in the digital world. These attacks trick users into providing sensitive information by imitating legitimate websites. Cybersecurity measures such as machine learning and artificial intelligence have become essential tools for enhancing online safety. By leveraging these technologies, we can detect phishing attempts and attacks more accurately and in real time, providing a higher level of protection for users in today’s world.

In this project, we use the Phishing Websites Dataset, which has been specifically curated to train and test phishing detection models. The goal is to accurately classify websites as either legitimate or phishing. To achieve this, we use a binary classification model based on 30 features, including URL structure, domain information, and web page characteristics. These features are key indicators of phishing detection, allowing the model to distinguish between phishing and legitimate sites. It involves extracting relevant features from websites and applying machine learning techniques to classify them as either legitimate (1) or phishing (-1).

In the next section, we will explore how previous research has approached phishing detection using different machine learning methods.

1. In this paper [2], they have explored how well to classify phishing URLs from the given set of URLs containing benign and phishing URLs. They use feature extraction using lexical analysis which includes domain names subdomains and other components, they trained different classifiers e.g. Logistic Regression, Naïve Bayes Classifier, Random Forest, Decision Tree and KNearest Neighbor. The performance metrics show that all classifiers are suitable for the phishing URL detection tasks, the classifiers Random Forest and Gaussian Naïve Bayes classifiers result in better accuracies of about 98%. The Area Under the Curve (AUC) values were similar for all classifiers, but Gaussian Naïve Bayes had the highest AUC of 0.991, making it the most suitable model for phishing URL classification in this experiment.

2. This study is about phishing website detection [3], it compares 16 machine learning classifiers using semantic features such as URL and domain identity, HTML, and JavaScript characteristics. The best classifiers, Gradient Boosting and Random Forest, achieved about 97% accuracy. Meanwhile, models like GaussianNB and Stochastic Gradient Descent underachieved. The research demonstrates the effectiveness of semantic features in classifying phishing websites and highlights the growing threat of phishing attacks due to increasingly advanced techniques.

3. The paper's [4] author tried to address phishing attacks, an increasingly concerning problem in cybersecurity. The document focuses on identifying phishing attacks through machine learning (ML) methodologies. The author's proposed the development of a model using machine learning algorithms, Random Forest (RF) and Decision Tree (DT), for the detection of phishing websites. The dataset used covered many features related to phishing websites. Feature selection approaches, including Principal Component Analysis (PCA), have been used to enhance accuracy and minimize unnecessary data. To solve this problem, the author created a model using two machine learning algorithms, Random Forest and Decision Tree, to classify phishing websites. For the feature selection, PCA was performed to identify significant features from the dataset, hence minimizing redundancy. The model's accuracy and performance were assessed by a confusion matrix, which measured accuracy, precision, recall, and F1 score. Random Forest attained an accuracy of 97%, which shows that the model is more capable of managing overfitting compared to Decision Trees.

3 Dataset

Our dataset consists of 11,055 instances, each defined by 30 attributes that describe various characteristics of websites, crucial for distinguishing between legitimate sites and phishing sites. We selected this comprehensive dataset from Kaggle [5] because it offers a broad and detailed spectrum of data points, essential for training our phishing detection model with high accuracy. Developing this model is vital as phishing attacks continue to be a significant threat to online security, causing substantial financial and data losses each year. By improving our ability to detect and prevent phishing attempts, we not only enhance web security but also safeguard personal and organizational assets against cyber threats. This dataset is pivotal for our project as it forms the foundation for developing and refining our ability to effectively detect phishing websites. Table 1 shows the summary statistics of the subset of the dataset we will be using.

Attribute	Description
Number of instances	11,055
Number of attributes	30

Table 1. Dataset summary statistics

4 Contributions

Name	ID	Responsibilities
Lina Alharbi	443201045	Motivation
Leen Alqahtani	443200591	Background (Part1& Part2 point1)
Jaida Alfadda	443200581	Background (Part1& Part2 point2)
Dana Alomar	443203037	Dataset
Aafia Ghulam	443203869	Background (Part2 point3)

Table 2.Contributions

5 References

[1] ChatGPT, "Phishing websites are increasingly common and dangerous," OpenAI, Sep. 2024. [Online]. Available: https://chat.openai.com/

[2] J. Kumar, B. Rajendran, A. Santhanavijayan, B. Bindhumadhava, and B. Janet, “Phishing Website Classification and Detection Using Machine Learning,” 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, Jan. 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104162. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9375997.

[3] A. Almomani, M. Alauthman, M. T. Shatnawi, M. Alweshah, A. Alrosan, W. Alomoush, and B. B. Gupta, "Phishing website detection with semantic features based on machine learning classifiers: A comparative study," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 18, no. 1, pp. 1-24, 2022. Available: https://www.igi-global.com/article/phishing-website-detection-with-semantic-features-based-on-machine-learning-classifiers/297032

[4] M. N. Alam, D. Sarma, F. F. Lima, I. Saha, R. -E. -. Ulfath and S. Hossain, "Phishing Attacks Detection using Machine Learning Approach," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 1173-1179. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9214225.

[5] A. Kumar, "Phishing Website Dataset," Kaggle, 2020. [Online]. Available: https://www.kaggle.com/datasets/akashkr/phishing-website-dataset/data . [Accessed: Sep. 15, 2024].