Vol-08 Issue 11, November -2024 ISSN: 2456-9348
Impact Factor: 7.936

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

PHISHTOR: A PHISHING SITE DETECTION BROWSER EXTENSION

Trupti Firke
Assistant Professor, D Y Patil College of Engineering Akurdi, Pune
Yash Ithape
Bharti Ghule
Komal Gawande
Mansi Kawtikwar
UG Student, D Y Patil College of Engineering Akurdi, Pune

ABSTRACT
Phishing is defined as mimicking a creditable company's website aiming to take private in- formation of a user. In order to eliminate phishing, different solutions proposed. However, only one single magic bullet cannot eliminate this threat completely. Data mining is a promising technique used to detect phishing attacks. In this paper, an intelligent system to detect phishing attacks is presented. We used different data mining techniques to decide categories of websites: legitimate or phishing. Different classifiers were used in order to construct accurate intelligent system for phishing website detection. Classification accuracy, area under receiver operating characteristic (ROC) curves (AUC) and F measure is used to evaluate the performance of the data mining techniques. Results showed that Random Forest has outperformed best among the classification methods by achieving the highest accuracy 97.36%. Random forest runtimes are quite fast, and it can deal with different websites for phishing detection.

Keywords:
Web threat; Phishing Website; Random Forest Classifier; Data Mining Techniques.

INTRODUCTION
Various web threats can lead to identity theft, the theft of private information, financial loss, and diminished trust in online banking and e-commerce, raising concerns about the reliability of the internet for commercial transactions. One such threat is phishing, which involves the act of impersonating a legitimate company's website. Fraudsters create phishing sites that closely resemble genuine websites, deceiving unsuspecting users. With the increasing number of phishing sites, this has become a serious issue, even for experienced computer users. Detecting phishing attacks is vital for secure online transactions, as many users believe they are protected simply by using anti-phishing tools. Phishing attacks typically begin with an email that appears to be from a trusted company, prompting victims to update or confirm personal information via a link in the email. Phishers use various techniques to create phishing sites, making it increasingly difficult to identify them. Two primary methods are employed to differentiate between legitimate and phishing websites: the first checks whether the URL is on a blacklist, while the second, meta-heuristic method, gathers features from the website to classify it as either legitimate or phishing. The effectiveness of meta-heuristic methods depends on extracting distinguishing features to differentiate between the two types of sites.

Data mining techniques are commonly used to extract features and uncover patterns or relationships between them. These techniques are crucial for decision-making, as they provide rules based on the data for classification. In this paper, we compare various data mining algorithms for detecting phishing websites and evaluate their performance using classification accuracy, ROC curve analysis, and F-measure. The paper is structured as follows: Section II reviews related work and methods for phishing detection. Section III outlines the features and methods used for phishing detection. Section IV presents the experiments and results of the classification algorithms, and Section V concludes the paper.

OBJECTIVES
A key objective of the research is to determine which classification model is most effective in distinguishing phishing websites from legitimate ones. Through rigorous testing, the authors find that the Random Forest classifier achieves the highest accuracy rate at 97.36%. This model also excels in speed and robustness, making

it particularly suited for phishing detection. Random Forest’s ensemble approach, which combines multiple decision trees to make final classifications, helps to improve accuracy and reduce errors by considering diverse attributes.

The study also highlights the importance of using a comprehensive dataset for evaluating classifier performance. The researchers use a publicly available phishing website dataset from the UCI Machine Learning Repository, ensuring that the system can analyze a wide variety of phishing characteristics. The paper ultimately aims to contribute a more reliable, efficient browser extension tool capable of detecting phishing sites, thereby improving online security and helping users avoid falling victim to phishing attacks.

RELATED WORKS

Aburrous et al. [7] proposed an intelligent system for detecting phishing webpages in e banking, combining fuzzy logic with data mining algorithms to identify phishing site characteristics and categorize phishing types. Using 10-fold cross-validation, they achieved a classification accuracy of 86.38%, which is relatively low. He et al. [8] developed a model that uses HTTP transactions, page content, and search engine results to detect phishing pages, reaching a classification accuracy of 97%. Arade et al. [9] introduced an intelligent algorithm based on approximate string matching to compare webpage addresses with a database, though it raised concerns about false positives, where legitimate pages might be flagged as phishing sites. Shahriar & Zulkernine [10] proposed a model that evaluates webpage reliability using a finite state machine to trace webpage behavior, from submission to response. Ajlouni et al. [11] presented the MCAR method, building on Aburrous et al.'s features and achieving 98.5% accuracy, although the number of rules extracted using MCAR was not specified. Barraclough et al. [12] proposed a Neuro-Fuzzy classifier with five inputs for phishing detection, achieving an accuracy of 98.5%. Ramesh et al. [13] suggested an approach that distinguishes direct and indirect links of a webpage, relying on third-party DNS lookup and search engine results, achieving a 99.62% accuracy. However, their method depends on external sources and fails to detect phishing pages hosted on compromised domains. Mohammed et al. [6] introduced a model using conventional features and associative classification algorithms, with C4.5 yielding an average error rate of 5.76%. Abdelhamid et al. [14] proposed a Multi-label Classifier based Associative Classification (MCAC) to extract rules from training data, achieving 97.5% accuracy but requiring a large number of rules. Zhang et al. [15] applied Sequential Minimal Optimization classifiers with five features to detect Chinese phishing sites, although the model is limited to Chinese-language pages. Li et al. [17] used transductive support vector machines to classify phishing webpages, extracting features from web page images. Montazer et al. [18] combined fuzzy logic with rough sets-based data mining for phishing detection. Li et al. [19] proposed a method based on differences between phishing sites and their targets, using a ball-based SVM algorithm to distinguish phishing sites. Moghimi et al. [16] employed approximate string matching for page resource elements and hyperlinks, instead of direct comparisons.

METHODOLOGY AND METHODS

A. Phishing Data Websites

For this research, we employed the publicly available phishing website dataset from the UCI Machine Learning Repository [20], contributed by Mohammad et al. [21][22][23][1]. The dataset features are detailed in [22].

B. Artificial Neural Networks (ANNs)

Artificial Neural Networks (ANNs) are modeled after biological neural networks, comprising interconnected nodes (neurons). The connections between nodes have assigned weights that are adjusted during the learning phase to optimize predictions. Although ANNs are often criticized for long training times and limited interpretability, their strengths lie in pattern recognition, clustering, and classification, even for previously unseen data. Their parallel nature facilitates faster computations, and rule extraction can also be performed through specific techniques. These characteristics make ANNs valuable for classification tasks and numerical predictions in data mining [5].

C. K-Nearest Neighbour(KNN)

The k-NN algorithm operates by comparing a test instance to training instances based on their similarity, typically using distance metrics. Each attribute is treated equally, which can lead to decreased accuracy when handling noisy or irrelevant data. However, methods such as pruning and data editing can help address this issue. The optimal number of neighbors can be determined through experimentation, with the value that minimizes the error rate chosen for the classification task [5].

D. Support Vector Machine(SVM)

Support Vector Machines (SVMs) classify both linear and nonlinear data by transforming the input into a higher-dimensional space, where a hyperplane is determined to separate the data into different classes. SVMs are highly effective for binary classification problems but can be computationally expensive with large datasets. Additionally, SVM performance can vary depending on kernel choice, and further research is necessary to enhance efficiency in handling multiclass data and selecting optimal kernels for specific datasets [5].

E. C4.5 Decision Tree

A decision tree is a directed graph where internal nodes represent tests, and terminal nodes hold class labels. Branches indicate the outcomes of tests, with the root node being the starting point. Decision trees are popular because they are easy to interpret, require no domain expertise, and can handle both categorical and numerical data. They perform recursive splitting of the dataset from the root node, but pruning is necessary to eliminate noise and outliers. Two types of pruning exist: pre pruning (halting node splitting) and post-pruning (removing subtrees from a fully grown tree) [24].

F. Random Forests (RF)

Random Forests, introduced by Leo Breiman, create an ensemble of uncorrelated decision trees through random attribute selection and bagging. In this approach, the input traverses through multiple trees, and the final classification is determined by averaging the outputs or using a majority vote for categorical data. This ensemble method reduces overfitting seen in single decision trees and enhances classification accuracy. The strength of Random Forests relies on the independence of individual classifiers and their ability to work together to produce more robust results [5].

G. Rotation Forest (RoF)

Rotation Forest (RoF) is an ensemble classifier that splits the feature set into K subsets and applies Principal Component Analysis (PCA) to each subset before training classifiers. Building on the Random 2 Forest concept but focusing on feature extraction, RoF has shown to deliver better accuracy. By rotating the feature space, RoF encourages both accuracy and diversity among classifiers. Each classifier is trained in parallel using bootstrap samples, and the ensemble method ensures high accuracy by creating multiple diverse classifiers simultaneously [26][27].

RESULTS AND DISCUSSION

This study evaluates the performance of various machine learning models using publicly available phishing website datasets from the UCI Machine Learning Repository. The performance of the classifiers was assessed using the open-source WEKA machine learning tool, where metrics such as accuracy, F-measure, and the area under the ROC curve (AUC) were tested. All classification models were evaluated using 10-fold cross-validation. Accuracy was used as the primary metric to measure classifier performance. The accuracy is calculated using the formula:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

where TP, TN, FP, and FN represent the number of true positives, true negatives, false positives, and false negatives, respectively. Additionally, the AUC (Receiver Operating Characteristic curve) was used to assess classifier performance, where a higher AUC indicates better prediction reliability. The F measure was also used to evaluate the classifiers, defined as:

$$F\text{-measure} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

where Precision and Recall are calculated using the formulas:

$$\text{Precision} = \frac{TP}{TP + FP}, \quad \text{Recall} = \frac{TP}{TP + FN}$$

Several machine learning classifiers were tested, including Artificial Neural Networks (ANN), k Nearest Neighbors (k-NN), Support Vector Machines (SVM), C4.5 Decision Tree, Random Forest (RF), and Rotation Forest (RoF). The results, shown in Table 1, reveal that Random Forest achieved the highest classification accuracy at 97.36%, followed closely by k-NN at 97.18%. Other classifiers performed as follows: SVM at 97.17%, ANN at 96.91%, Rotation Forest at 96.79%, C4.5 at 95.88%, CART at 95.79%, and Naive Bayes (NB) at 92.98%.

The F-measure results were consistent with the accuracy results, showing that Random Forest achieved the highest F-measure of 0.974, matching its accuracy. This consistency in results across different evaluation metrics further confirms the reliability of the Random Forest classifier. The AUC values corroborated these findings, with Random Forest obtaining the highest AUC of 0.996, followed by ANN (0.995), Rotation Forest (0.994), k-NN (0.989), C4.5 (0.984), CART and NB (0.981), and SVM (0.970).

Overall, the performance of the classifiers— measured through accuracy, F-measure, and AUC— demonstrated that machine learning algorithms are highly effective in detecting phishing attacks. The results consistently indicated that Random Forest is the most reliable model for phishing detection, but other models also showed strong performance, proving the effectiveness of machine learning tools in combating phishing threats.

ACKNOWLEDGEMENT

We extend our heartfelt thanks to all those who supported us throughout this project, undertaken as part of the B.E. Information Technology Engineering curriculum. We express our sincere gratitude to our Project Guide, Trupti Firke, and to Dr. Preeti Patil, Head of the Department of Information Technology, for their invaluable assistance and willingness to help with a wide range of challenges encountered during the project. We also wish to thank the department staff and our colleagues who contributed directly or indirectly to the successful completion of this project. Above all, we are grateful to our families for their support and encouragement, and to God for His guidance.

CONCLUSION

Phishing is a deceptive tactic that involves fake emails and websites to steal individuals' personal information, disrupting their ability to engage in online activities. Detecting phishing websites is essential for the online community due to its significant impact on e-commerce and other web-based transactions. Random Forest (RF) is a machine learning technique that has gained attention for its speed and high classification accuracy. In this research, we developed a machine learning model to analyze the relationships between features of phishing websites and extract simple, effective rules for detection. We utilized an RF classifier model to automatically and intelligently identify phishing websites using a publicly available dataset. The proposed RF model demonstrated high performance in classification accuracy, F-measure, and AUC. Additionally, our findings indicate that RF is faster, more robust, and more accurate compared to other classifiers. The Random Forest algorithm performs efficiently, detecting phishing websites more swiftly than alternative models.

REFERENCES

[1] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Predicting phishing websites based on self-structuring neural network,” Neural Comput. Appl., vol. 25, no. 2, pp. 443–458, 2014.
[2] S. Gastellier-Prevost, G. G. Granadillo, and M. Laurent, “Decisive heuristics to differentiate legitimate from phishing sites,” presented at the Network and Infor- mation Systems Security (SAR-SSI), 2011 Conference on, 2011, pp. 1–9.
[3] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, “Canti- na+: A feature-rich machine learning framework for de- tecting phishing web sites,” ACM Trans. Inf. Syst. Secur. TISSEC, vol. 14, no. 2, p. 21, 2011.
[4] N. Sanglerdsinlapachai and A. Rungsawang, “Using domain top-page similarity feature in machine learning- based web phishing detection,” presented at the Knowledge Discovery and Data Mining, 2010. WKDD’10. Third International Conference on, 2010, pp. 187–190.
[5] J. Han, J. Pei, and M. Kamber, Data mining: concepts and techniques. Elsevier, 2011.
[6] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Intelligent rule-based phishing websites classification,” IET Inf. Secur., vol. 8, no. 3, pp. 153–160, 2014.
[7] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, “Intelligent phishing detection system for e-banking us- ing fuzzy data mining,” Expert Syst. Appl., vol. 37, no. 12, pp. 7913–7921, 2010.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[8] M. He et al., "An efficient phishing webpage detector," Expert Syst. Appl., vol. 38, no. 10, pp. 12018–12027, Sep. 2011.
[9] M. S. Arade, P. Bhaskar, and R. Kamat, "Antiphishing model with url & image based webpage matching," Int. J. Comput. Sci. Technol. IJCST, vol. 2, no. 2, pp. 282– 286, 2011.
[10] H. Shahriar and M. Zulkernine, "Trustworthiness testing of phishing websites: A behavior model-based ap- proach," Spec. Sect. SS Trust. Softw. Behav. SS Econ. Comput. Serv., vol. 28, no. 8, pp. 1258–1271, Oct. 2012. M. I. A. Ajlouni, W. Hadi, and J. Alwedyan, "Detecting phishing websites using associative classification," Im- age (IN), vol. 5, no. 23, 2013.
[11] M. I. A. Ajlouni, W. Hadi, and J. Alwedyan, "Detecting phishing websites using associative classification," Im- age (IN), vol. 5, no. 23, 2013.
[12] P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," Expert Syst. Appl., vol. 40, no. 11, pp. 4697–4706, Sep. 2013.
[13] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," Decis. Support Syst., vol. 61, pp. 12–22, May 2014.
[14] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," Expert Syst. Appl., vol. 41, no. 13, pp. 5948–5959, 2014.
[15] D. Zhang, Z. Yan, H. Jiang, and T. Kim, "A domain- feature enhanced classification model for the detection of Chinese phishing e-Business websites," Inf. Manage., vol. 51, no. 7, pp. 845–853, 2014.
[16] M. Moghimi and A. Y. Varjani, "New rule-based phish- ing detection method," Expert Syst. Appl., vol. 53, pp. 231–242, 2016.
[17] Y. Li, R. Xiao, J. Feng, and L. Zhao, "A semi-supervised learning approach for detection of phishing webpages," Opt.-Int. J. Light Electron Opt., vol. 124, no. 23, pp. 6027–6033, 2013.
[18] G. A. Montazer and S. ArabYarmohammadi, "Detection of phishing attacks in Iranian e-banking using a fuzzy– rough hybrid system," Appl. Soft Comput., vol. 35, pp. 482–492, 2015.
[19] Y. Li, L. Yang, and J. Ding, "A minimum enclosing ball based support vector machine approach for detec- tion of phishing websites," Opt.-Int. J. Light Electron Opt., vol. 127, no. 1, pp. 345–351, 2016.
[20] "UCI Machine Learning Repository: Phishing Websites Data Set." [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Phishing+Website s#. [Accessed: 29-Jan-2017].
[21] R. M. Mohammad, F. Thabtah, and L. McCluskey, "An assessment of features related to phishing websites using an automated technique," presented at the Internet Tech- nology And Secured Transactions, 2012 International Conference for, 2012, pp. 492–497.
[22] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Phishing websites features," Unpubl. Available Httpe- prints Hud Ac Uk243306RamiPhishingWebsitesFeatures Pdf, 2015.
[23] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Intelligent rule-based phishing websites classification," IET Inf. Secur., vol. 8, no. 3, pp. 153–160, 2014.
[24] M. Hall, I. Witten, and E. Frank, "Data mining: Practical machine learning tools and techniques," Kaufmann Bur- lingt., 2011.
[25] L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.
[26] L. I. Kuncheva and J. J. Rodríguez, "An experimental study on rotation forest ensembles," presented at the MCS, 2007, pp. 459–468.
[27] J. J. Rodriguez, L. I. Kuncheva, and C. J. Alonso, "Rota- tion forest: A new classifier ensemble method," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 10, pp. 1619–1630, 2006.
[28] J. A. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic (ROC) curve.," Radiology, vol. 143, no. 1, pp. 29–36, 1982.
[29] N. A. Obuchowski, "Receiver Operating Characteristic Curves and Their Use in Radiology 1," Radiology, vol. 229, no. 1, pp. 3–8, 2003.
[30] J. A. Swets, "ROC analysis applied to the evaluation of medical imaging techniques.," Invest. Radiol., vol. 14, no. 2, pp. 109–121, 1979.