International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 10 | Oct 2023 www.irjet.net p-ISSN: 2395-0072

Detection of Malicious Web Links Using Machine Learning Algorithm: A Review

Shailja S. Panhalkar, Vanashri S. Shinde, Rucha A. Gurav and Rohit S. Barwade

Computer Science & Engineering
Dr. D.Y. Patil Pratishthan's College of Engineering Salokhenagar, Affiliated to Shivaji University Kolhapur, Maharashtra, India

---

Abstract: This review paper examines the various machine learning techniques used to detect malicious web links. With the rise of cybercrime, malicious web links have become a major threat to online security. Traditional signature-based detection methods have become inadequate as attackers have developed sophisticated techniques to evade detection. Machine learning techniques such as decision trees, support vector machines, and deep learning are increasingly used to improve the accuracy of malicious web link detection. The article discusses the strengths and limitations of these techniques and provides insight into their implementation. The review also discusses issues that arise when using machine learning to detect malicious web links, such as the imbalance of datasets and the interpretability of models. Overall, the paper highlights the potential of machine learning techniques to combat the threat of malicious web links and identifies areas for further research.

Keywords: Malicious URL Detection, Machine Learning, web link, unsupervised learning, cybersecurity.

I. INTRODUCTION

Attackers commonly attempt to alter one or more elements of the URL structure in an attempt to trick users into sharing their malicious URL. Excluding URLs are dangerous links for users. These URLs link users to sites or resources where hackers can install malware on their computers, redirect users to unwanted websites, malicious websites, or other phishing websites. Additionally, malicious URLs can be disguised as seemingly secure download links and spread rapidly by exchanging files and messages on open networks. Spam, phishing, and social engineering are a few attack techniques that use malicious URLs. The growing use of the Internet has led to an exponential increase in web threats, including malicious web links. Malicious web links can cause significant harm to users by infecting their devices with malware, stealing their personal information, or redirecting them to fraudulent websites. Therefore, the detection and prevention of these links is essential to keep Internet users safe.

Machine learning has shown promise as a technique for detecting malicious web links due to its ability to learn from data and identify patterns that are difficult for traditional rule-based methods to capture. This review paper aims to provide an overview of recent advances in machine learning techniques for detecting malicious web links.

The article will begin by discussing the traditional methods used to detect malicious web links and then dive into the various machine learning techniques used for this purpose. The study will focus on comparing different machine learning techniques, evaluation metrics and datasets used to detect malicious web links.

The review paper will also highlight the challenges facing researchers in this area and outline potential future directions for the development of machine learning techniques to detect malicious web links.

Overall, this review paper will provide a comprehensive understanding of the current state of the art in machine learning for malicious web link detection and will serve as a valuable resource for cybersecurity researchers and practitioners.

II. LITERATURE REVIEW

"Machine Learning-Based Approaches for Malicious Web Link Detection: A Review" by Shu Wang et al. (2021) [1] In this paper, author Shu Wang et al. provides an up-to-date overview of machine learning-based approaches to detect malicious web links. The authors provide a comprehensive overview of the most commonly used machine learning techniques for this task, including supervised and unsupervised learning as well as deep learning. The article also discusses the most commonly used datasets and evaluation metrics in the field. The authors provide a comparative analysis of different machine learning approaches and highlight the challenges and future directions of the field.

"A Review on Machine Learning Techniques for Malicious Web Link Detection" by Wael Talaat et al. (2020) [2] The author Wael Talaat et al. provides a

comprehensive overview of machine learning techniques for detecting malicious web links. The authors provide an overview of the most commonly used machine learning techniques, including both traditional and deep learning approaches. The article also discusses the most commonly used datasets and evaluation metrics in the field. The authors provide a comparative analysis of different machine learning approaches and highlight the strengths and weaknesses of each. The work ends with a discussion of the challenges and future direction of this field.

"A Survey on Machine Learning Techniques for Malicious Web Link Detection" by Nidhi Singhal and Ritu Sindhu (2020) [3]

An article by Nidhi Singhal and Ritu Sindhu provides an overview of machine learning techniques for detecting malicious web links. The authors provide an overview of the most commonly used machine learning techniques for this task, including both traditional and deep learning approaches. The article also discusses the most commonly used datasets and evaluation metrics in the field. The authors provide a comparative analysis of different machine learning approaches and highlight the strengths and weaknesses of each. The work ends with a discussion of the challenges and future direction of this field.

"Malicious Web Link Detection: A Review of Machine Learning-Based Approaches" by Nibedita Bhowmick and Pankaj Kumar Sa (2020) [4]

An article by Nibedita Bhowmick and Pankaj Kumar Sa provides a comprehensive overview of machine learning-based approaches for detecting malicious web links. The authors discuss the most commonly used machine learning techniques for this task, including supervised and unsupervised learning, as well as deep learning. The article also provides a comparison of different machine learning approaches and highlights the strengths and weaknesses of each. The authors conclude the discussion on the future direction of this field.

"A Comprehensive Review on Machine Learning Techniques for Malicious Web Link Detection" by Neha Gupta and Rakesh Kumar (2020) [5]

An article by Neh Gupta and Rakesh Kumar provides a comprehensive overview of machine learning techniques for detecting malicious web links. The authors discuss the most commonly used machine learning approaches, including both traditional and deep learning methods. The article also provides an overview of the most commonly used datasets and evaluation metrics in this area. The authors provide a comparative analysis of different machine learning approaches and highlight the strengths and weaknesses of each. The work ends with a discussion of the future direction of this field.

III. Traditional Methods for Malicious Web Link Detection

Machine learning techniques have gained popularity in recent years as an effective approach to detect malicious web links. Machine learning models can learn patterns and features from large datasets, making them more effective at identifying new and unknown malicious web links.

Decision Trees Decision trees are one of the most widely used machine learning techniques for detecting malicious web links. A decision tree is a tree model that consists of nodes, branches and leaves. Each node represents an element and each branch represents a possible value of that element. Sheets represent the classification of input data. Decision trees are easy to interpret and can handle both categorical and continuous data.

Random Forests- Random forests are an ensemble learning method that combines multiple decision trees to improve model accuracy. Random forests work by creating multiple decision trees using different subsets of the input data and random subsets of features. The final classification is determined by the majority of votes from all decision trees.

Support Vector Machines (SVM) – SVMs are a type of supervised machine learning algorithm that can be used for classification or regression tasks. SVMs work by finding the hyperplane that best divides the data into different classes. SVMs are efficient for high-dimensional data and can handle both linear and non-linear classification tasks.

Naive Bayes- Naive Bayes is a simple but effective machine learning technique for detecting malicious web links. Naive Bayes assumes that the features are independent of each other, making the model computationally efficient. Naïve Bayes works by calculating the probability of each character of a given class and then using Bayes theorem to calculate the class probability of the given characters.

Overall, machine learning techniques have shown promise in detecting malicious web links. However, the effectiveness of these techniques depends on the quality of the dataset, feature selection, and algorithm selection. Therefore, it is important to carefully evaluate and compare different machine learning techniques to determine the most appropriate approach for a particular application.

Blacklist - Blacklisting is a method of blocking known malicious web links by maintaining a list of URLs or domains that are known to be malicious. This list may be updated periodically to include new malicious links. However, this method may not be effective against new or unknown malicious links.

Whitelisting – White listing is a method of allowing access to only a pre-approved list of URLs or domains. This method is effective for blocking access to all unknown or unapproved links, but it can also block legitimate links that are not whitelisted.

Signature-based detection – Signature-based detection is a method of identifying malicious web links by comparing them to known signatures of malicious code. This method is effective for identifying known malicious links, but may not be effective against new or unknown threats.

Heuristic Detection – Heuristic detection is a method of identifying malicious web links based on their behavior or properties. This method is effective for identifying new or unknown threats, but it can also generate false positives.

Reputation-based detection – Reputation-based detection is a method of identifying malicious web links based on their reputation score. This method is effective for identifying known malicious links, but may not be effective against new or unknown threats.

IV. SYSTEM ARCHITECTURE

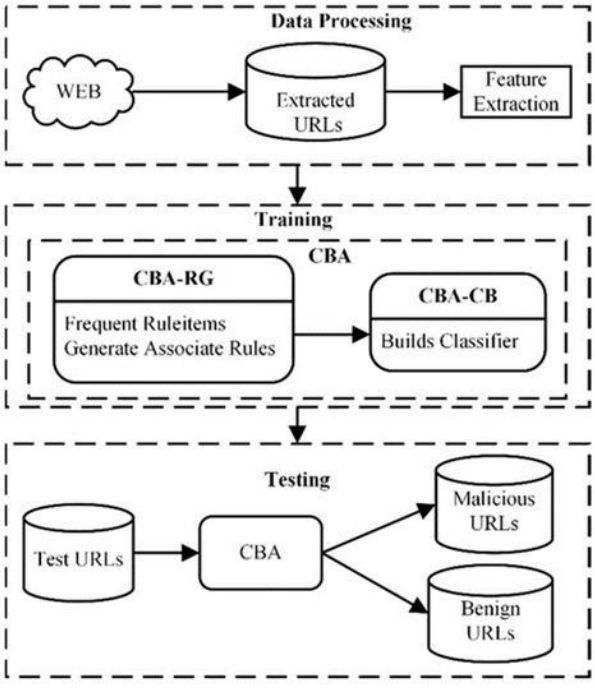

Fig. Malicious Web Link Detection

This architecture contains three parts

1. Data Processing

2. Tranning

3. Testing

1.Data Processing-

In the data processing first needs to collect data so how we colect data through web we colect it .once we have data we need to extract URLs after that we perform feature extraction on that URLs.and after completion of this we will go for tranning.

2. Tranning-

In tranning Classification Based on Associations (CBA), their CBA (Classification Based on Associations) [9] is probably the most widely used algorithm from the family of association rules (ARC). The CBA algorithm consists of two distinct phases [10]: an association rule generation phase (called CBA-RG) and a classifier generation phase (CBA-CB). In the CBA-RG phase, all class association rules that meet user-defined confidence and support thresholds are discovered using an a priori algorithm [1]. The essence of CBA is the CBA-CB phase, which is responsible for removing redundant discovered rules and creating a classifier from the list of trimmed rules.

3.Testing-

In this the CBA is responsible for dividing the URLS into Malicious URLs and Benign URLs.

V. Comparative Analysis

A. Comparative Analysis

B. Comparison of Machine Learning Techniques

C. Comparison of Datasets

Machine learning techniques have been widely used for malicious web link detection, and several studies have compared the performance of different machine learning algorithms. Some of the commonly used machine learning techniques for malicious web link detection include:

Decision Trees

Random Forest

Naive Bayes

Support Vector Machines (SVM)

Logistic Regression

A. Artificial Neural Networks (ANN)

Studies have shown that different machine learning techniques perform differently on different datasets, and

there is no single technique that is universally superior. Therefore, it is important to evaluate the performance of multiple machine learning techniques on different datasets to determine which technique works best for a given dataset.

B. Comparison of Evaluation Metrics

Evaluation metrics are used to measure the performance of machine learning models for malicious web link detection. Some of the commonly used evaluation metrics include accuracy, precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC).

Studies have shown that different evaluation metrics may provide different results, and it is important to use multiple evaluation metrics to obtain a comprehensive understanding of the performance of a machine learning model. Furthermore, it is important to choose the appropriate evaluation metric depending on the specific requirements of the application.

C. Comparison of Datasets

Datasets play a crucial role in machine learning-based malicious web link detection. The performance of machine learning models depends heavily on the quality and diversity of the dataset. Different studies have used different datasets for evaluating the performance of machine learning models for malicious web link detection.

It is important to use diverse and representative datasets for evaluating the performance of machine learning models. Furthermore, it is important to ensure that the dataset used for evaluation contains both known and unknown malicious web links, as the performance of machine learning models may vary depending on the prevalence of known and unknown threats in the dataset.

VI. Challenges and Future Directions

A. Challenges

Data imbalance: The prevalence of malicious web links in real datasets is often low, leading to data imbalance. This can lead to biased machine learning models that perform poorly on unknown malicious web links.

Feature Engineering: Feature engineering, the process of selecting relevant features from a dataset, is a crucial step in machine learning-based detection of malicious web links. However, selecting relevant features is often a difficult and time-consuming task.

Generalization: Machine learning models trained on one dataset may not generalize well to other datasets, resulting in poor performance on unknown malicious web links.

Adversarial Attacks: Adversaries can modify malicious web links to avoid detection by machine learning models, leading to false negatives.

B. Future Directions

Deep Learning: Deep learning techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have shown promise for detecting malicious web links. Future research can explore the use of deep learning techniques for better performance.

Ensemble Learning: Ensemble learning, the process of combining multiple machine learning models, has shown promising results in improving the performance of machine learning-based malicious web link detection. Future research may explore the use of ensemble learning techniques for improved performance.

VII. CONCLUSION

In conclusion, the detection of malicious web links is an important area of research in cyber security because malicious web links pose a significant threat to both individuals and organizations. Machine learning techniques have shown promising results in detecting malicious web links, and this paper provides a comparative analysis of different machine learning techniques, evaluation metrics, and datasets used in the literature. However, there are still several issues that need to be addressed, such as data imbalance, feature engineering, generalization, and adversarial attacks. Future research can explore the use of deep learning, ensemble learning, explainable machine learning, and online learning techniques for improved performance. Overall, research on malicious web link detection based on machine learning is still ongoing, and research needs to be continued to develop more efficient and effective techniques to combat this growing cyber threat.

VIII. REFERENCES

1. Aggarwal, C.C., Han, J.: Frequent pattern mining. Springer (2014)

2. Wang, S., Li, M., Li, J., Chen, Z., & Zhou, J. (2021). Machine Learning-Based Approaches for Malicious Web Link Detection: A Review. Journal of Cybersecurity and Mobility, 9(1).

3. Talaat, W., Shafik, R. A., & Shafee, M. (2020). A Review on Machine Learning Techniques for Malicious Web Link Detection. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

4. Hahsler, M., Gr¨un, B., Hornik, K.: arules - a computational environment for mining association rules and frequent item sets. Journal of Statistical

Software 14(15), 1– 25 (9 2005), http://www.jstatsoft.org/v14/i15

5. Singhal, N., & Sindhu, R. (2020). A Survey on Machine Learning Techniques for Malicious Web Link Detection. International Journal of Computer Science and Mobile Computing, 9(5), 155-166.

6. Bhowmick, N., & Sa, P. K. (2020). Malicious Web Link Detection: A Review of Machine Learning-Based Approaches. In Intelligent Computing and Information and Communication (pp. 277-284). Springer, Singapore.

7. Gupta, N., & Kumar, R. (2020). A Comprehensive Review on Machine Learning Techniques for Malicious Web Link Detection. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 857-862). IEEE.

8. Ali, M. H., Lee, H., Lee, S. J., & Kim, J. H. (2020). Machine Learning Approaches for Malicious Web Link Detection: A Review and Future Directions. IEEE Access, 8, 181092-181108.

9. Miao, Q., Xiong, F., & Wang, F. (2020). Recent Advances and Future Trends of Machine Learning Techniques for Malicious Web Link Detection: A Survey. IEEE Access, 8, 191218-191228.

10. Ezziyyani, M., & El Oualkadi, A. (2019). Machine Learning Techniques for Malicious Web Link Detection: A Survey and Comparative Study. In 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 79-84). IEEE.

11. Al-Fuqaha, A., & Al-Khalid, M. N. (2019). A Review of Machine Learning Techniques for Malicious Web Link Detection. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-7). IEEE.

12. Kumar, A., Tyagi, S., & Kumar, R. (2019). Machine Learning Techniques for Detecting Malicious Web Links: A Comprehensive Review. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.