Paper Title:
Malicious Domain Detection using NLP Methods

Paper Link:
https://ieeexplore.ieee.org/document/10046882

1 Summary

1.1 Motivation

The motivation of this paper is to address the prevalent problem of cyber attacks and the need to identify and block malicious URLs. The paper highlights the challenges of identifying malicious URLs and discusses the use of natural language processing (NLP) and machine learning (ML) techniques to detect these URLs. The goal is to provide an overview of NLP techniques for text processing and explore recent domain-related research in order to aid future research in identifying and blocking harmful web pages or links.

1.2 Contribution

The contribution of this paper is to provide an overview of various natural language processing (NLP) techniques for text processing in order to identify malicious URLs. The paper explores recent domain-related research and discusses the use of machine learning algorithms, such as SVM and Random Forest, along with NLP techniques like N-gram, vectorization techniques such as the Bag of Words model (BoW), and Term Frequency-Inverse Document Frequency (TF-IDF) for detecting malicious URLs. The authors also review related work from other researchers who have used different datasets and NLP methods, such as the N-gram technique, count vectorizer, hash vectorizer, TF-IDF vectorizer, and word decomposer, among others.

1.3 Methodology

The methodology discussed in the Malicious Domain Detection using NLP Methods Proceedings involves the use of natural language processing (NLP) and machine learning (ML) techniques to identify malicious URLs. Researchers utilize various NLP techniques for text processing and employ machine learning algorithms such as Support Vector Machines (SVM) and Random Forest, along with vectorization techniques like Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF), to detect malicious URLs. The paper also mentions the use of blacklists and deep learning techniques in the detection process. Several studies and models are mentioned in the literature review section that propose different approaches and algorithms for identifying malicious URLs.

1.4 Conclusion

In conclusion, the Malicious Domain Detection using NLP Methods highlight the escalating problem of cyber attacks, particularly through the use of malicious URLs. These attacks lead to various malicious acts, such as credential theft and the compromise of sensitive information. Researchers have increasingly turned to Natural Language Processing (NLP) and machine learning (ML) techniques to tackle this issue. The research in this area emphasizes the use of machine learning algorithms, such as SVM and Random Forest, and NLP techniques like N-gram, alongside vectorization techniques such as Bag of Words (BoW) and TF-IDF, to effectively detect malicious URLs.

2 Limitations

2.1 First Limitation

The first limitation is that the vector length will increase if new sentences contain new words. This means that as new words are introduced, the size of the vectors used in the analysis will grow, potentially causing computational challenges.

2.2 Second Limitation

Another limitation is that the N-gram models used in natural language processing (NLP) techniques for text processing do not capture long-distance context well. This means that the models struggle to understand the meaning and context of words based on their surrounding text, which can impact their ability to accurately identify malicious URLs. Additionally, N-gram models may result in sparse matrices with numerous zeros, which can further affect the effectiveness of the models.

3 Synthesis

The paper discusses the increasing problem of cyber attacks and the use of malicious URLs by cybercriminals to deceive internet users and carry out malicious acts. The paper provides an overview of various NLP techniques for text processing and reviews recent research in this domain. The literature review reveals that machine learning algorithms, such as SVM and Random Forest, along with NLP techniques like N-gram and vectorization methods like Bag of Words and TF-IDF, are effective in detecting malicious URLs. The paper also discusses the CTI-MURLD model proposed which uses RF algorithm and ensemble learning for predicting malicious URLs. Additionally, This paper proposes a phishing detection system that combines machine learning algorithms and NLP techniques to identify phishing attacks. Another approach discussed is the use of word vector representation and n-gram models for classifying URLs, which has shown promising results with high accuracy using SVM.