WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Social Engineering Attacks on Email Conversations

Mr. K. Mohana Krishna

3rd Year B.Sc.Computer Technology, Department of Computer Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamilnadu

mkrishhh11@gmail.com

ABSTRACT

This study investigates the detection of social engineering attacks in email communications by leveraging machine learning techniques, specifically Random Forest classifiers and Word2Vec embeddings. A prototype system was developed to classify emails as either phishing or legitimate. The system was trained on a dataset of email contents, transformed into numerical vectors using Word2Vec, and subsequently classified using a Random Forest algorithm. The model demonstrated promising accuracy in distinguishing phishing emails from legitimate ones, underscoring the potential of combining natural language processing with machine learning for cybersecurity applications.

Keywords*: Selective ticket cancellation, Online booking systems, User-controlled cancellations, Partial booking cancellations, Ticket management flexibility*

INTRODUCTION

Social engineering attacks, particularly phishing emails, have become a prevalent threat in cybersecurity. These attacks manipulate individuals into divulging confidential information or performing actions compromising organizational security. Traditional detection methods, such as blacklists and rule-based systems, often fall short due to the evolving nature of phishing tactics. Consequently, there is a pressing need for adaptive and intelligent

detection mechanisms. Machine learning (ML) offers dynamic solutions capable of learning from data and identifying patterns indicative of phishing attempts. This study explores the efficacy of integrating Word2Vec embeddings with a Random Forest classifier to detect phishing emails, aiming to enhance the robustness and accuracy of email security systems.

LITERATURE REVIEW

Numerous studies have applied ML techniques to phishing detection. Akinyelu et al. (2014) utilized Random Forest models to analyze email branches, achieving a 99.7% accuracy rate in phishing detection [6]. Similarly, a study employing Support Vector Machine (SVM) and Random Forest classifiers reported a maximum accuracy of 99.87% in classifying emails as phishing or legitimate [7]

Deep learning approaches, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have also been explored for phishing detection, with CNNs being effective for image-based phishing identification and RNNs suitable for analyzing URL patterns and email messages [8]. However, these methods often require extensive computational resources and large datasets. The integration of Word2Vec embeddings with traditional ML algorithms, like Random Forests, offers a balance between performance and computational efficiency, making it a viable approach for phishing email detection.

METHODOLOGY

Data Collection and Preprocessing: A sample dataset was curated, comprising email contents labeled as phishing or legitimate. Each email was tokenized into words to prepare for embedding.

Word2Vec Embedding: The Word2Vec model was trained on the tokenized email dataset to capture semantic relationships between words. Each email was then represented as an average of its constituent word vectors, producing fixed-length numerical representations suitable for classification.

Feature Scaling: To ensure uniformity in the feature set, the numerical representations were standardized using a StandardScaler, normalizing the data to have zero mean and unit variance.

Model Training: A Random Forest classifier was trained on the standardized embeddings to classify emails as phishing or legitimate. The model's performance was evaluated using metrics such as accuracy, precision, recall, and the area under the receiver operating characteristic curve (AUC-ROC).

RESULTS

The Random Forest classifier, combined with Word2Vec embeddings, achieved high accuracy in distinguishing phishing emails from legitimate ones. The model's performance metrics indicate its effectiveness in identifying phishing attempts, with precision and recall rates reflecting a low incidence of false positives and false negatives, respectively. These results align with findings from previous studies that reported high accuracy rates using Random Forest classifiers for phishing detection [9]

CONCLUSION

This study demonstrates that integrating Word2Vec embeddings with Random Forest classifiers is an effective approach for detecting social engineering attacks in emails. The methodology leverages the semantic understanding of email content through word embeddings and the robust classification capabilities of Random Forests. Future work could involve expanding the dataset to include more diverse email samples and exploring the integration of this model into real-time email filtering systems to enhance cybersecurity measures.

BIBLIOGRAPHY

1. **Akinyelu, A. A., & Adewumi, A. O.(2014).** https://scholar.smu.edu/cgi/viewcontent.cgi?article=1215&context=datasciencereview
2. **Chataut, R., & Venkatesan, R. (2024).** https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai. 2024.1414122/full
3. **Adebowale, M. A., Lwin, K. T., & Sanchez, A. (2023).** https://pmc.ncbi.nlm.nih.gov/articles/PMC11013960/
4. **Al-Subaiey, A., Al-Thani, M., Alam, N. A., Antora, K. F., A. (2024).** https://arxiv.org/abs/2405.11619
5. **Shmalko, M., Abuadbba, A., Gaire, R., Wu, T., Paik, H.-Y., & Nepal, S. (2022).** https://arxiv.org/abs/2208.08745
6. scholar.smu.edu
7. researchgate.net
8. ijcse.com
9. rontiersin.org
10. **Social Engineering Attacks Detection Approach,(2023),** https://ieeexplore.ieee.org/document/10416499