Marathwada Mitra Mandal's College of Engineering, Pune Department of computer Of Computer Engineering

Presentation   
On

Phishing Classifier   
By

TC133 Ganesh Gajanan Kanade

Guided by   
Dr.S.N.Shekapure

Phishing Classifier by Machine Learning   
Welcome to this presentation on building a Phishing Classifier using Machine Learning. We will explore the different components of the

system and discuss its applications and future prospects.

Introduction   
Understanding the growing threat of phishing attacks and their impact on individuals and organizations.

1   
The Need for Phishing Detection   
Exploring the reasons why there is a significant demand for effective phishing detection mechanisms.

2   
Scope of the Project   
Defining the scope of the project and its objectives in developing a robust phishing classifier.

3   
Significance of Machine Learning   
Highlighting the role of machine learning in effectively identifying and preventing phishing attacks.

System Architecture   
An overview of the architecture and components involved in building the phishing classifier system.

Neural Network   
Illustrating the use of neural networks for training and classifying phishing emails.

Feature Extraction   
Explaining the process of extracting relevant features from emails for effective classification.

Training Data   
Describing the importance of high-quality training data to improve the accuracy of the classifier.

Proposed System (Algorithm)   
Detailing the algorithmic approach for training and classifying phishing emails using machine learning techniques.

Data Preprocessing   
Discussing the steps involved in cleaning and preparing the training data for the classifier.

Feature Selection   
Explaining the process of selecting the most relevant features for accurate classification.

Algorithm Training   
Highlighting the training process of the classifier using labeled phishing and non-phishing emails.

Classification and Evaluation   
Examining the classification process and evaluating the performance of the phishing classifier.

Results

Presenting the evaluation results and performance metrics of the developed phishing classifier system.

1   
Accuracy Measures   
Analyzing accuracy, precision, recall, and other metrics to measure the effectiveness of the classifier.

2   
Comparison with Existing Techniques   
Comparing the performance of the proposed system with other state-of-the-art phishing detection techniques.

3   
Robustness Testing   
Testing the classifier with different types of phishing attacks to assess its robustness.

Application   
Highlighting the potential applications and real-world scenarios where the phishing classifier can be deployed.

1   
Protecting Individuals   
Exploring how the classifier can be used to protect individuals from

falling victim to phishing attacks.

2   
Securing Organizations   
Discussing the role of the classifier in safeguarding organizations from phishing-related security breaches.

3   
Integration with Email Clients   
Illustrating the integration of the classifier into popular email clients for real-time protection.

Literature Survey   
An overview of existing research and studies related to phishing detection and machine learning techniques.

Traditional Methods   
Examining the traditional approaches used for phishing detection and their limitations.

Machine Learning Techniques   
Reviewing various machine learning algorithms and their effectiveness in classifying phishing emails.

Feature Extraction   
Discussing the importance of feature extraction in identifying key indicators of phishing attacks.

Future Work

Identifying potential future work and areas for further research and development in the field of phishing classification.

1   
Enhanced Feature Extraction   
Exploring advanced feature extraction techniques to improve the classifier's accuracy.

2   
Real-Time Analysis   
Investigating real-time analysis and detection of evolving phishing attacks to enhance security measures.

3   
Behavioral Analysis   
Considering the incorporation of behavioral analysis to identify phishing attempts with changing patterns.

Conclusion   
Summarizing the key findings and contributions of the phishing classifier project.

Achievements   
Highlighting the successful development of an accurate and efficient phishing detection system.

Future Enhancements   
Discussing potential areas for improvement and future research directions in phishing detection methods.

References

Adarsh Mandadi, Saikiran Boppana, Vishnu Ravella., "Phishing Website Detection Using MachineLearning,”2022 IEEE 7th International conference for Convergence in Technology (I2CT) | 978-1-6654-2168-3/22/$31.00 ©2022 IEEE, doi: : 10.1109/ I2CT54291.2022.9824801.

2. Yingying Xu1 ,Guangxuan Chen1 \*, Qiang Liu1, Wanpeng Xu2, "A Phishing Website Detection and

RecognitionMethod Based on Naive Bayes,” 2022 IEEE 6th Information Technology and

Mechatronics Engineering Conference (ITOEC) | 978-1-6654-3185-9/22/$31.00 ©2022 IEEE |, doi:

10.1109/ITOEC53115.2022.9734474.

3. Manimuthu Ayyannan, S. Gayathri Priya, V. Arun A. N.

Arularasan, M Jogendra Kumar, “HybridOptimization Algorithm to Mitigate Phishing URL Attacks In Smart Cities”, 2023 3rd   
InternationalConference on Innovative Practices in Technology and Management (ICIPTM) | 979-8-3503-3623-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIPTM57143.2023.10118171

4. Malak Aljabr, Dorieh M. Alomari, Menna Aboulnour, “Fake News Detection Using Machine Learning Models”, 2022 14th   
International Conference on Computational Intelligence and   
Communication Networks (CICN) | 978-1-6654-8771-9/22/$31.00

©2022 IEEE | DOI: 10.1109/CICN56167.2022.10008340

5. YAZAN AHMAD ALSARIERA 1 , VICTOR ELIJAH ADEYEMO 2 , ABDULLATEEF OLUWAGBEMIGA BALOGUN 3,4, (Member, IEEE), AND AMMAR KAREEM ALAZZAWI, “AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites”, Received July 19, 2020, accepted July 29, 2020, date of publication August 3, 2020, date of current version August 14, 2020

6. Manimuthu Ayyannan, S. Gayathri Priya, V. Arun A. N.

Arularasan, M Jogendra Kumar, “Hybrid Optimization Algorithm to Mitigate Phishing URL Attacks In Smart Cities”, 2023 3rd   
International Conference on Innovative Practices in Technology and Management (ICIPTM) | 979-8-3503-3623-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIPTM57143.2023.10118171

7. Adarsh Mandadi, Saikiran Boppana, Vishnu Ravella, ” Phishing Website Detection Using Machine Learning”, 2022 IEEE 7th International conference for Convergence in Technology (I2CT) | 978-1-6654-2168-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ I2CT54291.2022.9824801