Web Phishing Detection using hyper-tuned Convolution Neural Network model

Vansh Bansal

*Dept. of Artificial Intelligence Amity University*Noida, India vb.vansh04@gmail.com

**Problem Statement**

The increasing sophistication of phishing attacks poses a significant threat to individuals and organizations, as cybercriminals exploit the growing reliance on the internet for day-to-day activities. Despite advancements in cybersecurity measures, a study by Intel reveals that 97% of security experts struggle to distinguish phishing emails from genuine ones. This alarming statistic underscores the urgent need for improved detection methods, particularly in the context of web pages where phishing attacks are becoming more intricate and challenging to identify. Moreover, the escalating complexity of phishing attacks demands innovative solutions to stay ahead of cybercriminal tactics. This research seeks to address the pressing need for advanced and accurate phishing detection mechanisms, offering a proactive defense against evolving threats in the dynamic landscape of online security.

***Keywords: Phishing detection, Cybersecurity, Binary Classification, Deep Learning***

1. SIGNIFICANCE OF THE WORK
2. **Protecting Personal and Financial Information:** As phishing attacks remain a highly successful method for cybercriminals to defraud individuals, the development of effective detection techniques becomes crucial to safeguard personal and financial information. This work aims to mitigate the risk of identity theft and financial loss for individuals and businesses.
3. **Preserving Online Trust:** The prevalence of phishing erodes trust in online platforms and communication channels. By enhancing the ability to detect phishing attempts in web pages, this research contributes to maintaining the integrity of online interactions and fostering a secure digital environment.
4. **Cybersecurity Resilience**: As cyber threats evolve, it is imperative to strengthen cybersecurity resilience. Improved detection of phishing attacks on web pages not only protects individuals but also enhances the overall resilience of digital ecosystems, making it more difficult for cybercriminals to exploit vulnerabilities

In conclusion, the significance of this work lies in its potential to enhance the detection of phishing attacks in web pages, thereby fortifying online security, protecting personal and financial information, and contributing to the overall resilience of digital ecosystems in the face of increasingly sophisticated cyber threats.

1. DATASET USED

The dataset at hand comprises 11,430 URLs, serving as a comprehensive benchmark for the evaluation of deep learning-based phishing detection systems. This curated dataset assumes paramount significance in the realm of cybersecurity research, offering a diverse and extensive pool for assessing the efficacy of detection mechanisms. Comprising 87 meticulously extracted features, the dataset is structured to encapsulate the multifaceted nature of phishing attacks and legitimate URLs alike.

These features are meticulously categorized into three distinct classes, providing a nuanced perspective for analysis. The first class encompasses 56 features derived from the structural and syntactical attributes of URLs, enabling a granular examination of the inherent characteristics. The second class incorporates 24 features extracted from the content of corresponding web pages, delving into the intricacies of page-level attributes. Additionally, the third class involves 7 features extracted through queries to external services, broadening the scope of assessment beyond the confines of individual URLs.

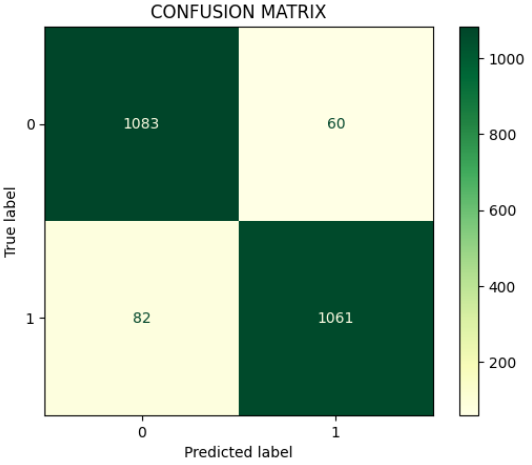
Notably, the dataset is meticulously balanced, maintaining a precise equilibrium with 50% phishing and 50% legitimate URLs. This equilibrium ensures a fair representation of both classes, fostering a robust foundation for the development and evaluation of machine learning models. As a result, this dataset emerges as a valuable resource in advancing the field of cybersecurity, empowering researchers, and practitioners to enhance the sophistication and accuracy of phishing detection systems in the ever-evolving landscape of cyber threats.

1. METHODLOGY

The proposed methodology utilizes a Convolutional Neural Network (CNN) architecture for automated detection of phishing URLs. The CNN model comprises several layers including convolutional, pooling, batch normalization, and dense layers. Each convolutional layer is followed by dropout regularization to prevent overfitting, while batch normalization aids in stabilizing and accelerating the training process. The model is trained using the Adam optimizer with binary cross-entropy loss function to optimize classification performance. To prevent overfitting and ensure generalization, early stopping and model checkpoint callbacks are employed during training. Training is conducted on a dataset split into training and validation sets, with performance monitored using accuracy metrics.

1. RESULTS

The proposed methodology achieved a classification accuracy of 94% on the test set, outperforming traditional manual methods. This demonstrates the effectiveness of the deep learning approach in web phishing detection.



Confusion matrix explains a good ratio of true positives and true negatives explaining the model’s exceptional performance to differentiate between different classes.

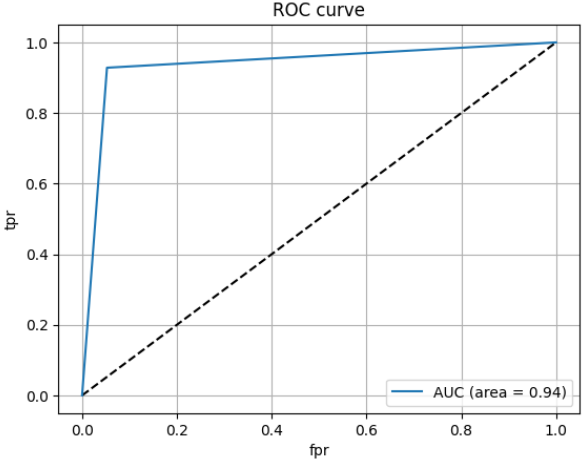


Fig. 1

Fig 1 explains the ROC curve and AUC of the model.

ROC (Receiver Operating Characteristic) curve visually represents the trade-off between true positive rate and false positive rate for a binary classification model.

AUC (Area Under the Curve) quantifies the overall performance of a binary classification model based on the ROC curve.

|  |  |  |
| --- | --- | --- |
|  | Legitimate | Phishing |
| Precision | 0.93 | 0.95 |
| Recall | 0.95 | 0.93 |
| F1 Score | 0.94 | 0.94 |
| Support | 1143 | 1143 |

Table 1

Table 1 shows the Classification Report of the model.

1. CONCLUSION

In summary, the suggested approach presents a hopeful automated method for identifying phishing URLs. Through the utilization of deep learning methods, this technique enhances both the effectiveness and precision of the process, thereby offering advantages to cybersecurity professionals and online users. Future investigations might delve into implementing this approach in web services to assess its practical value in real-life situations.