**Critical Analysis Report**

The analysis focuses on detecting malicious URLs using various machine learning and deep learning models. The study involves extensive exploratory data analysis, feature extraction, model training, and performance evaluation. This report presents key findings, model comparisons, and challenges encountered during the process.

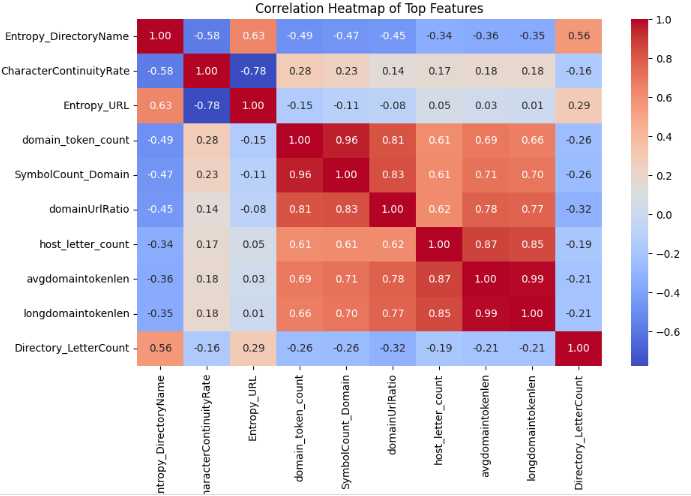
**Exploratory Data Analysis (EDA)**

Descriptive statistics were generated, revealing variations in URL structures. Malicious URLs exhibited distinct characteristics, such as excessive use of special characters, longer lengths, and multiple subdomains. Visualizations, such as histograms and box plots, highlighted the distribution of these attributes.

**Graphs and Plots**

Multiple visualizations were created to better understand the dataset and its patterns. The following were the most significant:

* **URL Length Distribution**, **Frequency of Special Characters**, **Word Cloud of Domain Name, Class Distribution Bar Chart**, **Feature Importance Plot**



**Feature Extraction**

Feature engineering played a crucial role in enhancing model performance. Structural features such as URL length, number of subdomains, and presence of suspicious characters were extracted. Additionally, NLP-based embeddings were applied using:

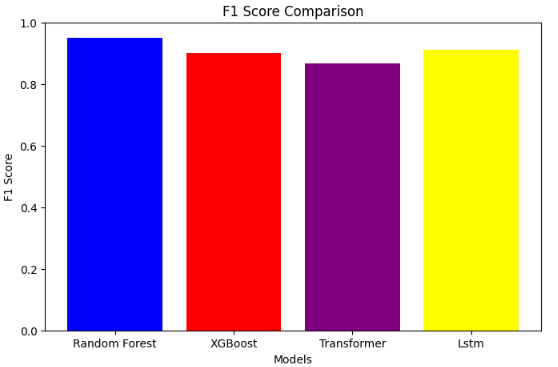
* **TF-IDF**: Captured word relevance within URLs.

Sequence-based feature extraction was also explored using character-level tokenization, aiding models in identifying deceptive URL structures.

**Machine Learning & LLM-Based Models**

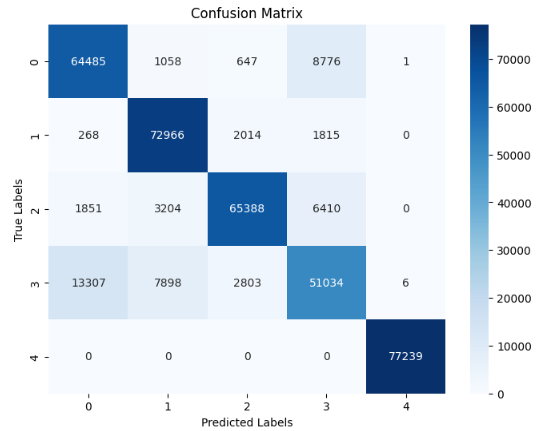
Three categories of models were employed for malicious URL detection:

* **Traditional ML Models**: Random Forest, XGBoost, and SVM were trained on extracted features. Random Forest achieved the highest performance with an F1 score of **0.95**.
* **Deep Learning Models**
* **LLM-Based Models**



**Results Visualization**

To compare model effectiveness, confusion matrices and ROC curves were generated. Traditional ML models, particularly Random Forest and XGBoost, demonstrated superior accuracy and interpretability. The deep learning models performed well but required more data preprocessing. LLM-based approaches provided promising results but were computationally expensive.



Most useful features highlighted were:

For now, these were the most useful features for predicting labels:

****

**Summary:**

* Traditional ML models have provided better results.
* While LLM-based requires computational resources but Improvements may include hybrid models that integrate handcrafted features with transformer-based embeddings to enhance detection capabilities.