पोखरा विश्वविद्यालय
POKHARA UNIVERSITY

Phishing Detection In Emails Using Lightweight Machine Learning Models For Edge Devices.

Presented by:

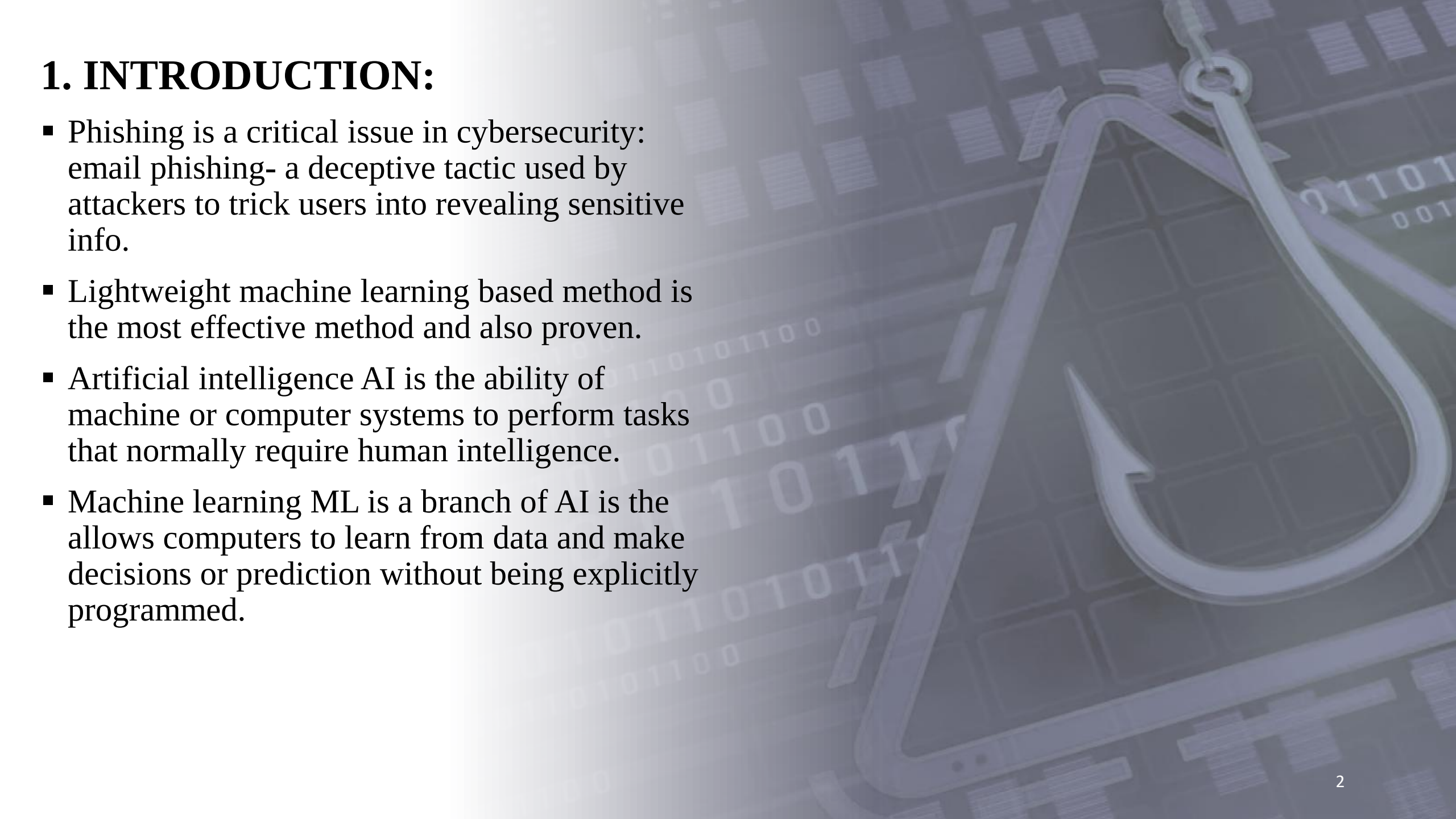
Prabhat Amgain

Puskar Shrestha

Sushovan Bikram Shahi

1. INTRODUCTION:

- Phishing is a critical issue in cybersecurity: email phishing- a deceptive tactic used by attackers to trick users into revealing sensitive info.
- Lightweight machine learning based method is the most effective method and also proven.
- Artificial intelligence AI is the ability of machine or computer systems to perform tasks that normally require human intelligence.
- Machine learning ML is a branch of AI is the allows computers to learn from data and make decisions or prediction without being explicitly programmed.



2. OBJECTIVES:

- A phishing email is a fraudulent message sent by cybercriminal designed to trick us into revealing sensitive information.
- This project is to develop lightweight machine learning models for effective phishing detection, specifically designed to run on edge devices such as smartphones, tablets and IOT systems.
- The main goal is to provide high accuracy with low false positives while enabling fast, scalable and secure integration into email platforms and mobile applications.

3. APPROACH:

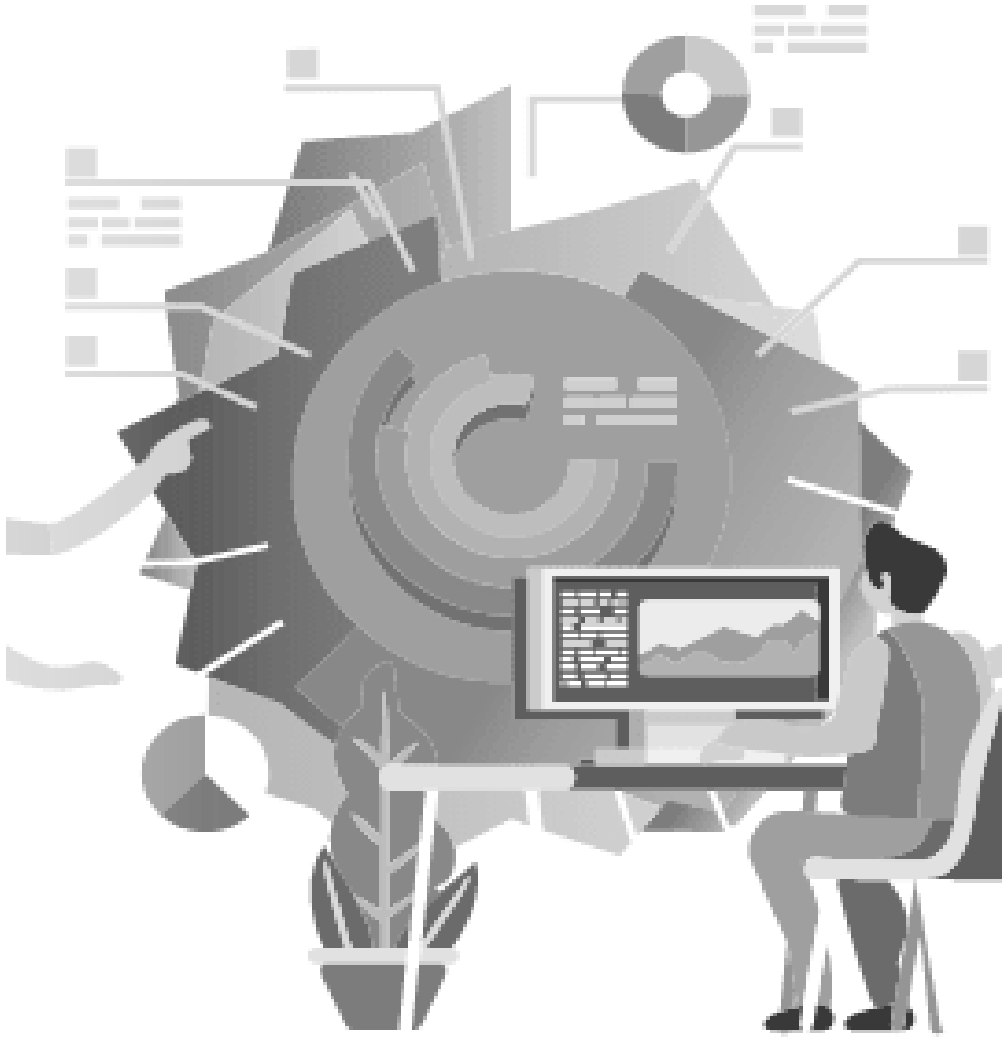
- Collect dataset containing phishing and legitimate emails from the open source platforms.
- Analyze and preprocess the dataset by EDA techniques.
- Run selected machine learning and deep neutral network algorithms like SVM, Random forest, Autoencoder on the dataset.
- Divide the dataset into training and testing sets.

4. DATA COLLECTION:

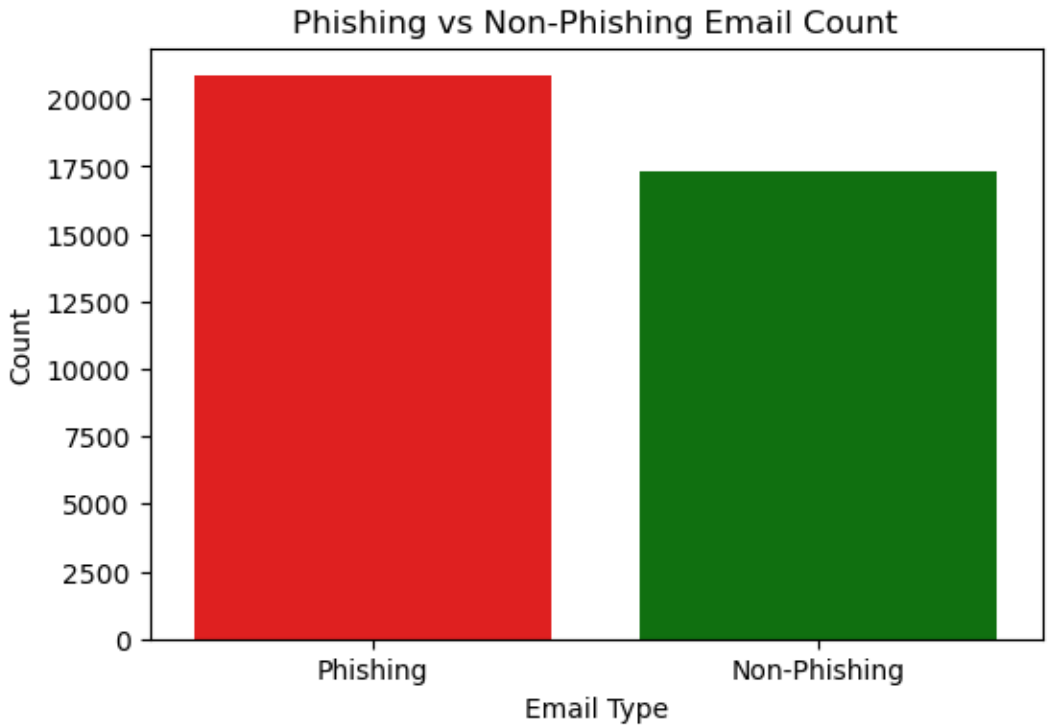
- Legitimate and phishing emails are collected from the website https://www.kaggle.com/datasets/naserabdullahalam/phishing-email-dataset.
- Phishing emails are collected from opensource service called Kaggle. This service provides a set of phishing emails in multiple formats like csv, json etc. that gets updated hourly.

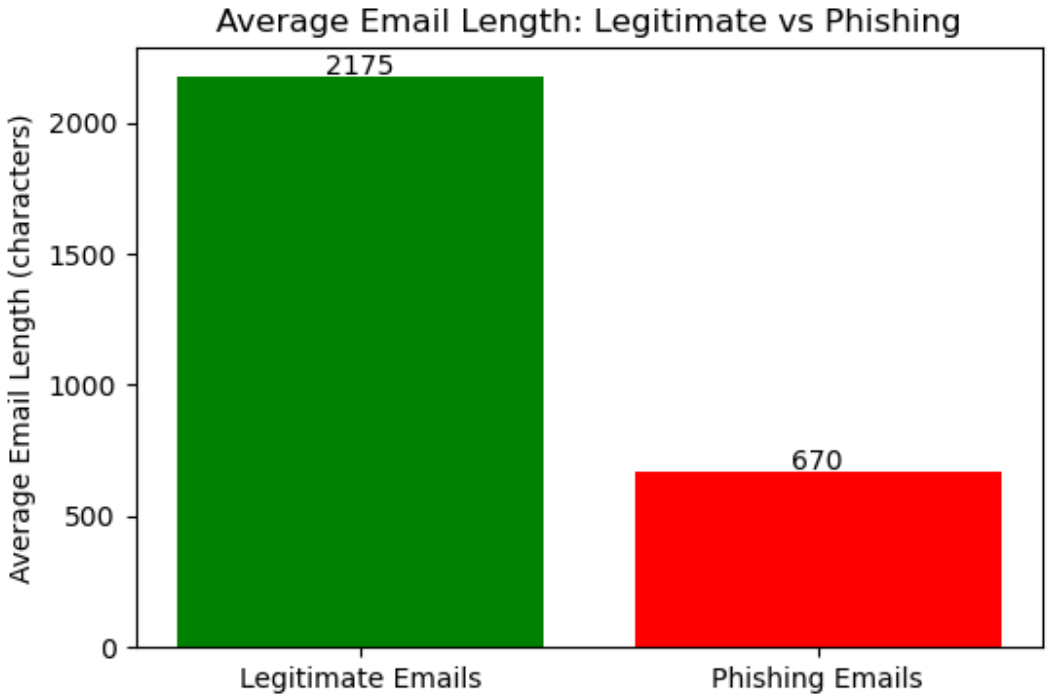
5. FEATURE SELECTION:

- The following features are selected:
  1. URL (1 / 0)
  2. Sender Name
  3. Sender Domain
  4. Text (Subject + Body)
  5. Label (Phishing = 1, Legit =0)
  6. Hours
  7. Day of Weeks

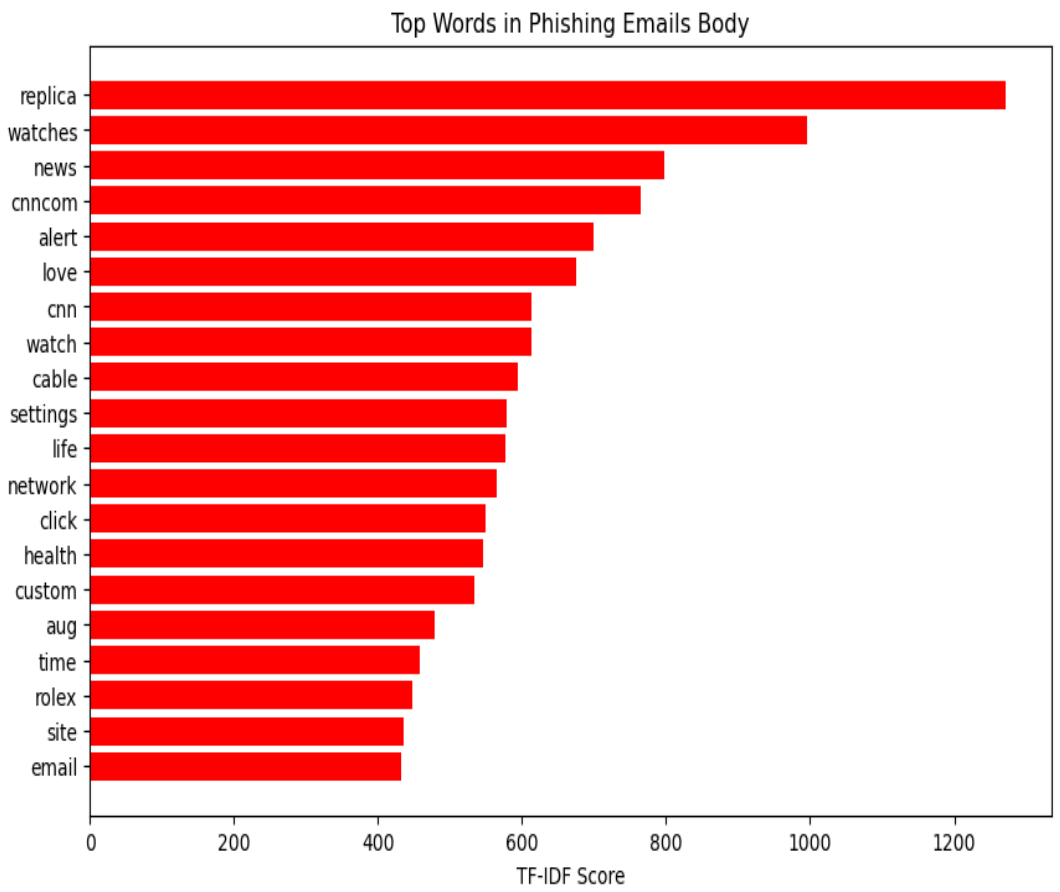


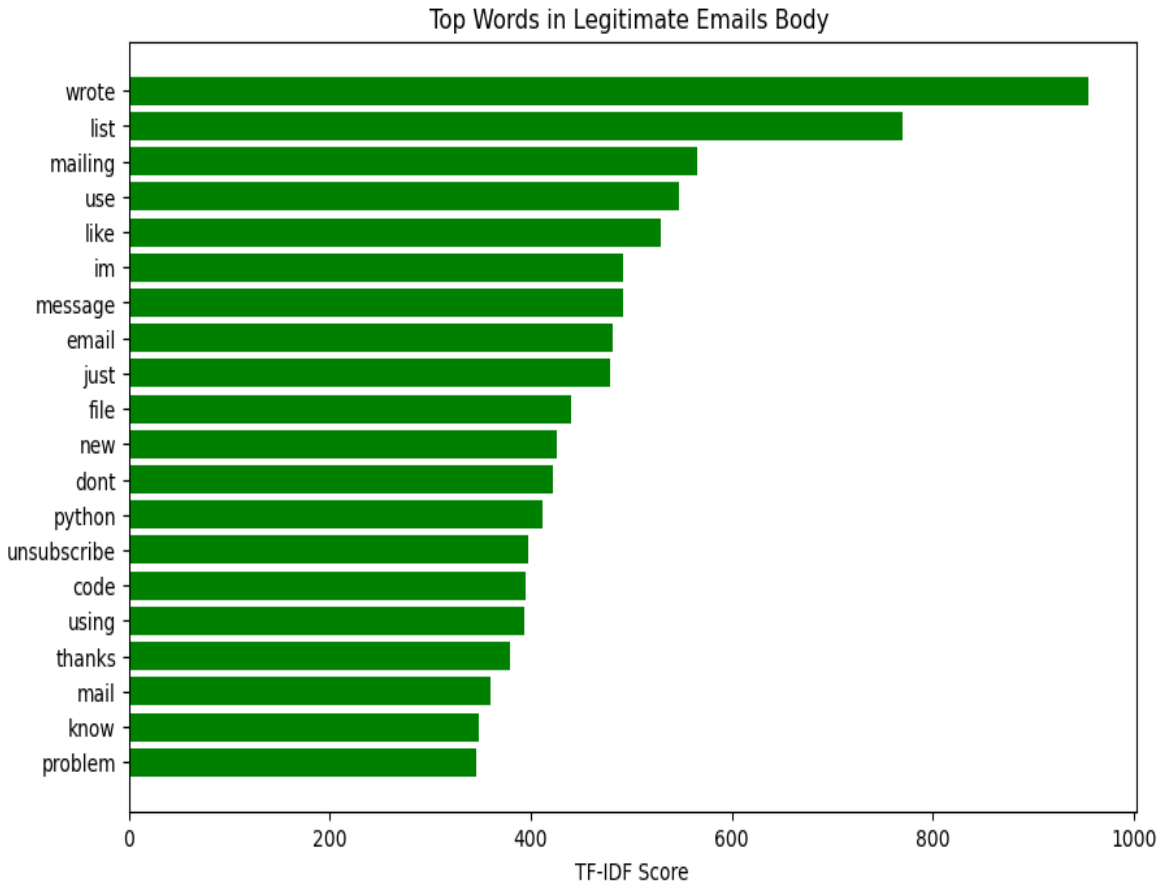
6. FEATURE ANALYSIS:



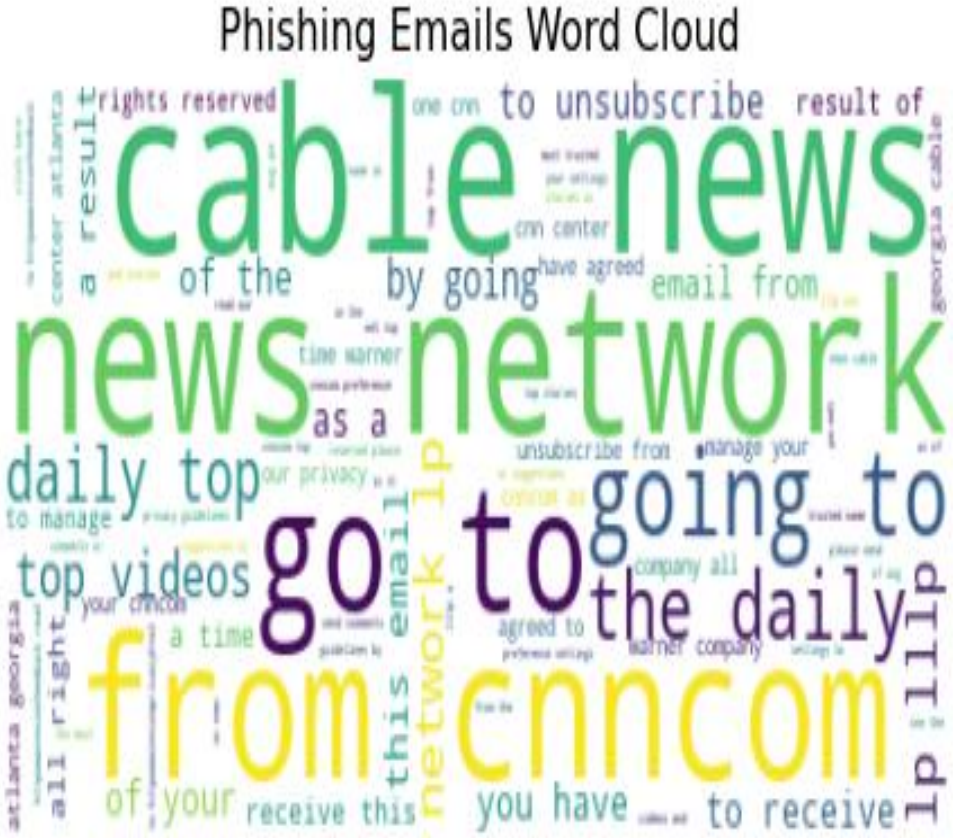


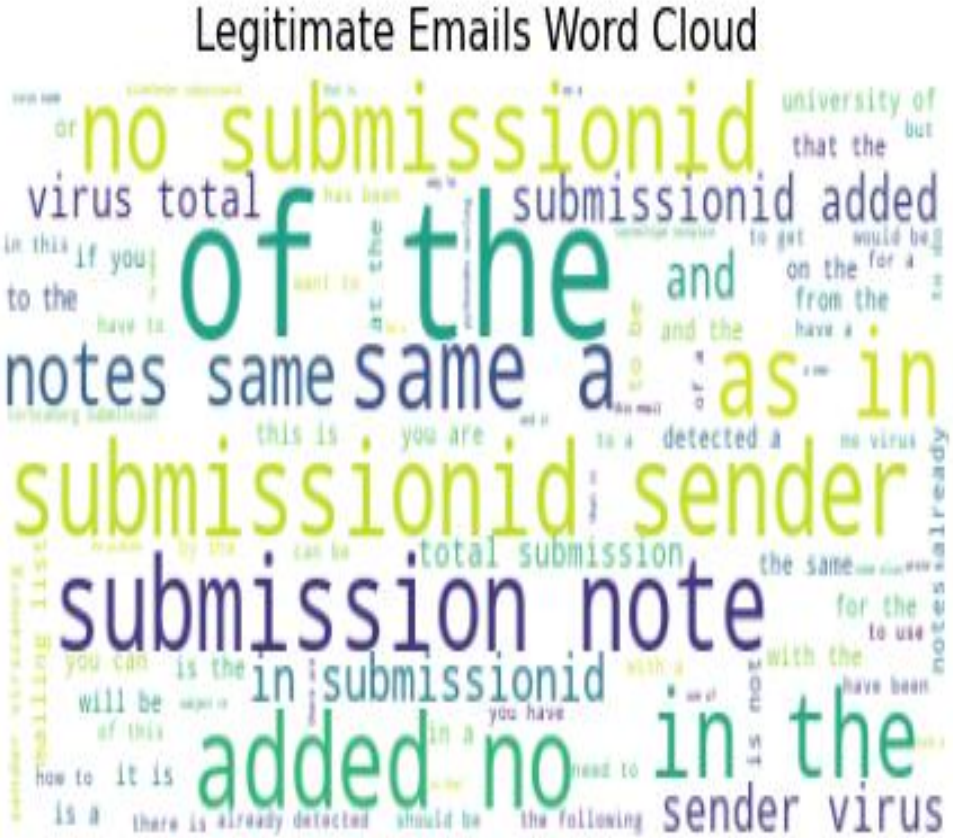
6. FEATURE ANALYSIS:



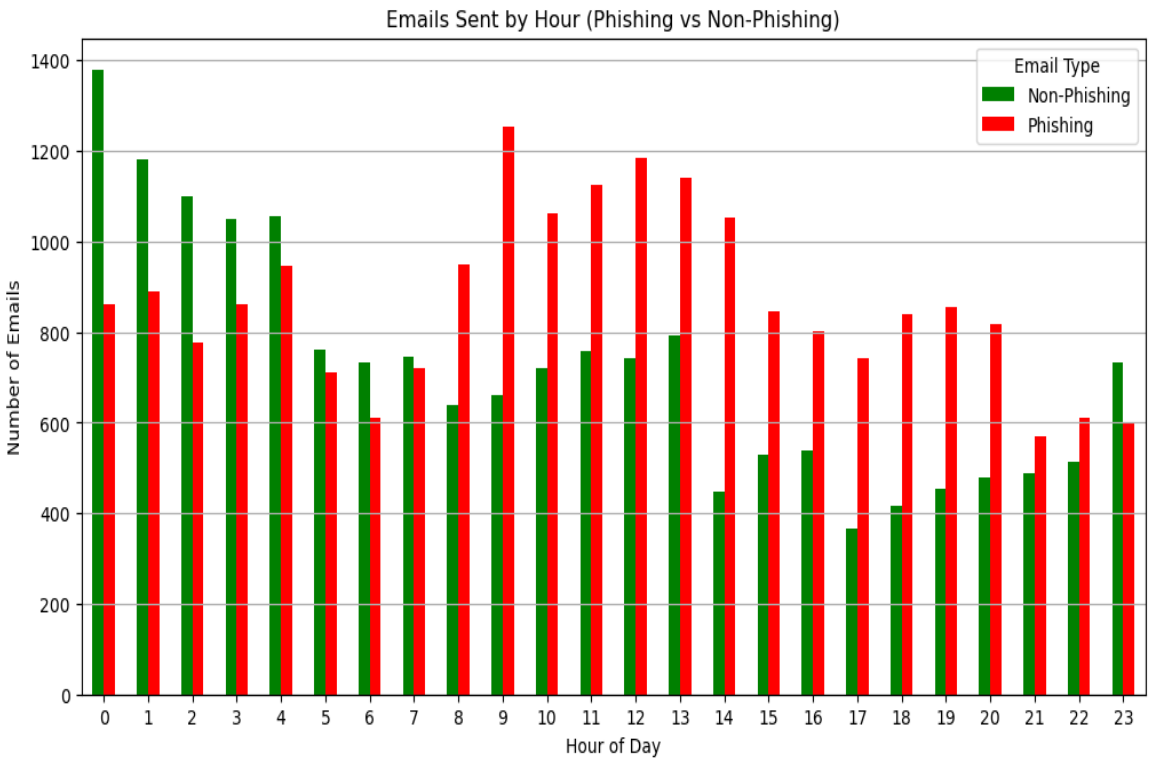


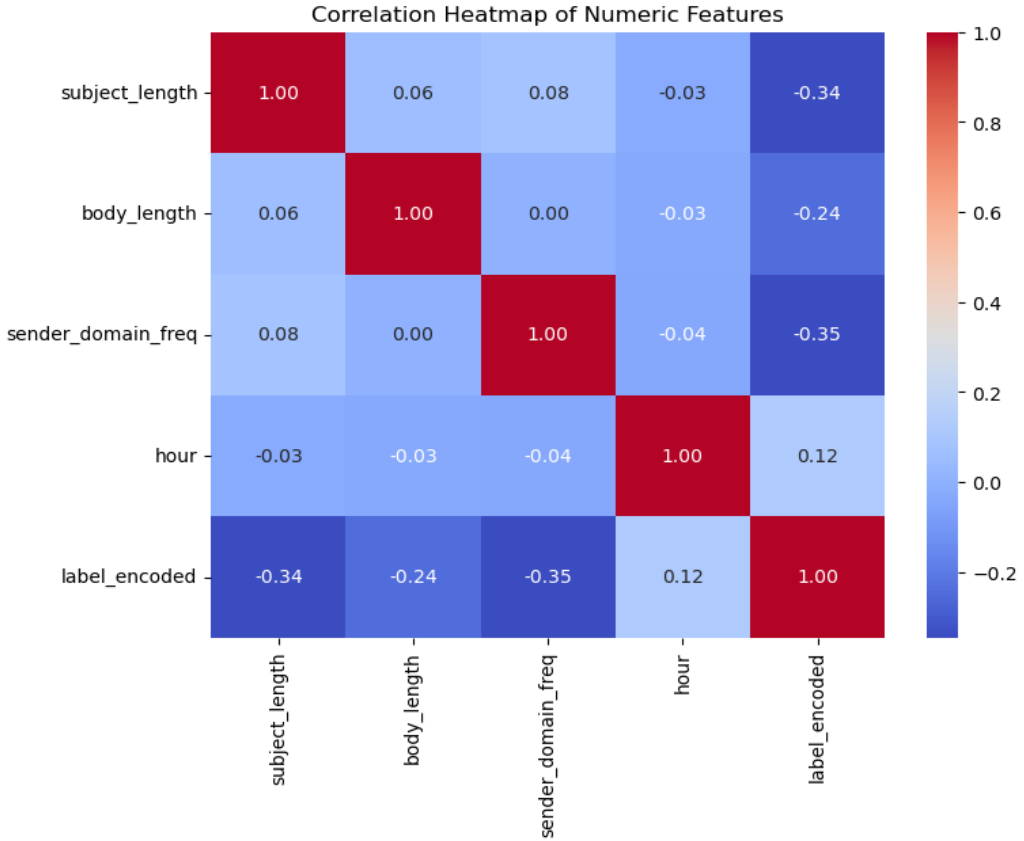
6. FEATURE ANALYSIS:



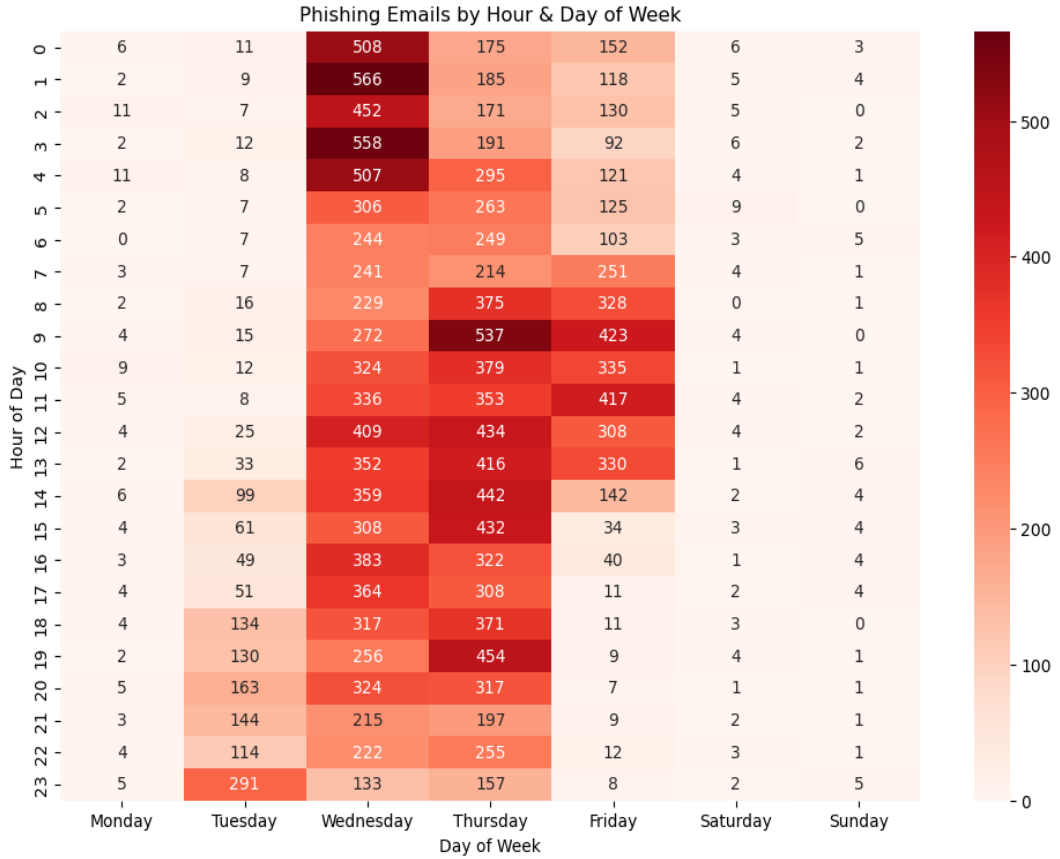


6. FEATURE ANALYSIS:

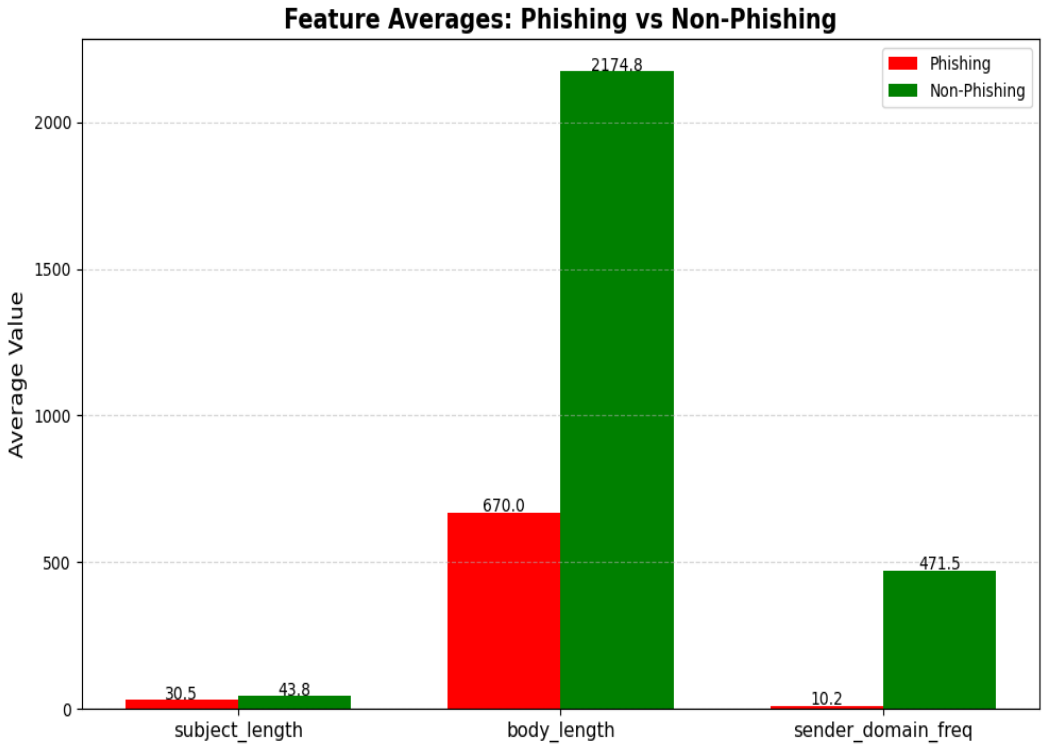


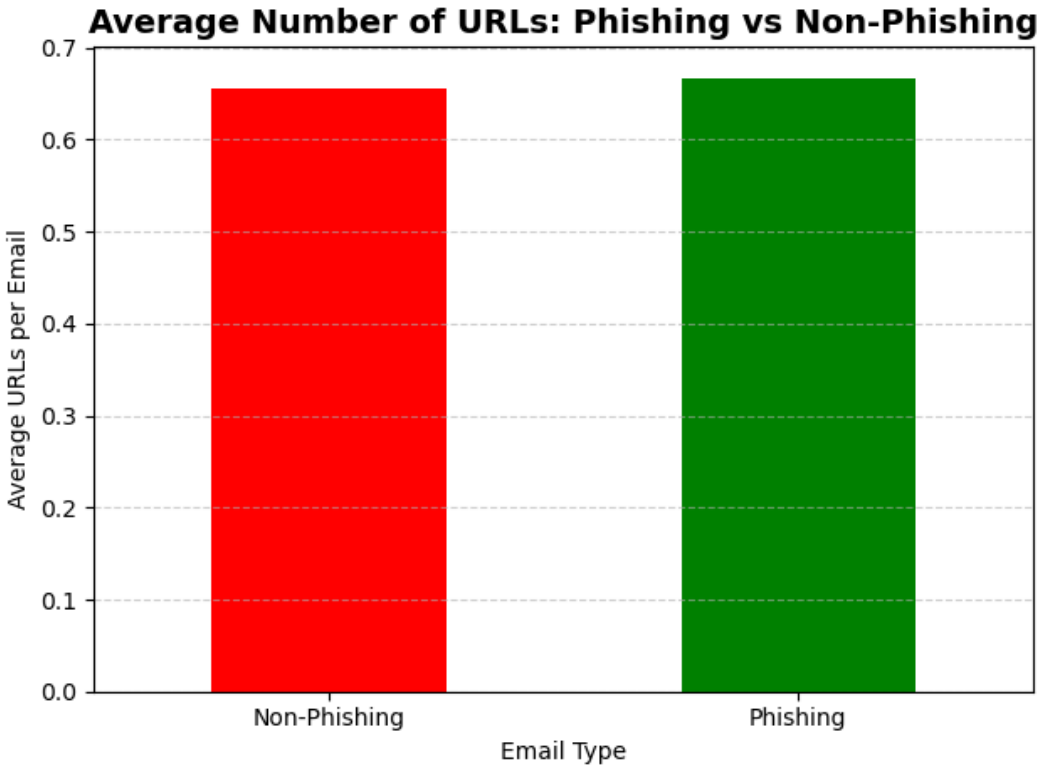


6. FEATURE ANALYSIS:



6. FEATURE ANALYSIS:





7. Models Selection:

- This dataset comes under classification problem, as the email is classified as phishing (1) legitimate(0): the machine learning models (classification) considered to train the dataset in this notebook are:

1. Random Forest.
2. Multilayer Perceptron (MLP).
3. Support Vector Machine (SVM).
4. Logistic Regression.
5. Naive Bayes.

8. Model Evaluation:

- The performance of our machine learning models was evaluated using metrics such as accuracy, precision, recall, and F1-score. We also used a confusion matrix to visualize the model's predictions. These metrics helped us understand how well each model detected phishing emails while minimizing false positives and false negatives.

Labels: Legit = 0 | Phishing = 1 (0/1)

S.N.	Models	Accuracy	Precision	Recall	F1-Score
1.	Random Forest	0.99	0.99 | 0.99	0.99 | 1.0	0.99 | 0.99
2.	Naive Bayes	0.98	0.95 | 1.0	1.0 | 0.96	0.97 | 0.98
3.	Logistic Regression	0.99	1.00 | 0.99	0.99 | 1.0	0.99 | 1.00
4.	Multilayer perceptron	1.00	1.00 | 1.00	1.00 | 1.0	1.00 | 1.00
5.	SVM	1.00	1.00 | 1.00	1.00 | 1.0	1.00 | 1.00

9. Conclusion:

- All tested models achieved high performance in phishing detection, with Multilayer Perceptron and SVM reaching perfect scores across all metrics. Among lightweight models, Logistic Regression performed exceptionally well, achieving near-perfect precision and recall. These results demonstrate that even simple models can be effective for phishing detection on edge devices, making them suitable for real-time and resource-constrained environments.

10. Next Steps:

- As we wrap up this phase of our project, PhishShield, we are excited about the journey ahead. We enjoyed exploring various machine learning models and understanding the patterns behind phishing emails. Our next steps include optimizing the trained models to run efficiently on edge devices, such as Raspberry Pi, ensuring real-time detection with minimal resource usage. We also plan to expand our dataset for better accuracy and robustness. In addition, we aim to design a simple user interface for easy interaction and begin deployment and testing in real-world scenarios. With each step, we look forward to making PhishShield a practical and impactful solution for phishing prevention.