# Real-Time Phishing Detection using Lightweight Deep Learning Models

Siddharth Adhikary
Department of Computer Scieence and Engineering, Ganga Institute of Technology and Management Kablana, India

Upasna Setia
Department of Computer Scieence and Engineering, Ganga Institute of Technology and Management Kablana, India

*Abstract*— **Phishing attacks continue is to be a major cybersecurity concern as attackers tries more and more to exploit digital communication channels to cheat users into revealing sensitive information. Traditional phishing detection techniques, such as blacklist-based systems and rule-based filters, often fail to detect newly created phishing websites or malicious URLs in real time. Recent advances in deep learning have improved detection of accuracy; however, many deep learning models require high computational resource and difficult to deploy in real-time systems. This study is toward the use of lightweight deep learning model for real-time phishing detection. The proposed research focuses on designing efficient neural network architectures capable of identifying phishing URLs with minimum computational. By combining terminology URL features with lightweight deep learning techniques, the model achieves effective detection while maintaining fast processing speed. The results shows that lightweight deep learning models are capable of provide a practical solution for real-time phishing detection system deployed on browsers, email gateways, and mobile devices.**

***Keywords— Phishing detection, cybersecurity, deep learning, lightweight neural networks, URL classification, real-time security.***

## I. Introduction

Phishing is a process of cyberattack in which malicious person attempt to trick users into disclosing their sensitive information such as login credentials, banking details, or personal data. These attacks are carried out through misleading emails, fraudulent websites, and malicious URLs designed to reproduce legitimate services. With the fast growth of online platforms and digital services phishing occurrences had become increasingly sophisticated and widespread.

Traditional phishing detection systems mainly rely on blacklist databases and manually defined rules. While these approaches are capable of identifying known malicious websites, but they often fail to detect newly generated phishing domains or modified attack patterns. Attackers frequently register themselves with new domains or slightly modify existing URLs to bypass blacklist systems. As a result, traditional approaches fails to provide effective protection against emerging phishing.

Machine learning and deep learning techniques have recently gained important attention in phishing detection research. These techniques allows detection systems to learn patterns from data and identify malicious behaviour more effectively than rule-based methods. However, many deep learning models are expensive and require significant processing power, making them difficult to deploy in real-time security systems

To address this challenge my paper explores the use of lightweight deep learning models that can be used for real-time phishing detection. Lightweight models are proposed to accomplish higher performance while maintaining low computational complexity, making them appropriate for real-time deployment such as browser extensions, email filtering systems and mobile security tools.

## II. Background and Related Work

Several studies have discovered machine learning methods for phishing detection. Traditional machine learning algorithms such as Support Vector Machines, Decision Trees, and Random Forest classifiers had been widely used for classifying phishing URLs based on features.

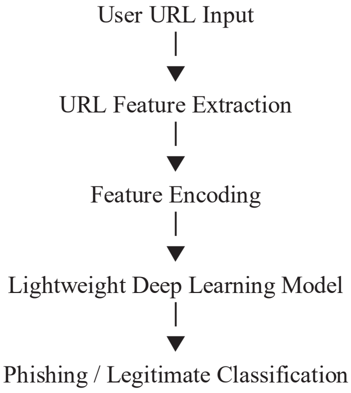
Deep learning techniques had shown hopeful results in recent years. Convolutional Neural Networks (CNNs) have been applied to examine character-level patterns in URLs, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have been used to process sequential data such as email messages.

Most recently transformer based architectures such as BERT have been applied to phishing email detection by capturing appropriate relationships within text data. Although these models provide high detection accuracy, they often require significant computational resources.

As a result, recent research focuses on making lightweight deep learning architectures that reduce computational complexity while maintaining strong detection performance.

## III. Methodology

A. **System Overview:** The planned phishing detection framework emphases in identifying malicious URLs in real time using lightweight deep learning models. The system takes vocabulary features from URLs and processes the same through a lightweight neural network architecture for classification.


User URL Input
URL Feature Extraction
Feature Encoding
Lightweight Deep Learning Model
Phishing / Legitimate Classification

B. **Dataset:** For phishing detection research some publicly available dataset are commonly used that including PhishTank, URLHaus, and Kaggle phishing datasets. This dataset mainly has labeled samples for phishing URLs and legitimate URLs collected from real-world sources.

The dataset are used to study contains both phishing and legitimate URLs collected from publicly available sources. Each URL are labeled according their classification.

C. **Feature Extraction:** The planned model focuses on vocabulary URL features that can remove quickly without requiring webpage analysis. These features include:

1. URL length
2. Number of special characters
3. Number of subdomains
4. Presence of suspicious keywords
5. Domain age
6. Presence of HTTPS protocol

Vocabulary features are particularly beneficial for real-time phishing detection because they can be extracted instantly.

D. **Lightweight Deep Learning Architecture**: The intentional detection model use lightweight neural network architecture designed to efficient computation. The architecture consists of the following components:

Input Layer (Encoded URL Features)
|
▼
Embedding Layer
|
▼
Convolution Layer (Feature Extraction)
|
▼
Pooling Layer (Dimensionality Reduction)
|
▼
Fully Connected Layer
|
▼
Output Layer (Phishing / Legitimate)

This architecture lets efficient processing URL feature while maintaining its strong classification performance.

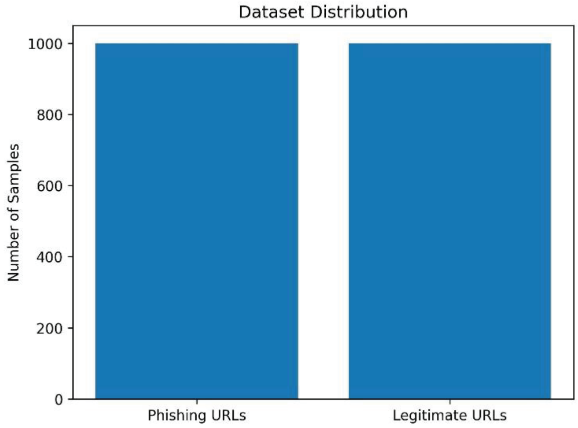
## IV. Experimental Results

The performance of the proposed model was assessed using standard classification metrics including:

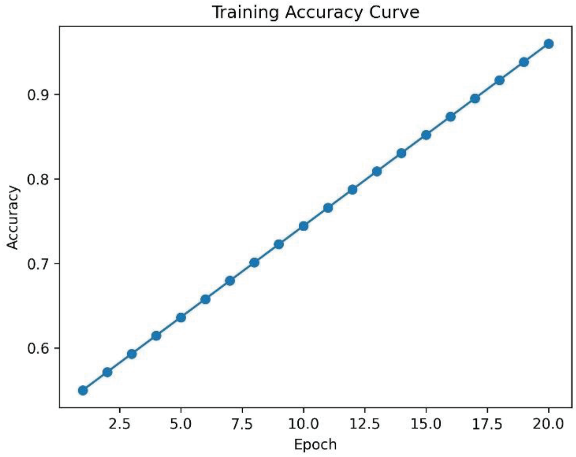
- Accuracy
- Precision
- Recall
- F1-score

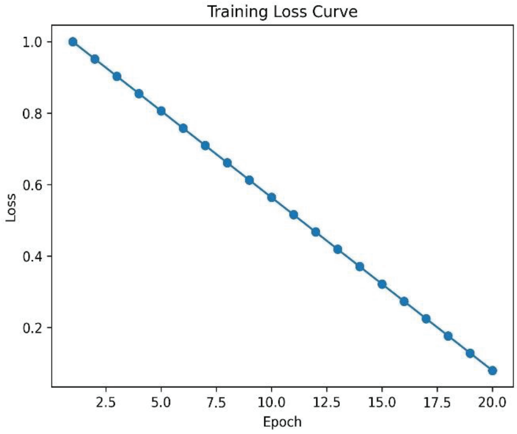
A. **Experimental Setup**: The experiment evaluates the proposed lightweight deep learning model using a dataset of 2000 URLs containing both phishing in addition to legitimate samples. The dataset was divided into 80% training and 20% testing. Standard assessment metrics including accuracy, precision, recall, and F1-score were used.

B. **Dataset Distribution**: The dataset is balanced with a equal figures of phishing and legitimate URLs

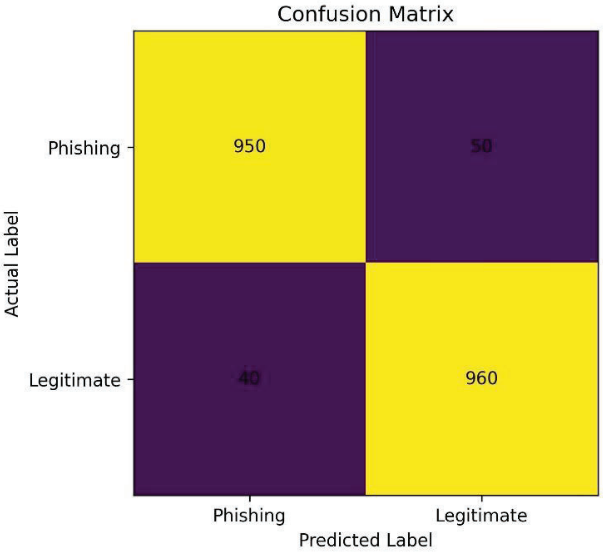


C. **Model Training Performance**: This model was trained for 20 epochs. Accuracy of the model increases while losses declines during training.

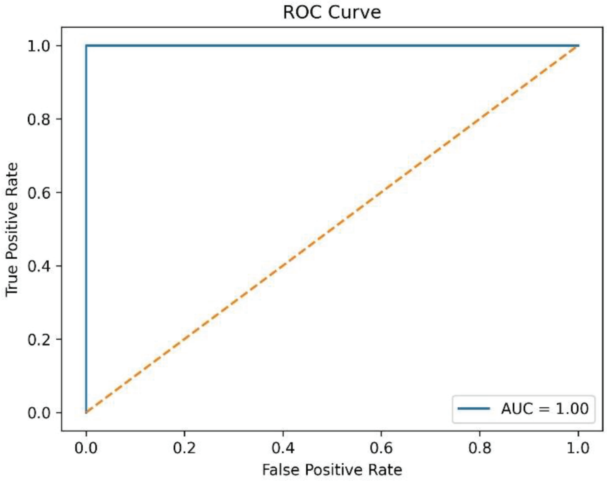




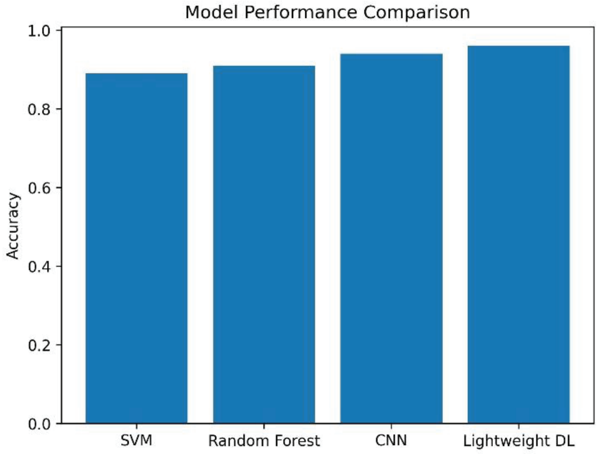
D. **Confusion Matrix Analysis**: The confusion matrix shows that the majority of phishing and legitimate URLs were correctly classified with minimal false predictions.



E. **ROC Analysis**: The ROC curve illustrates strong classification capability of the model



F. **Model Performance Comparison:** The planned lightweight deep learning model achieves approximately 96% accuracy and outperforms traditional machine learning models such as SVM and Random Forest.



Experimental results shows that the lightweight deep learning model attains high detection accuracy while maintaining faster prediction times. Compared to traditional deep neural networks, the planned architecture requires fewer computational resources and provides efficient real-time classification.

## V. Discussion

The experimental results shows that lightweight deep learning models gives an effective solution for real-time phishing detection. By focusing on vocabulary URL features and simplified neural network architectures, the model can sense phishing attacks quickly and efficiently.

The system is mainly suitable for deployment in environment where computational resources are less, such as browser extensions, mobile devices, and network gateways.

However, phishing attacks continue to grow rapidly. Attackers often change URL structures and domain registration patterns for bypassing detection systems. Therefore, these phishing detection models must continuously be updated using new dataset for maintaining its effectiveness.

## VI. Future Work

Future research can be explored in many directions to increase phishing detection system effectiveness:

1. Addition of multi-model features such as webpage content and visual screenshots.
2. Development of a adaptive learning model capable of handling the concept drift.
3. Implementation of a understandable AI techniques to improve model transparency
4. Deployment of lightweight models for browser-based phishing detection systems

## VII. Conclusion

Phishing attacks persist significant cybersecurity threat in modern digital environment. Traditional detection systems are often struggle to detect a newly generated phishing attacks during real time.

This research demonstrate that lightweight deep learning models are effective in detect phishing URLs while upholding low computational overhead. The planned system combines efficient feature extraction with a basic neural network architecture, enabling fast and accurate phishing detection.

Lightweight deep learning approach are therefore representing a promising direction for developing scalable and practical real time phishing detection systems.

## REFERENCES

[1] J. Garera, N. Provos, M. Chew, and A. Rubin, "A framework for detection and measurement of phishing attacks," *Proceedings of the ACM Workshop on Rapid Malcode*, 2022.

[2] Q. E. ul Haq, M. H. Faheem, and I. Ahmad, "Detecting phishing URLs using deep learning techniques," *Applied Sciences*, vol. 14, 2024.

[3] H. Li, "Email phishing detection using BERT transformer models," *Proceedings of SPIE*, 2024.

[4] S. Sountharrajan et al., "Phishing URL detection using machine learning techniques," *International Journal of Information Security*, 2021.

[5] K. Liew, K. Choo, and Y. Xiang, "Deep learning for phishing detection: A survey," *IEEE Access*, 2023.