iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70715

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Proactive Detection of Phishing and Malicious Link

Dr. Kavitha V[1], Dr. R.G. Suresh Kumar[2], Mr. Ragu K[3], Mr. Thamizhselvan K[4], Mr. Sathiyan D[5]
[1]*Professor, RGCET, Puducherry*
[2, 3, 4]*B.Tech (CSE), RGCET, Puducherry*

Abstract: In Deep Learning is a branch of Artificial Intelligence (AI) that has proven effective in various predictive tasks, including identifying malicious URLs and phishing links. It recognize Complex patterns in text, picture, sound and other data to produce accurate insights and predictions.

Existing systems often rely on unsupervised algorithms to detect phishing links; These methods typically suffer from lower prediction accuracy and are limited in scope, focusing only on phishing detection.

To address these limitations, We Prove a hybrid model combining Deep Learning and Transfer Learning algorithms has been developed. This approach enhances the accuracy of predictions. Then, the hybrid model extends the detection capabilities to both malicious and phishing links, ensuring comprehensive protection .

Keywords: Bolstering cybersecurity, phishing URLs and malicious links, deep learning techniques.

I. INTRODUCTION

Malicious URLs present serious risks in the world of digital networks since they act as trickery access points for fraud, cyberattacks, and scams. These carefully crafted URLs have the potential to spread malware, start spear-phishing or phishing campaigns, and aid in other types of online fraud. Their threat stems from their propensity to blend in, which makes them difficult to spot and more likely to be ignored. As the human factor in cybersecurity is acknowledged, education becomes essential. Users that receive security awareness training are better equipped to recognize and handle the complex web of harmful links.

Organizations may improve their overall resistance against the ubiquitous threat ofharmful URLs by cultivating a culture of cyber literacy and caution.

This will make the digital world more secure for both individuals and enterprises.

Phishing connections represent yet another dishonest technique employed by cybercriminals to take advantage of people and institutions. These links are usually placed within what appear to be innocent emails, messages, or webpages in an attempt to deceive users into disclosing private information such login passwords, bank account information, or personal information. Phishing connections frequently use social engineering techniques, in which hackers create websites or communications that look like trustworthy organizations in order to install a false sense of urgency and trust.

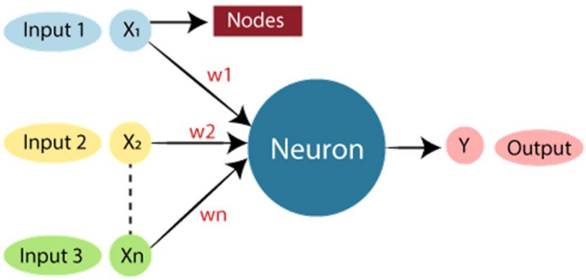


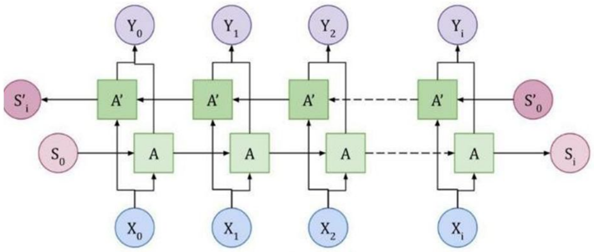
FIG 1.1. Deeplearning Architecture

Users should use caution and confirm the legitimacy of unexpected messages or emails before clicking on embedded links in order to combat phishing risks. To teach users how to spot and steer clear of phishing efforts, firms must implement email filtering systems and security awareness training.

An additional line of protection against these misleading links comes from online browsers and cybersecurity software, which frequently include antiphishing tools to identify and prevent access to known dangerous websites. When it comes to cybersecurity, awareness, education, and cutting-edge technologies continue to be essential components of protecting against ever-changing dangers such as malicious URLs and phishing attempts.

A. Bidirectional Long Short-Term Memory (BiLSTM)

A Bidirectional Long Short-Term Memory (BiLSTM) is a type of recurrent neural network (RNN) architecture commonly used for sequence processing tasks, such as natural language processing and time series analysis. The key feature of a BiLSTM is that it consists of two LSTM layers: one processing the input sequence in a forward direction, and the other processing it in a backward direction. The forward LSTM processes the input sequence from the beginning to the end, while the backward LSTM processes it in the reverse order, starting from the end and moving towards the beginning. This bidirectional processing allows the BiLSTM to capture information from both past and future states of the input sequence.

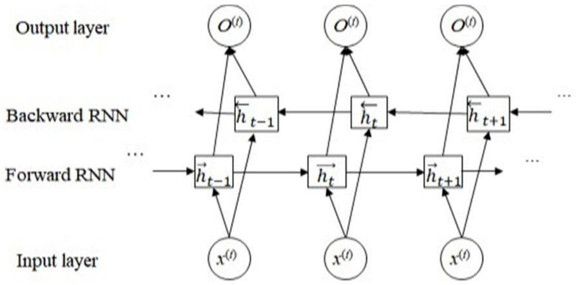


Bidirectional LSTM layer Architecture

By having two LSTM layers operating in opposite directions, a BiLSTM effectively increases the amount of context available to the network. For example, when processing a sentence, the forward LSTM can understand the context of each word based on the words that come before it, while the backward LSTM can understand the context based on the words that come after it. Combining information from both directions enables the BiLSTM to have a more comprehensive understanding of the input sequence.

B. BIGRU (Bidirectional Gated Recurrent Unit):

BiGRU, short for bidirectional gated recurrent unit, represents a recurrent neural network architecture designed to effectively capture contextual information from input sequences. Comprising two separate GRU (Gated Recurrent Unit) layers, the BiGRU model processes input data in both the forward and backward directions. Each GRU layer independently analyzes the sequence, leveraging its gating mechanisms to control the flow of information and capture long-range dependencies within the data.



In the forward direction, the first GRU layer processes the input sequence sequentially, while the second GRU layer operates in the reverse direction, analyzing the input sequence from the end to the beginning. This bidirectional processing allows the BiGRU model to extract contextual information from both past and future states of the input data, enhancing its understanding of the temporal dynamics and relationships within the sequence.

II. RELATED WORK

The research introduces a transfer learning-based hybrid model for detecting phishing URLs and malicious links, addressing key cybersecurity challenges [1]. By leveraging deep neural networks and transfer learning, the model effectively captures intricate patterns in URL structures. A curated dataset undergoes rigorous preprocessing to enhance input quality. The model integrates soft and hard voting mechanisms to improve accuracy, while feature selection and hyperparameter optimization refine performance. Comprehensive evaluation metrics validate its robustness, ensuring enhanced threat detection.

This innovative approach strengthens cybersecurity defenses, providing a more adaptive and efficient solution against evolving phishing and malicious cyber threats. [2] In the intricate web of the digital realm, malicious URLs stand as insidious gateways designed to perpetrate scams, cyber-attacks, and fraud. Crafted with deceptive intent, these URLs pose a severe threat, capable of triggering downloads of ransomware, initiating phishing or spear-phishing endeavors, and fostering diverse forms of cybercrime. The inherent danger lies in their ability to disguise themselves, making them inconspicuous and easy to overlook, thereby heightening the risk they pose to the digital landscape.

Mitigating the menace of malicious URLs requires a multi-faceted approach. Individual users can fortify their defenses by adopting vigilant practices, such as refraining from opening suspicious links or downloading files from dubious emails or websites. For businesses, a proactive stance involves implementing robust security measures, including the utilization of secure email gateways like ContentCatcher and next-generation firewalls equipped with updated subscriptions for URL filtering.

These technological safeguards serve as vital barriers against the infiltration of malicious URLs. [3] Phishing characteristics, denoting distinct properties found in phishing websites, play a crucial role in enhancing cybersecurity measures. The efficacy of incorporating these characteristics is evident in the observation that the proposed approach outperformed methods relying solely on blacklists by significantly detecting more phishing websites at the zero-hour mark. This capability is particularly noteworthy, as it reflects the proactive nature of the approach, enabling the identification of phishing threats in their early stages before widespread recognition and blacklisting. The emphasis on catching a substantial number of phishing websites at zero hour is instrumental in preemptively countering cyber threats, preventing potential harm, and fortifying overall cybersecurity resilience.

Traditional reliance on blacklists may face limitations in swiftly detecting emerging threats, underscoring the added value of incorporating phishing characteristics to stay ahead of evolving phishing tactics. [4] A notable disadvantage associated with complex models like gradient boosting and the proposed hybrid LSD model is the potential for overfitting. Overfitting occurs when a model is excessively tuned to the nuances and noise present in the training data, to the extent that it may struggle when exposed to new, unseen data.

While these models can achieve impressive performance on the training dataset, their ability to generalize to real-world scenarios, particularly with diverse and unfamiliar data, may be compromised.

The risk of overfitting is particularly pronounced when dealing with intricate and intricate models. Gradient boosting, for example, is known for its capacity to fit the training data very closely, which can inadvertently lead to capturing noise or outliers that do not represent true patterns in the underlying data distribution.

As a result, the model may exhibit reduced performance when applied to different datasets or when faced with previously unseen instances, as it might struggle to discern genuine patterns from the noise present in the training data. Mitigating overfitting often involves strategies such as regularization techniques, cross-validation, and careful feature selection. While these methods can help alleviate overfitting to some extent, the risk remains, and finding the right balance between model complexity and generalization capability is a persistent challenge in the development of robust machine learning models. [5] Overfitting is a common challenge in machine learning, particularly when dealing with complex models like gradient boosting and the proposed hybrid LSD model. It occurs when a model becomes too intricately tailored to the specific patterns and noise present in the training data. As a result, the model may perform exceptionally well on the data it was trained on, but when exposed to new, unseen data—such as real-world scenarios or a different dataset—it may struggle to generalize accurately.

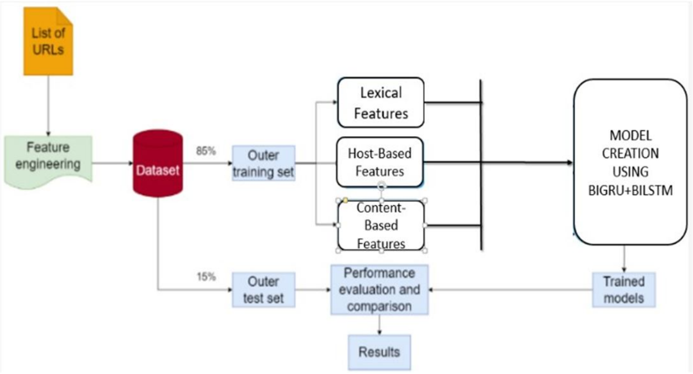
The root cause of overfitting lies in the model's ability to capture not only the underlying patterns in the data but also the noise, outliers, or random fluctuations unique to the training dataset. Complex models, by their nature, have a higher capacity to learn intricate details and nuances, but this heightened capacity can lead to the model memorizing specific examples from the training data rather than learning the true underlying patterns. When faced with new data, the overfit model may attempt to apply the same overly detailed patterns it learned during training, even if those patterns were specific to the noise in the training data.

As a result, the model's performance degrades, as it struggles to discern genuine signals from the noise it memorized. This lack of generalization can undermine the model's effectiveness in real-world applications, where the goal is to make accurate predictions or classifications on unseen instances.

The contemporary internet landscape is rife with vulnerabilities, exposing novice or careless users to a myriad of threats [6]. Notorious individuals exploit various tools and techniques to compromise users' personal data, leading to significant losses and security breaches. Despite continuous efforts by web users, software developers, and application creators to fortify IT infrastructure through encryption, digital signatures, and certificates, phishing remains a persistent and challenging problem.

This paper takes a focused approach to address the issue of phishing, aiming to detect and predict phishing website URLs.

A. Architecture Diagram



The architecture of the BiLSTM-BiGRU hybrid model for phishing and malicious link detection is designed to effectively analyze URL sequences and extract meaningful patterns. It begins with an input layer, where raw URLs undergo preprocessing, including text normalization and tokenization.

These URLs are then transformed into numerical representations using word embeddings such as Word2Vec or FastText, allowing the model to understand semantic relationships between different URL components. Next, the model incorporates a feature extraction layer, which processes lexical, hostbased, and content-based features.

This step ensures that the model captures key characteristics distinguishing legitimate URLs from phishing or malicious ones. The extracted features are then passed into the Bidirectional Long Short-Term Memory (BiLSTM) layer, which analyzes the URL sequence from both forward and backward directions. This bidirectional approach enables the model to retain long-range dependencies and better understand contextual information within the URL structure.

Following BiLSTM, the Bidirectional Gated Recurrent Unit (BiGRU) layer enhances computational efficiency while maintaining sequential learning capabilities. Since BiGRU has fewer parameters than LSTM, it reduces the computational load without sacrificing accuracy. The combination of BiLSTM and BiGRU allows the model to learn complex URL patterns, improving its ability to detect phishing and malicious links.To further refine predictions, the model employs a voting mechanism, integrating both soft and hard voting techniques. Soft voting aggregates probability scores from multiple classifiers, while hard voting makes the final decision based on the majority outcome. This ensemble learning technique ensures greater robustness and accuracy in threat detection.

III. PROPOSED SYSTEM

The proposed approach introduces a hybrid BiLSTM-BiGRU model for enhanced cybersecurity, focusing on phishing and malicious link detection. Unlike traditional models, BiLSTM and BiGRU efficiently capture sequential dependencies and temporal patterns in URLs, making them well-suited for identifying cyber threats.

These networks analyze URL structures bidirectionally, improving pattern recognition and reducing misclassification. To enhance detection accuracy, the model employs soft and hard voting mechanisms. Soft voting aggregates probability scores from multiple classifiers, refining predictions, while hard voting ensures reliability by selecting the most frequent classification.

This ensemble technique boosts robustness, stability, and accuracy in phishing detection. Additionally, the system can detect both phishing and malicious URLs simultaneously, addressing multiple cybersecurity concerns. Unlike conventional methods that focus on one threat type, this integrated approach enhances security coverage, offering a more comprehensive defense mechanism against evolving cyber threats. By leveraging deep learning and ensemble techniques, this model ensures a scalable, adaptable, and highly accurate cybersecurity solution. Its ability to detect subtle URL manipulations makes it particularly useful for real-time threat prevention, safeguarding users against phishing attacks and malicious links in today's dynamic digital environment.

A. Data Collection

Data collection is the first and most critical step in developing a BiLSTM-BiGRU-based phishing and malicious link detection model. A high-quality dataset is essential to ensure accurate training and evaluation of the model. For this purpose, publicly available datasets from platforms such as Kaggle, PhishTank, and OpenPhish are used. These datasets contain a mixture of legitimate and malicious URLs, including phishing links designed to steal user credentials.

The dataset is curated to include a diverse range of URL structures, domains, and attack patterns, ensuring the model learns from real-world cases. Additional features, such as URL length, domain age, presence of special characters, and embedded redirections, are extracted to provide more context. The dataset is then split into training, validation, and testing sets to facilitate model development and prevent overfitting.

To enhance dataset quality, data augmentation techniques are applied, ensuring a balanced representation of both phishing and legitimate URLs. By collecting large-scale and diverse data, the model can generalize better across different phishing attempts. Proper labeling and verification of URLs are performed to maintain data integrity and reliability, ensuring the model is trained on accurate and unbiased information.

B. PRE-Processing

Pre-processing is essential to clean and prepare the collected dataset for efficient model training. Since raw URLs contain unnecessary information, multiple pre-processing steps are applied to improve data quality. First, data cleaning is performed to remove duplicate URLs, missing values, and inconsistent entries. This step ensures that redundant data does not introduce bias into the model. Next, tokenization is applied, breaking URLs into meaningful components such as protocols (HTTP/HTTPS), subdomains, domain names, and paths. This helps the model understand URL structures better. Further, special characters, numbers, and symbols are either removed or replaced with specific tokens to maintain uniformity. Feature encoding techniques, such as one-ht encoding and word embeddings, are used to convert categorical URL components into numerical representations suitable for deep learning models. To ensure better model generalization, data balancing techniques like Synthetic Minority Oversampling Technique (SMOTE) are applied to avoid class imbalance. Normalization is also performed to scale numerical features between 0 and 1, preventing bias toward larger values. By implementing these comprehensive preprocessing steps, the dataset becomes well-structured, reducing noise and improving

C. Feature Extraction

Feature extraction plays a crucial role in training an accurate phishing and malicious URL detection model. Instead of relying solely on raw URLs, key linguistic and structural features are extracted to help the BiLSTM-BiGRU model learn patterns efficiently.

The extracted features are categorized into lexical, host-based, and content-based features. Lexical features include URL length, presence of special characters, number of dots, hyphens, and entropy levels, which help detect obfuscation techniques used in phishing URLs. Host-based features analyze domain age, WHOIS registration details, SSL certificate validity, and DNS record information, identifying whether the URL originates from a legitimate or suspicious source. Content-based features focus on redirect chains, embedded links, and frequency of sensitive keywords like "login" or "verify." Additionally, Natural Language Processing (NLP) techniques such as word embeddings (Word2Vec, TF-IDF) convert textual components of URLs into numerical vectors. This enables deep learning models to identify hidden patterns within URLs.

The extracted features are then normalized and fed into the BiLSTM-BiGRU model, ensuring that it learns key attributes distinguishing phishing links from legitimate ones. Feature extraction significantly enhances the model's ability to generalize across different types of phishing threats, improving detection accuracy and robustness.

D. Model Creation

The BiLSTM-BiGRU hybrid model enhances phishing and malicious link detection by capturing sequential patterns and contextual relationships within URLs. BiLSTM processes sequences both forward and backward, ensuring comprehensive dependency capture, while BiGRU reduces computational complexity with efficient gating mechanisms. The architecture includes an Embedding Layer (converts URLs into numerical vectors), BiLSTM Layer (captures long-range dependencies), BiGRU Layer (enhances feature extraction), Dropout Layer (prevents overfitting), Fully Connected Layer (classifies URLs), and a Softmax Output Layer (assigns probability scores). By combining BiLSTM and BiGRU, the model improves accuracy, efficiency, and robustness in detecting phishing threats.

E. Test Data

The test data phase ensures the model’s ability to generalize beyond the training dataset. After training, the BiLSTM-BiGRU model is evaluated using a separate set of unseen URLs. This dataset consists of both phishing and legitimate links, carefully labeled for objective assessment. Before feeding the test data into the model, it undergoes the same pre-processing and feature extraction steps as the training data.

This maintains consistency and ensures that the model receives properly formatted inputs. To measure the model’s performance, key evaluation metrics such as accuracy, precision, recall, and F1-score are used. Accuracy measures the overall correctness of predictions, while precision and recall assess how well the model distinguishes phishing URLs.

The F1-score balances precision and recall, providing a holistic measure of performance. During testing, the model is subjected to real-world phishing scenarios, including sophisticated attacks involving obfuscated URLs, redirections, and domain spoofing.

The results are compared with traditional classifiers like Random Forest (RF) and Support Vector Machines (SVM) to validate the superiority of the BiLSTM-BiGRU model. By evaluating the model on unseen test data, its generalization capability, robustness, and reliability in detecting phishing threats are assessed.

F. Prediction

Once trained, the BiLSTM-BiGRU model predicts phishing and malicious URLs in real-time. A new URL undergoes pre-processing (cleaning, tokenization), feature extraction (lexical, host-based, content-based), and model inference (analyzing patterns). If the predicted probability surpasses a threshold, the URL is flagged as phishing; otherwise, it is classified as legitimate. To enhance reliability, soft and hard voting mechanisms refine decision-making. When integrated into cybersecurity systems, detected phishing links can be automatically blacklisted. This deep learning-based approach ensures fast, automated, and accurate phishing detection, strengthening cybersecurity defenses against evolving threats.

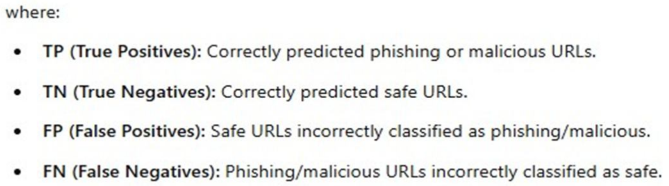
IV. RESULT AND DISCUSSION

In the context of your research, performance analysis entails a careful review and assessment of the cybersecurity models that have been built. This procedure comprises the use of strict metrics to evaluate several facets of the models' functionality. Accuracy, precision, recall, F1 score, and area under the receiver operating characteristic (ROC) curve are a few examples of these measurements. ThZ research aims to provide a nuanced understanding of how well the Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN), integrated through transfer learning, perform in detecting and mitigating malicious links and phishing URLs by utilizing such extensive evaluation criteria. An essential first step in confirming the resilience and effectiveness of the suggested cybersecurity solution is the performance analysis. Researchers and practitioners can use it to assess how well the model adjusts to the ever-changing and dynamic world of cyber threats, and it can provide valuable information about its advantages, disadvantages, and possible areas for development. All things considered, the performance analysis plays a crucial role in proving the validity and practicality of the generated models in strengthening cybersecurity defenses.

A. Accuracy

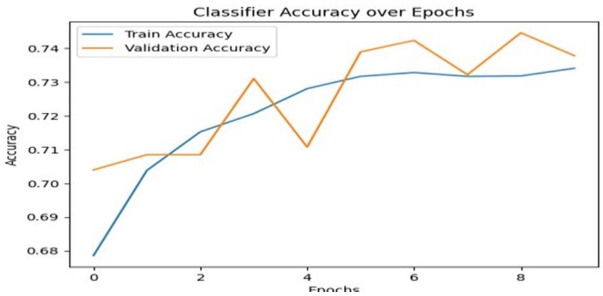
Accuracy is a key metric for evaluating the performance of the proposed BiLSTM-BiGRU hybrid model in detecting phishing and malicious links. It measures how well the model correctly identifies phishing and malicious URLs while minimizing misclassification. The formula for accuracy is:

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$



where:

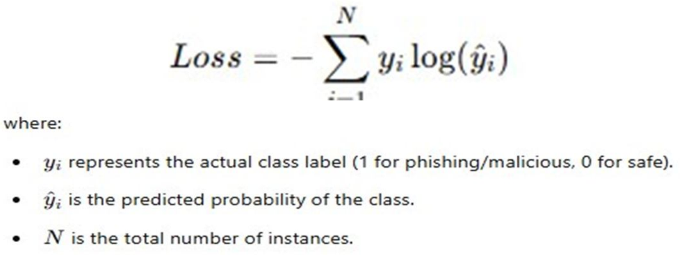
- **TP (True Positives):** Correctly predicted phishing or malicious URLs.
- **TN (True Negatives):** Correctly predicted safe URLs.
- **FP (False Positives):** Safe URLs incorrectly classified as phishing/malicious.
- **FN (False Negatives):** Phishing/malicious URLs incorrectly classified as safe.



A high accuracy value indicates that the model effectively distinguishes between safe and harmful links, leading to better cybersecurity protection. However, accuracy alone may not be sufficient, especially in imbalanced datasets where phishing URLs are far fewer than safe ones. In such cases, a model predicting mostly "safe" URLs can still achieve high accuracy but fail to detect actual phishing threats. Therefore, the integration of precision, recall, and F1-score alongside accuracy provides a more comprehensive assessment. By leveraging BiLSTM and BiGRU's sequential learning capabilities and the voting mechanism, the hybrid model ensures high accuracy while maintaining balance between false positives and false negatives, making it a reliable cybersecurity solution.

B. LOSS

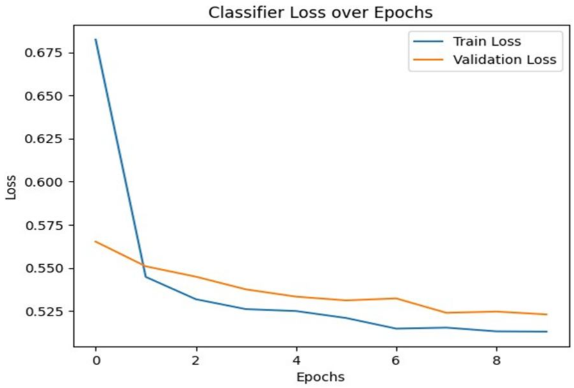
Loss functions measure the discrepancy between the predicted output of a model and the actual target values. In classification tasks like phishing and malicious URL detection, categorical cross-entropy loss is commonly used. The formula for cross-entropy loss is:



$$Loss = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

where:

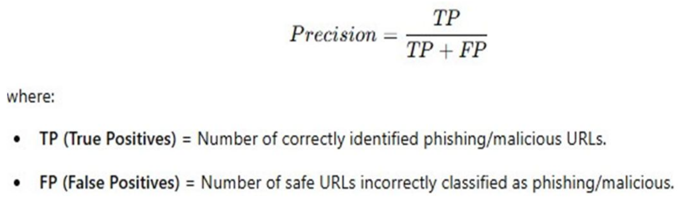
- y_i represents the actual class label (1 for phishing/malicious, 0 for safe).
- $\hat{y}_i$ is the predicted probability of the class.
- N is the total number of instances.



This loss function penalizes incorrect predictions more when the model is highly confident but wrong, encouraging better probabilistic predictions. In the BiLSTM-BiGRU hybrid model, minimizing the crossentropy loss is crucial for improving accuracy. Since both architectures excel in learning sequential dependencies, the model gradually refines its predictions by adjusting weights to reduce loss. Lower loss values indicate better alignment between predicted and actual labels, leading to improved classification. However, if loss remains high, it may indicate overfitting, underfitting, or insufficient training data. Regularization techniques like dropout and batch normalization can help stabilize the learning process, ensuring the model generalizes well to unseen URLs.

C. Precision

Precision is a key metric used to evaluate the performance of classification models, particularly in phishing and malicious URL detection. It measures the proportion of correctly predicted positive cases (phishing/malicious URLs) out of all predicted positive cases. The formula for precision is:



$$Precision = \frac{TP}{TP + FP}$$

where:

- **TP (True Positives)** = Number of correctly identified phishing/malicious URLs.
- **FP (False Positives)** = Number of safe URLs incorrectly classified as phishing/malicious.

A high precision value indicates that the model makes fewer false positive errors, meaning it correctly identifies most phishing/malicious URLs while minimizing misclassification of safe URLs. Low precision, on the other hand, means that the model incorrectly flags many safe URLs, leading to unnecessary security alerts. In the BiLSTM-BiGRU hybrid model, optimizing precision ensures that only genuine phishing/malicious URLs are flagged, reducing unnecessary warnings while maintaining strong cybersecurity defenses. Adjusting the decision threshold and fine-tuning model parameters can help balance precision with other metrics like recall for optimal performance.

D. Recall

Recall measures how well a model correctly identifies all actual positive cases (phishing or malicious URLs). It calculates the proportion of correctly predicted positive cases out of all actual positive cases. The formula for recall is:

$$Recall = \frac{TP}{TP + FN}$$

where:

- **TP (True Positives)** = Correctly detected phishing/malicious URLs.
- **FN (False Negatives)** = Actual phishing/malicious URLs that were incorrectly classified as safe.

A high recall means that the model successfully detects most phishing/malicious URLs, reducing the risk of undetected threats. However, a high recall with low precision may lead to false alarms, affecting system reliability.

E. F1 Score

F1 Score is the harmonic mean of precision and recall, balancing both metrics to provide a single performance measure. It is useful when there is an imbalance between false positives and false negatives. The formula is:

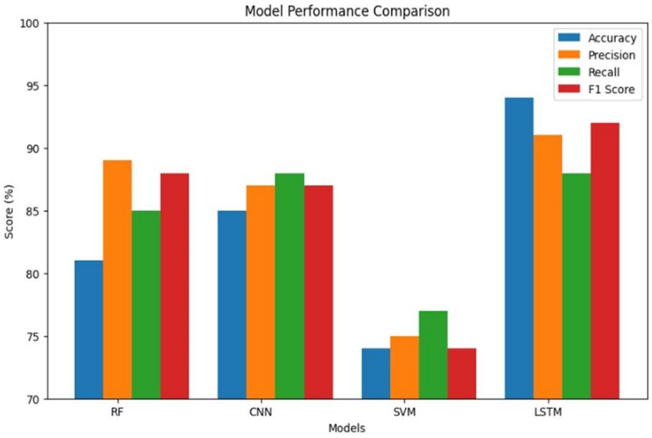
$$F1Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

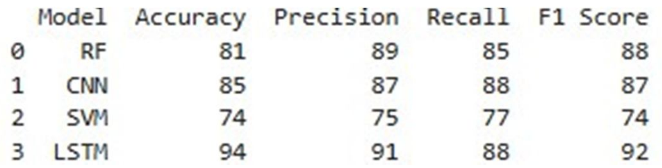
A high F1 Score indicates that the model maintains both high precision and recall, ensuring accurate detection while minimizing false alerts. In the BiLSTM-BiGRU model, optimizing the F1 Score ensures that the system detects phishing and malicious URLs effectively without excessive misclassification.

F. Comparison Graph

The comparison of different models—Random Forest (RF), Convolutional Neural Network (CNN), Support Vector Machine (SVM), and Long Short-Term Memory (LSTM)—highlights the performance differences in terms of accuracy, precision, recall, and F1-score. Among these, LSTM outperforms all other models with an accuracy of 94%, making it the most effective for emotion detection from speech.

It also achieves a high F1-score of 92, indicating a balanced performance across precision and recall.





```
  Model  Accuracy  Precision  Recall  F1 Score
0    RF        81         89      85        88
1   CNN        85         87      88        87
2   SVM        74         75      77        74
3  LSTM        94         91      88        92
```

CNN follows closely with an accuracy of 85%, showing strong generalization ability, particularly in recognizing key emotional patterns. However, its F1score (87) is slightly lower than LSTM, suggesting that it may not capture sequential dependencies as effectively. Random Forest (RF) achieves an accuracy of 81%, demonstrating good performance but lower than CNN and LSTM due to its inability to process temporal features efficiently. On the other hand, SVM performs the worst, with an accuracy of only 74%, struggling with recall and F1-score.

This suggests that SVM may not be well-suited for complex speech emotion recognition tasks. Overall, LSTM proves to be the most effective model, offering superior accuracy and balanced precision-recall tradeoffs, making it the best choice for real-world applications.

V. CONCLUSION

In conclusion, an era of escalating cyber threats, this research introduces a robust phishing and malicious URL detection model leveraging transfer learning with BiLSTM and BiGRU networks. By capturing sequential dependencies and temporal patterns, the model enhances detection accuracy beyond traditional approaches.

The integration of advanced feature selection and hyperparameter optimization ensures optimal performance, making the system adaptable to evolving threats. This research contributes to the field by presenting a scalable, intelligent, and adaptive solution, paving the way for enhanced digital security against phishing attacks and malicious links. Future work can focus on integrating real-time threat intelligence to detect emerging phishing URLs dynamically. Enhancing the model with ensemble learning using CNNs, Transformers, or Attention Mechanisms can improve accuracy.

REFERENCES

[1] Dhanalakshmi Ranganayakulu, Chellappan C., Detecting Malicious URLs in E-mail – An Implementation, AASRI Procedia, Vol. 4, 2013, Pages 125-131, ISSN 2212-6716, https://doi.org/10.1016/j.aasri.2013.10.020.

[2] Yu, Fuqiang, Malicious URL Detection Algorithm based on BM Pattern Matching, International Journal of Security and Its Applications, 9, 33- 44, 10.14257/ijsia.2015.9.9.04.

[3] K. Nirmal, B. Janet and R. Kumar, Phishing - the threat that still exists, 2015 International Conference on Computing and Communications Technologies (ICCCT), Chennai, 2015, pp. 139-143, doi: 10.1109/ICCCT2.2015.7292734.

[4] F. Vanhoenshoven, G. Napoles, R. Falcon, K. Vanhoof and M. K ´ oppen, ¨ Detecting malicious URLs using machine learning techniques, 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, 2016, pp. 1-8, doi: 10.1109/SSCI.2016.7850079.

[5] https://www.kaggle.com/xwolf12/ malicious-andbenign-websites accessed on 27.01.2021

[6] https://openphish.com/ accessed on 27.01.2021

[7] Doyen Sahoo, Chenghao lua, Steven C. H. Hoi, Malicious URL Detection using Machine Learning: A Survey, arXiv:1701.07179v3 [cs.LG], 21 Aug 2019

[8] Rakesh Verma, Avisha Das, What's in a URL: Fast Feature Extraction and Malicious URL Detection, ACM ISBN 978-1-4503-4909-3/17/03

[9] Frank Vanhoenshoven, Gonzalo Napoles, Rafael Falcon, Koen Vanhoof and Mario Koppen, Detecting Malicious URLs using Machine Learning Techniques, 978-1-5090-4240-1/16 2016, IEEE.