IJITS

International Journal of Intelligent Technologies and Systems

Vol. 2, Issue 1, September-October 2025

Enhancing Cybersecurity with Deep Learning based Malicious and Phishing Link Detection

[1]Dr. Sowri Raja Pillai N*, [2]Hema M, [3]Ranjana J, [4]Sangavi C
sowrirajacse@gmail.com

[1]Head, RAAK College of Engineering and Technology, Puducherry, India.

[2, 3, 4]RAAK College of Engineering and Technology, Puducherry, India.

OPEN ACCESS
Research Article

Received: 15 September, 2025
Revised: 06 October, 2025
Accepted: 24 October, 2025
Corresponding Author:
Dr. Sowri Raja Pillai N
sowrirajacse@gmail.com

Publisher:
Aarambh Quill Publications

ABSTRACT

In response to the pressing cybersecurity challenges posed by the proliferation of phishing URLs and malicious links, this research introduces a groundbreaking approach centered on transfer learning within deep neural networks. By leveraging transfer learning, intricate patterns within URLs and their content are unveiled, culminating in the development of a model seamlessly integrating Bidirectional Long Short-Term Memory (BiLSTM) and Bidirectional Gated Recurrent Unit (BiGRU) networks. These architectures effectively capture sequential dependencies, enhanced by their bidirectional variants accessing both past and future states to comprehend temporal dynamics and improve performance. Through meticulous evaluation and fine-tuning processes, the proposed cybersecurity solution demonstrates robustness and efficacy in defending against evolving threats. This research contributes significantly to advancing the cybersecurity domain, introducing an adaptive strategy that harnesses the strengths of BiLSTM and BiGRU networks within the framework of transfer learning, thus paving the way for more resilient and effective cybersecurity solutions.

Keywords: Deep learning methods, malware, phishing URLs, and cybersecurity.

1. INTRODUCTION

Bad URLs pose grave threats in the digital networks context as they serve as the points of deception as gateways to fraud, cybercracks, and fraud. Such well-thought-out URLs can be used to propagate malware, launch spear-phishing or phishing, as well as contribute to other forms of online fraud. Their menace lies in the fact that they tend to merge thus being hard to notice and more likely to be overlooked. Since the human aspect of cybersecurity is recognized, training is necessary. Security awareness-trained users have a greater capacity to be sensitive to the perilous web of vicious links. Companies can enhance their general susceptibility to the ever-present menace of malicious URLs through the development of a cyber-literacy and wary culture. This will help to make the digital world secure to individuals and enterprises alike.

Fraudulent networks are another fraudulent practice by hackers to exploit individuals and organizations. The links are normally found in what would seem to be harmless emails, messages or webpages in an effort to trick the users out of giving personal data like their login password, bank account, or personal details. Phishing attacks often rely on social engineering methods, where attackers design websites or messages that appear to represent reputable organizations to cause a feeling of urgency and trust.

https://doi.org/10.64909/IJITS.2025.2104

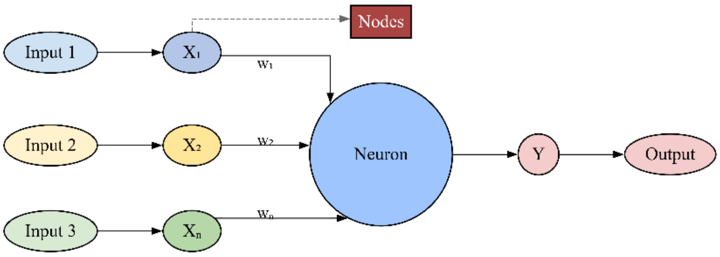

Figure 1: Deep learning Architecture

To counter phishing, users need to be cautious and verify sourcefulness of out-of-the-blue messages or emails prior to following links embedded in them. Firms should use email filters as well as security awareness education to educate users on how to identify and avoid phishing attacks. Another source of defense against these bogus links is online browsers and cybersecurity software that often includes anti-phishing features that can detect and block entry to websites that are classified as dangerous. With cybersecurity, knowledge, and latest technologies will remain crucial elements of safeguarding against the constantly evolving threats like rogue links and phishing.

BIDIRECTIONAL LONG SHORT-TERM MEMORY (BILSTM):

A Bidirectional Long Short-Term Memory (BiLSTM) is a recurrent neural network (RNN) architecture that can be trained to process sequences, including natural language processing and time series. The most important aspect of a BiLSTM is that it is made up of two layers of LSTMs one that takes the input sequence in a forward direction and the other one that takes the input sequence in a backward direction. The forward LSTM works through the sequence of input in forward order form the start to the end whereas the backward LSTM works in reverse order i.e. starting with the end and working towards the start. This is a bi-directional process that enables the BiLSTM to receive the information about the past and future states of the input sequence.

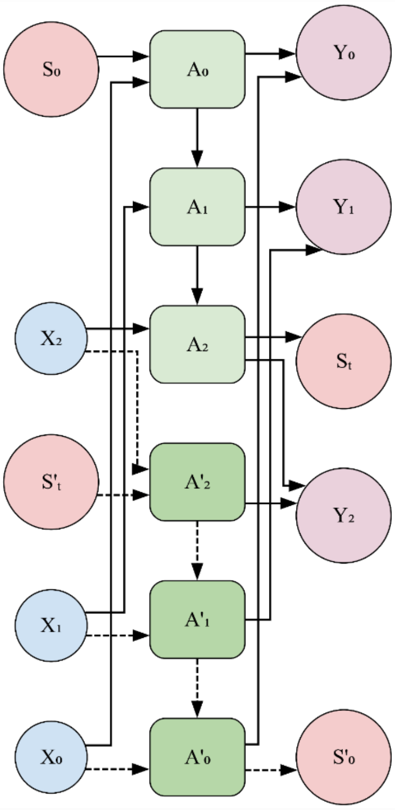

Figure 2: Bi-LSTM Architecture

With two layers of LSTMs that work in reverse directions, a BiLSTM has the effect of augmenting the context that the network has. As an illustration, the forward LSTM is able to know the context of each word, given the words that precede it whereas the backward LSTM is also able to know the context of each word, given the words that follow it. The integration of both directions allows the BiLSTM to have a more detailed insight into the input sequence.

BIGRU (BIDIRECTIONAL GATED RECURRENT UNIT):

BiGRU, also known as bidirectional gated recurrent unit, is a recurrent neural network model that is set up to effectively extract contextual information out of input sequences. The BiGRU model, consisting of two distinct GRU (Gated Recurrent Unit) layers, works with input data in both forward and backward directions. GRU layers process the sequence individually, using gating mechanisms to regulate the flow of information and extract long-range dependencies in the data.

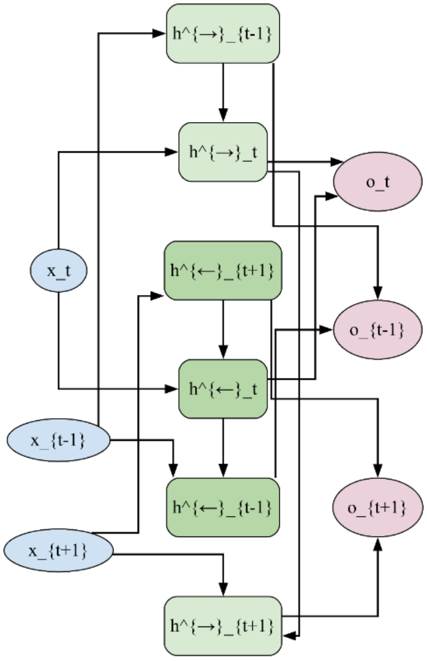

Figure 3: Bi-GRU Architecture

The first GRU layer works sequentially on the input sequence in the forward direction and the second GRU layer works reversely on the input sequence in the reverse direction, working through the input sequence in the reverse order. This two-way processing enables the BiGRU model to access some contextual information of both the previous and future conditions of the input data, which better its comprehension of the dynamics and relationships of the sequence over time.

2. RELATED WORKS

[1] Shantanu, Janet B [1] The study presents a phishing URL and malicious links detection model based on transfer learning, which tackles the most important threats in cybersecurity. The model is capable of capturing complex trends in the structure of URLs, due to the use of deep learning and transfer learning. A curated dataset is highly pre-processed in order to increase the quality of input. To enhance the accuracy, the model combines both soft and hard voting mechanism, whereas feature selection and hyperparameter optimization processes optimize the performance. Detailed assessment measures prove its strength to provide better threat identification. The new solution enhances cybersecurity capabilities by offering a more flexible and effective response to the threat of phishing and other malicious cybersecurity attacks that keep changing. [2] Cho Do Xuan1 , Hoa Dinh NguyeN [2] Malicious URLs are shrewd portals in the complex network of the digital world that are meant to commit fraud, cyber-attack, and scam. Developed with malicious intent, such URLs are extremely dangerous as they can lead to downloads of ransomware, the activation of phishing or spear-phishing activities and the emergence of various types of cybercrime. The fact that they can masquerade, therefore, making them inconspicuous and undetectable, increases the threat they represent to the world of the internet. The threat of malicious URLs will have to be addressed with a complex strategy. The user can also protect himself by taking proactive measures, including not clicking on suspicious links or attaching files on a suspicious email or webpage. In the case of a business, a proactive approach would be to put in place an effective protective system such as using secure email gateways such as ContentCatcher and next generation firewalls which have recent subscriptions in terms of URL filtering. These technological controls are important protection against the entry of malicious URLs. [3] A. Mishr and B. B. Gupta [3] Phishing features referring to specific features of phishing websites are essential in improving the level of cybersecurity. The effectiveness of the inclusion of these attributes is demonstrated by the fact that the suggested method was more effective in a comparison with the techniques that have been based exclusively on blacklists because they were able to identify more phishing sites at the zero-hour point. This feature is especially significant, as this aspect shows the proactive character of the practice, which allows detecting phishing during the initial stages before they can be recognized and blacklisted. The priority to detect a significant number of phishing sites at zero hour will serve as the key in the predictive counteraction of cyber threat, mitigating possible damage, and enhancing the overall cybersecurity resilience. The conventional use of blacklists might be constrained in identifying a new threat fast, and that is why it is important to integrate phishing features to keep abreast with new phishing schemes. [4]

Namrata Singh1 , Nihar Ranjan Roy [4] The first drawback that is related to the complex models such as gradient boosting and the given hybrid LSD model is the possibility of overfitting. When a model is over-adapted to the complexity and noise in the training data, it is said to overfit. Although these models are capable of showing high performance in the training set, they might fail to generalize to real life situations, especially in case of diverse and unfamiliar data. The danger of overfitting is especially high in the case of complex and complicated models. The ability of gradient boosting, e.g., to fit the training data is known to be very high, which may accidentally result in the phenomenon of picking noise or outliers that are not actually patterns of the underlying data distribution. This can lead to poorer performance by the model when they are used on new datasets or new data of unknown instances since the model may have a hard time distinguishing between actual patterns and the noise of the training data. Some of the methods used to mitigate overfitting include regularization methods, cross-validation, and feature selection. Although to some degree, these techniques can be used to reduce overfitting, the threat is still present, and establishing an adequate balance between the complexity of the model and the generalization ability is an ongoing problem of creating effective machine learning architectures. [5] MUZAMMIL AHMED, AHME ALTAMIMI, WILAYAT KHAN, MOHAMMAD ALSAFFAR [5] The issue of overfitting is typical with machine learning, especially when it comes to such complex kinds of models as gradient boosting and the suggested hybrid LSD model. It appears when a model is overly customized to the exact patterns and noise of the training data. Consequently, the model can be highly accurate when it is presented with the data that it has been trained on, but when a new unexplored data of the real-life situation or a different dataset is presented, it can not generalize properly.

ARCHITECTURE DIAGRAM:

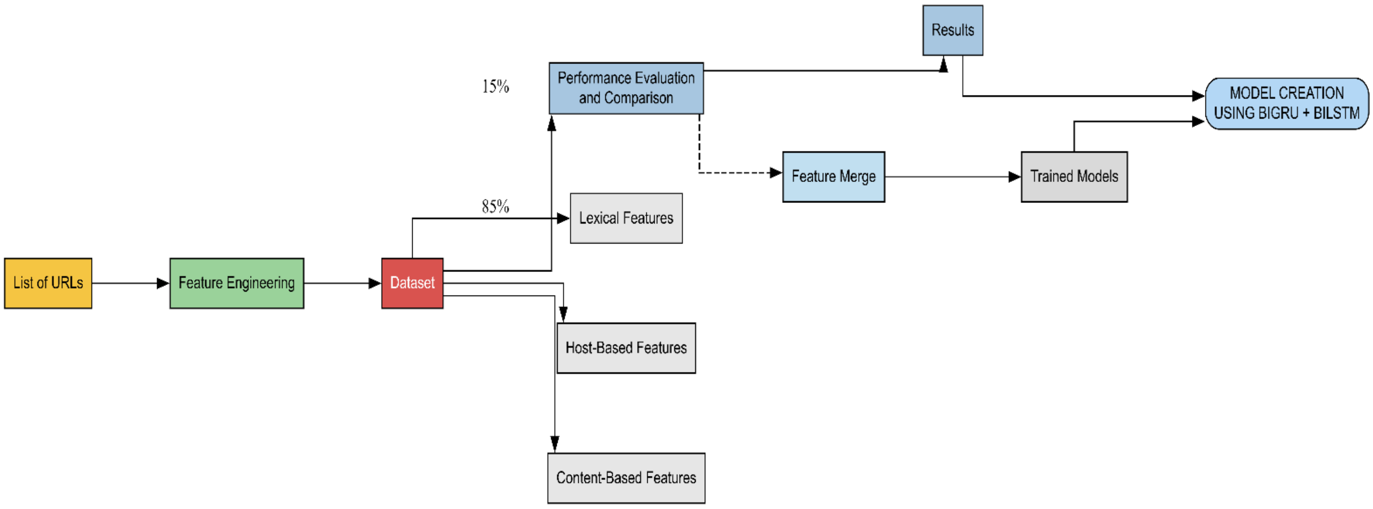

Figure 4: Overall Proposed Model

The fundamental cause of overfitting is in the fact that the model can be specially trained to not only reflect the underlying patterns of the training data, but also reflect the noise, outliers, or random fluctuations peculiar to the training set used. Complex models, by virtue of being such, are better able to learn complex details and nuances, but the increased ability results in the model simply remembering particular examples within the training data instead of being able to learn the underlying patterns. The overfit model can also seek to cooperate with new data by trying to use the same excessive patterns it has observed in the training data, when such patterns were merely local to the noise of that training data. Consequently, the performance of the model becomes poor because it becomes unable to differentiate between true signals and the noise that it has memorized. This non-generalization may compromise the application of the model in the real world where there is the objective of making the right predictions or classifications based on unknown examples. [6] Anjaneya Awasthi and Noopur Goel [6] Modern internet environment is full of vulnerabilities and beginners or careless users are opened to a multitude of threats. Famous individuals take advantage of different tools and methods to steal the personal information of users resulting in gross losses and attacks. Though there has been constant endeavors by the users of the web, software developers and application creators to strengthen the IT infrastructure with the help of encryption, digital signatures and certificates, phishing has continued to pose as a daunting problem. The paper is a narrow approach to tackling the problem of phishing whereby the paper attempts to identify and forecast phishing web address URLs. The analysis is based on the implementation of machine learning classifiers and novel ensemble-based methods on two different datasets and is conducted in three phases. Here, the first one is classification by base classifiers and then ensemble classifiers, and then testing of the ensembles with cross-validation and without cross-validation is done.

The BiLSTM-BiGRU hybrid model architecture of detecting phishing and malicious links is aimed at analyzing the sequence of URLs, extracting meaningful features of URL sequence. It starts with an input layer, at which raw URLs are preprocessed, through readings of text normalization and tokenization. The resulting URLs are then converted into numerical values through word embeddings like Word2Vec or FastText, which enables the model to comprehend the semantic relationships among the various parts of the URL. Then, the model uses a feature extraction layer, which manipulates lexical, host-based and content-based features. This measure will make sure that the model reflects important features that will differentiate between legitimate URLs and phishing or malicious URLs. The features obtained are then forwarded to Bidirectional Long Short-Term Memory (BiLSTM) layer that examines the sequence of URLs both forward and backward. The reciprocity of this model allows it to maintain long-range relationships and comprehend contextual information in the URL structure. After BiLSTM, the Bidirectional Gated Recurrent Unit (BiGRU) layer has much higher computing efficiency with the same sequential learning ability. BiGRU is less parameterized than LSTM, which minimizes the computational burden without affecting accuracy. BiLSTM and BiGRU are used together to enable the model to learn the patterns of complex URLs, which enhances its capability to detect phishing and malicious URLs.The model has a voting mechanism built upon it to improve predictions, using both soft and hard voting methods. Soft voting uses the combination of probability scores of a number of classifiers, whereas hard voting uses the final result of the majority vote. This is a more robust and accurate ensemble learning method of threat detection.

3. PROPOSED SYSTEM

The offered concept is a hybrid BiLSTM-BiGRU model of improved cybersecurity with the aim of detecting phishing and malicious links. Throughout the models, unlike the traditional ones, BiLSTM and BiGRU are effective at capturing the sequential dependencies and temporal patterns in the URLs, which suit the needs of detecting cyber threats. These networks perform bidirectional analysis on URLs, enhancing recognizing patterns and minimizing misclassification. The model uses soft and hard voting mechanisms in order to increase the rate of detection. Soft voting combines probability scores to the multiple classifiers, narrowing predictions, whereas hard voting offers reliability, by choosing the most common classification. This ensemble method enhances strength, stability, and phishing detection. Moreover, the system is able to identify phishing as well as malicious URLs at the same time, which covers several cybersecurity issues. This integrated approach provides a better defence mechanism against the changing cyber threats unlike the traditional method where emphasis is on a single type of threat. This model will guarantee scalable, flexible, and extremely precise cybersecurity solution by exploiting deep-learning as well as ensemble techniques. It can help to identify the manipulations of the URL that are not apparent and, that is why, it is especially helpful in the real-time threat protection of the users against phishing attacks and spammy links in the modern dynamic digital world.

Data collection:

The initial and the most important phase of the process of creating a BiLSTM-BiGRU-based model of detecting phishing and malicious links is data collection. To have effective training and testing of the model, a quality dataset is required. To this end, publicly available datasets on sites like Kaggle, PhishTank, and OpenPhish are consulted. These data sets will include a combination of legal and unwanted URLs with phishing links that may be tailored to steal user credentials. The dataset is selected to have a broad selection of different URL structure, domain, and attack pattern to ensure that the model is trained on real-world cases. Specifics of length of URL, age of the domain, the presence of special characters and embedded redirections are also extracted to offer more information. This dataset is then divided into training, validation and testing sets to help in model development and avoid overfit. In order to improve the quality of the dataset, the methods of data augmentation are employed, and there is an equal proportion of phishing and legitimate URLs. The model is able to propagate more across phishing schemes by gathering large and varied data. The URLs are labeled and verified well to ensure the integrity and reliability of data that the model is being trained on are accurate and unbiased.

PRE-PROCESSING:

It requires pre-processing to clean the dataset obtained and prepare it to be trained in an efficient model. Raw URLs have unnecessary information and, therefore, several steps are undertaken beforehand to enhance the quality of data. Data cleaning is done first to eliminate duplicate URLs, missing values and inconsistency. This measure will make sure that none of the redundant data is a source of bias in the model. A tokenization is then performed, which is the process of splitting URLs into meaningful bits (protocols (HTTP/HTTPS), subdomain, domain name and path).

This assists the model in realizing the structures of URLs. In addition to that, special characters, numbers, and symbols either get removed or changed to special tokens to ensure consistency. Various encoding methods, including one-ht encoding and word embeddings, encode categorical URL elements using feature encoding methods and generate numerical data that can be used to input deep learning networks. In order to guarantee improved model generalization, data balancing methods such as Synthetic Minority Over-sampling Technique (SMOTE) get used to prevent class imbalance. Normalization is also done to bring the numerical features between 0 and 1 to avoid large values being biased. These extensive pre-processing measures will ensure the dataset is well structured and minimized noise and enhanced.

FEATURE EXTRACTION:

The extraction of features is one of the key elements in the training of a proper phishing and malicious URL detection model. The key linguistic and structural characteristics are also extracted instead of using raw URLs only to ensure that the patterns are acquired effectively by the BiLSTM-BiGRU model.

The features extracted are classified into lexical, host-based and content-based features. The lexical features are the length of the URL, the number of dots, the number of hyphens, and the number of entropy and are used to identify the obfuscation techniques of phishing URLs. Host-based features examine the domain age, WHOIS registration information, validation of the SSL certificates and the information on the DNS records and determine the source of the URL as legitimate or suspicious. The content-based features are concerned with redirect chains, embedded links, and frequency of sensitive keywords such as login or verify.

Also, Natural Language Processing (NLP) models like word embeddings (Word2Vec, TF-IDF) transform textual elements of URLs to numeric vectors. This allows deep learning models to infer latent patterns in URLs. The extracted features are subsequently normalized and introduced into the BiLSTM-BiGRU model where it is ensured that it gains knowledge on important attributes between phishing links and legitimate links. Extraction of features contributes to a great extent in identifying the potential of the model to be generalized to various kinds of phishing threats contributing to better detection and soundness.

MODEL CREATION:

BiLSTM-BiGRU hybrid model improves the ability of phishing and malicious links detection by identifying sequential patterns and contextual relationships in URLs. BiLSTM is capable of processing sequences forward and backward, which captures dependencies in a comprehensive manner, and BiGRU is also able to simplify computation through effective gating. The structure consists of an Embedding Layer (turns URLs into numerical vectors), BiLSTM Layer (learns long-range dependencies), BiGRU Layer (enhances feature extraction), Dropout Layer (stops overfitting), Fully Connected Layer (classes URLs), and a Softmax Output Layer (assigns a probability score). The model is more accurate, efficient, and robust by utilizing the combination of BiLSTM and BiGRU to detect phishing threats.

TEST DATA:

The test data step is used to make sure that the model can make generalizations outside the training set. The BiLSTM-BiGRU model is then tested on another group of unseen URLs after training. The data is composed of phishing and legitimate links, which have been labeled with care to make an objective evaluation. The test data is processed by the same pre-processing and feature extraction as the training data before it is fed into the model. This keeps it constant and it makes sure that the model is fed with properly formatted inputs. Important evaluation measures like accuracy, precision, recall, and F1-score can be applied to measure the model performance. Measures of accuracy are the general accuracy of the predictions, whereas the measures of precision and recall are used to determine how the model discriminates between phishing and regular URLs. The F1-score balances precision and recall giving a comprehensive account of the performance. In testing the model is exposed to real-life phishing situation such as advanced phishing attacks such as obfuscated URLs, redirections, and domain spoofing. To prove the superiority of the BiLSTM-BiGRU model over the traditional ones, the results are compared with such classifiers as Random Forest (RF) and Support Vector Machines (SVM). The generalization capacity, the robustness and reliability of the model with regard to identifying phishing threats are evaluated by testing the model on hidden test data.

PREDICTION:

After being trained, the BiLSTM-BiGRU model can forecast phishing and malicious URLs in real-time. A new URL is pre-processed (cleaning, tokenizing), extracted (lexical, host based, content based) and model inferred (analyzing patterns). When the probability predicted exceeds a threshold, the URL is considered as phishing, where it is considered as legitimate. Soft and hard voting mechanisms are used to curb the decision-making process in order to improve reliability. It can be automatically blacklisted when detected phishing links are used as a part of cybersecurity systems. It is an approach to phishing which is fast, automated, and accurate, and it builds up the cybersecurity against the changing threats, as it is a deep learning-based method.

4. RESULTS AND DISCUSSIONS

Performance analysis, in your case, involves a stepwise analysis and evaluation of the constructed cybersecurity models. This process consists of the application of stringent measures to assess various aspects of the functionality of the models. Some of these measurements include accuracy, precision, recall and F1 score as well as area under the receiver operating characteristic (ROC) curve. The study will seek to offer a subtle insight into the effectiveness of the Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN) to identify and neutralize malicious links and phishing web addresses using such expansive evaluation metrics. The performance analysis is an important initial step that will help attest to the resilience and efficacy of the proposed cybersecurity solution. It can help researchers and practitioners to determine the degree to which the model can adapt to the dynamic and constantly changing environment of cyber threats and can give them valuable information concerning its strengths, weaknesses, and potential development. Overall, the performance analysis is important in demonstrating the relevance and feasibility of the developed models in enhancing cybersecurity defenses.

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:

$$\text{Accuracy} = \frac{(\text{TP+TN})}{(\text{TP+TN+FP+FN})} \tag{1}$$

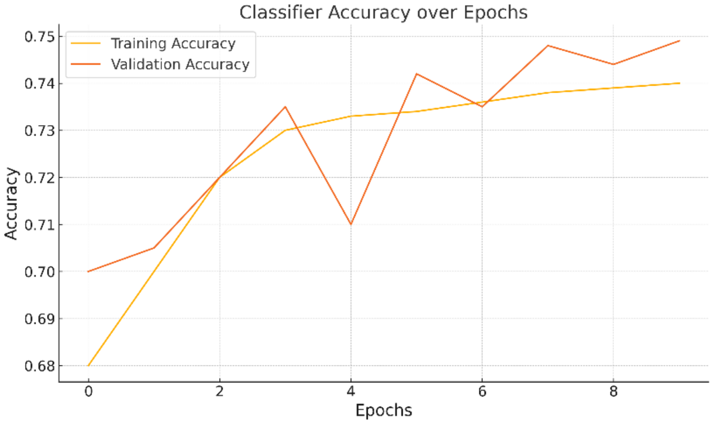

Figure 5: Accuracy Over Epochs

The high value of accuracy shows that the model is effective in separating safe and dangerous links, which increases the security of the cyber-space. Even accuracy might not be enough, however, particularly in skewed datasets such as phishing URLs being much less than safe URLs. Under these circumstances, a predictive model that classifies most of the safe URLs as safe will still have high accuracy yet it will not be able to detect real phishing websites. Thus, the combination of the accuracy with precision, recall, and F1-score give a more broad evaluation. With sequential capabilities of BiLSTM and BiGRU and the voting mechanism, the hybrid model ensures the high accuracy with a balance between false positives and false negatives and her with balance means that the hybrid is a reliable cybersecurity solution.

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:

$$Loss = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \tag{2}$$

Where, y_i represents the actual class label, $\hat{y}_i$ is the predicted probability of the class, N is the total number of instances.

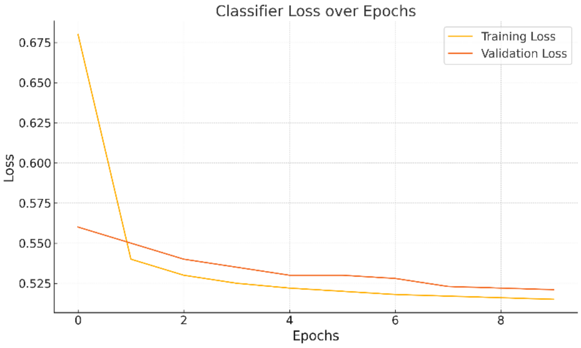

Figure 6: Loss Over Epochs

This loss also acts to discourage incorrect predictions which the model is very confident about thus promoting improved probabilistic predictions. The cross-entropy loss is minimized in the BiLSTM-BiGRU hybrid model which is important in enhancing accuracy. As the two architectures are optimal in handling sequential dependencies, the model is progressively improving its predictions through the addition of weights that make the model less prone to losing. Reduced values of losses imply the closer of the predicted and real labels, which results in the enhanced classification. Nevertheless, when the loss is still large, this can be a sign of overfitting, underfitting, or lack of training data. Such regularization methods as dropout and batch normalization can be used to stabilize the learning process so that the model could be generalized well to the unseen URLs.

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:

$$\text{Precision } = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

Where, TP – Number of correctly identified phishing/malicious URLs, FP- Number of safe URLs incorrectly classified as phishing/malicious.

The value of precision is high and this implies that the model commits fewer false positive errors i.e. it the model has identified most of the phishing/malicious URLs correctly with minimum misclassification of the safe URLs. The opposite is considered low precision; i.e. the model mis-labels a significance number of safe URLs and this will result in unnecessary security alerts. The BiLSTM-BiGRU hybrid model can be optimized to show only real phishing/malicious links, which helps minimize the number of unnecessary warnings and still have a high level of cybersecurity protection. Optimizing the model parameters and decision threshold can assist in balancing the preciseness and other measures such as recall to achieve optimal performance.

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:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

Where, TP – Correctly detected phishing/malicious URLs, FN – 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.

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:

$$\text{F1 Score} = 2 \times \frac{\text{Precision } \times \text{Recall}}{\text{Precison} + \text{Recall}} \tag{5}$$

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.

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.

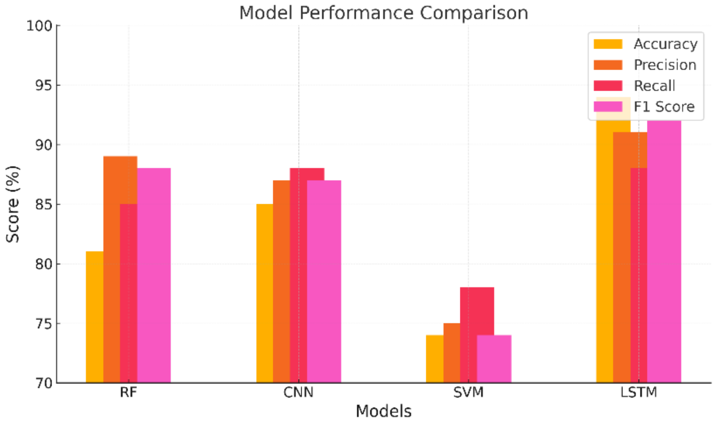

Figure 7: Performance Comparison

Table 1: Performance Evaluation

Model	**Accuracy**	**Precision**	**Recall**	**F1 Score**
RF	81	89	85	88
CNN	85	87	88	87
SVM	74	75	77	74
LSTM	94	91	88	92

CNN demonstrates good generalization capacity especially in the ability to identify important emotional patterns, and only falls behind with an accuracy of 85%. It has a low F1-score (87) though not significantly lower than LSTM though which indicates that it might not be able to capture sequential dependencies as well. RF has an accuracy of 81, which shows good performance although not as high as CNN and LSTM because it cannot analyze temporal features effectively. SVM, on the other hand, is the worst with the lowest accuracy at 74, and weak recall and F1-score. It indicates that SVM is not probably appropriate in complex speech emotion recognition. All in all, LSTM is the most efficient model, as it is the most accurate and has the best balance between precision and recall, thus being the most suitable in the real-world context.

5. CONCLUSION

To summarize, during the period of growing cybercrime, this study presents a strong phishing and malicious URL detection model based on transfer learning and using BiLSTM and BiGRU networks. The model is able to detect the sequential dependences and the time trends, which improves the accuracy of detection as compared to conventional methods. The combination of a sophisticated feature choice and hyperparameter optimization provides the best performance, and the system is flexible enough to address the changing threats. Strict assessment indicators confirm its efficiency, showing enhanced cybersecurity measures. This study will make a contribution to the field because the proposed solution is scalable, intelligent, and adaptive, which opens up the way to better digital security against phishing attacks and malicious links. The further development could be on incorporating the real-time threat intelligence to identify the new phishing URLs in real-time. The model could be improved with the suspicion of ensemble learning on CNNs, Transformers, or Attention Mechanisms to increase the accuracy. Adversarial attack resistance will be developed and will enhance the security against manipulation attempts. Phishing decisions can be made transparent with the help of explainable AI (XAI). The system can be made to be more robust by expanding the system to cross-domain adaptability, multilingual detection, and multimodal analysis.

ACKNOWLEDGEMENT

Not Applicable

Funding

No financial support was provided for the conduct of this research.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

Data Availability Statement

The datasets generated and analyzed during the current study are available from the corresponding author upon reasonable request.

References

[1] Kritika E. A comprehensive literature review on phishing URL detection using deep learning techniques. Journal of Cyber Security Technology. 2024 Jul 15:1-29.

[2] Alsubaei FS, Almazroi AA, Ayub N. Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. IEEE Access. 2024 Jan 9; 12:8373-89.

[3] Reyes-Dorta N, Caballero-Gil P, Rosa-Remedios C. Detection of malicious URLs using machine learning. Wireless Networks. 2024 Mar 6:1-8.

[4] Aljebreen M, Alrayes FS, Aljameel SS, Saeed MK. Political optimization algorithm with a hybrid deep learning assisted malicious URL detection model. Sustainability. 2023 Dec 13;15(24):16811.

[5] https://www.kaggle.com/xwolf12/ malicious-and-benign-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