FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 9, September, 2025, pp 200 – 206
DOI: https://doi.org/10.33003/fjs-2025-0909-4031

DEVELOPMENT OF A TEXT-BASED MODEL FOR DETECTING AND PREVENTING PHISHING ATTACKS USING DEEP LEARNING

***Ayomide Seyi-Ayodele, Sunday Eric Adewumi and Victoria Ifeoluwa Yemi-Peters**

Department of Computer Science, Federal University Lokoja, Kogi State, Nigeria.

*Corresponding authors' email: ayomideseyiayodele@gmail.com

ABSTRACT

Phishing attacks are cyber threats that have persisted over the years, and are often disguised as legitimate messages. Different studies have been focused on the detection of attempted phishing attacks, and significant milestone has been reached. However, previous studies rely mostly on URL-based phishing detection, with machine learning and deep learning models, but limited studies have focused on text-based phishing detection, and adoption of hybrid deep learning and transformer based models. Addressing these gaps, this study focused on the development of a text based phishing detection modes using a hybrid of CNN-LSTM with attention mechanism, and a transformer-based BERT model. Deep learning based models were train separately on a publicly available dataset collected from Kaggle. The dataset was pre-processed and used to train the two models. The model was evaluated using standard evaluation metrics. The experimental result shows that the CNN-LSTM-Attention model outperformed the BERT model across all evaluation metrics used, achieving 92.77% accuracy, 93.00% precision, 92.00% recall, 92.00% F1-score, and 93.00% AUC, while the BERT model had average performance with 76.55% accuracy, 74.00% accuracy, 75.00% precision, 73% recall, 75.00%, F1-scores, and 81.70% AUC. This study was compared with the baseline study that used the K-Nearest Neighbour (KNN) on URL-based features. Our study, CNN-LSTM-Attention model demonstrated superior performance. This study shows that hybrid deep learning with attention mechanism approach is highly effective in the detection of phishing attacks. Future research can focus on exploring multilingual capabilities, integratingbehavioural feature, and real-time model deployment to enhancecyber security.

Keywords: Cyber threats, Deep learning, Machine learning, Models, Phishing attacks

INTRODUCTION

Phishing attacks are cybercrimes that involves deceiving and tricking of people into given out sensitive and personal information, thisinformation could be passwords, credit cards or other personal details (Gallo et al., 2024). Cyber criminals carryout phishing attacks by sending phishing links to the general public through emails, websites, and social media platforms like Twitter, face book, Telegram, Tiktoks etc. These phishing linksappear to be legitimate and are very difficult to detect. During phishing attacks, the attacker gains access to a victim private information, after the victim must have clicked on the phishing link. Once there is a security breach, cyber criminals can execute ransom ware attacks, get unauthorized access to systems and request for ransom for the release of some materials (Etuh et al., 2021). A report by an Anti-Phishing Working Group (APWG, 2024), (Atawneh and Aljehani, 2023) shows that in Q2 2022, there are 1,097,811 phishing assaults, and a total of 1,270,883 phishing assaults in Q3 of 2022.

Technology advancement has made the traditional method of detecting phishing attacks insufficient. The traditional ways of detecting phishing attacks now have several limitations. A limitation to the traditional ways of detecting phishing attacks is its ineffectiveness against zero-day attacks and its lack of timeliness (Geest et al. 2024). Another limitation is that detection models with single-feature extraction can easily be targeted by cybercriminals (Alanezi, 2021). Recent advancement in machine learning technology offers a promising approach to detect phishing attackers faster with more accuracy and precision (Mohamed, 2023). Machine learning models have the ability to analyze large amount of data, learn patters and detect anomalies that indicates phishing attempt (Osemwegie and Amadin, 2023). Deep learning is a subset of machine learning which offers promising solution to the enhancement of phasing detection.

Researchers have applied both machine learning and deeplearning techniques on phishing detection, and they have produce promising result (Prasad and Chandra, 2024). However, recent phishing detection have mostly focused on URL-methods, which analyze links structures, host information, and domain features to detect anomalies and identify phishing links. These method present good result, but fails to detect phishing attempt that are embedded in deceptive textual content, especially when the URLs are masked, and looks legitimate. Due to the continuous evolvement of phishing techniques to language-based manipulation, there is a rising need to shift focus toward text-based detection. The analysis of messages, email content and social media post will allow models to understand the internet more, and will make text-based approaches more adaptable and robust against sophisticated phishing attacks.

To address these gaps, this study presents a text-based phishing detection model, using an hybrid Convolution Neural Network (CNN) and Long-Term-Short-Term Memory (LSTM) with attention mechanism (CNN-LSTM-Attention) to improve performance, and a transformer based mode (BERT). The adoption of these models aims to improve model performance in detecting sophisticated phishing attacks by capturing both semantic context and sequential patterns in phishing messages.

Literature Review

Different researchers have employed different machine learning and deep learning approaches to detect phishing attacks in recent times, these approaches have yielded promising result and have help in the war against phishing attacks over the years. Some of these are reviewed bellow.

Mehndiratta et al. (2023) presented a machine learning-based phishing detection method to detect malicious URLs. The study made used of the K-Nearest Neighbours (KNN)

algorithm and compared the result with other state-of-the-art machine learning models. The experimental result shows that the proposed KNN model was able to achieve 90% accuracy, outperforming all other compared algorithms

Alam et al. (2020) conducted a research that focus on the development of a phishing attack model using machine learning approach. The study utilized the random forest and the decision tree algorithms. The study utilized a dataset collected from Kaggle respiratory, which contain phishing URLs. The result from the experiment shows that the random forest was able to outperform the decision tree, achieving the highest accuracy of 97%.

Saha et al. (2020) conducted a research on the detection of phishing webpage. This study proposed a framework that can be used to detect phishing websites. The designed framework was implemented using webpage dataset collected from Kaggle respiratory. The study used a CNN model to train the dataset. The result shows that the proposed model achieved 95% training accuracy, and 93% testing accuracy.

Aldakheel et al. (2023) carries out a research on the detection of phishing attacks with the use of deep learning model. The CNN algorithm was trained on the PhishTank dataset with URL features. The proposed deep learning based phishing detection model was able to achieve 98.77% accuracy, outperforming all other compared algorithms.

Alshingiti et al. (2023) conducted a study that proposed three different deep learning approaches to the detection of phishing websites. The study presented, a CNN, an LSTM and a hybrid CNN-LSTM models. The proposed algorithms were trained on an open source dataset. The result from the experiment conducted show that the proposed CNN, LSTM, and CNN-LSTM models achieved CNN, LSTM–CNN, and LSTM models achieved 99.2%, 96.8%, and 97.6%, accuracies respectively.

Rashid et al. (2020) proposed a phishing detection technique using a support Vector Machine (SVM) classifier. A standard phishing datasets of the University of California Irvine archive was used to train the proposed model. The result from the experiment shows that the proposed model achieved 95.66% accuracy.

NajwaAltwaijry et al. (2024) carried out a research that presented a one dimensional CNN-based model for phishing detection in emails. The study utilized the Phishing Corpus and Spam Assassin as dataset used to train the model. The result showed that the proposed model achieved accuracy of 99.68%, F1 score of 99.66%, recall of 99.32%, and precision of 100%.

Benavides-Astudillo et al. (2023) developed a deep learning based model that can detect suspicious websites, using the text content of the website and not the URL. The algorithms used include the LSTM, BiLSTM, Gated Recurrent Unit (GRU), and Bidirectional GRU (BiGR U). The proposed algorithm all archive high accuracies of not lea than 96.7%, while the BiGRU achieve the highest accuracy of 97.39%.

Ige et al. (2024) conducted a research that combines LSTM and RF for phishing detection based on image data from videos. The deep-fake videos and images were generated and used as dataset to train the hybrid model. The result from the training shows that the proposed model was able to achieve 98% accuracy, outperforming the compared traditional approaches.

Sultan et al. (2024) conducted a research on the detection of three types of phishing attacks. The types of phishing attacks includes: Tiny URL, Browsers in the Browser, and the regular phishing attacks. The BiLSTM was used to train the URL based dataset. The result from the model training shows that the proposed method was able to achieve 99% precision, recall, and F1 score.

Feng et al. (2020) developed a phishing detection model using three features which are URL, HTML, and Document Object Model (DOM). The study utilized the Stacked Autoencoder (SAE). The result from the experiment shows that the proposed method achieves 90% accuracy, outperforming other compared algorithms,

Jayaraj et al. (2024) carried out a research that focused on the detection of phishing URL using a multi-layer adaptive approach. The study proposed a framework that incorporate two different dataset which are Mendely phishing dataset and Kaggle spam dataset. The framework was implemented and the result shows that the proposed model achieved 98% detection accuracy.

Abed et al. (2023) carried out a research that aims to improve anti-phishing system using URL features. The dataset was curated by collecting phishing and legitimate URL from different sources. The study made use of different machine learning algorithms like decision trees, random forest, and SVM. The result shows that the machine learning algorithms were able to achieve high performance of not less than 88.3% accuracy.

These literature shows evidence of the advancement of phishing detection methods. However, despite this advancement, some gaps still exist in the existing literatures, particularly in the adoption of text-based approach in the detection of phishing emails. We observed that existing study mostly rely on URL-based dataset, with limited focus on text based which is vital in detecting phishing attempt in emails. Also, most existing study rely on machine learning and deep learning model but limited study has been done on hybrid model, or the use of Transformer based model which has proven to be effective in analysing text. To address these gaps, this study proposes a deep learning based hybrid model that combines CNN-LSTM with attention mechanism to improve model performance, and a transformer based mode (BERT) which has proven effective in natural language processing, to detect phishing attempt in email text.

MATERIALS AND METHODS

The method used to achieve the aim of this study follows a unique pattern with different phases. These phases are described below:

Data collection

Dataset used in this study was collected from an open source respiratory (Kaggle). The dataset contain 5000 labeled as legitimate (0) and phishing (1), which was designed for phishing binary classification. The sample of the dataset is presented in Figure1.

	text	label
2	Security alert: Unauthorized login attempt. Confirm your identity https://secure-login.com.	1
3	Urgent: Your payment was declined. Update details here: https://update-info.com.	1
4	Dear user, your account will be suspended unless you verify it https://update-info.com.	1
5	You've won a prize! Click https://update-info.com to claim it now.	1
6	Security alert: Unauthorized login attempt. Confirm your identity https://secure-login.com.	1
7	Get your refund by submitting your details now at https://claim-now.com.	0
8	Dear user, your account will be suspended unless you verify it https://secure-login.com.	1
9	Dear user, your account will be suspended unless you verify it https://claim-now.com.	1
10	You've won a prize! Click https://secure-login.com to claim it now.	1
11	Security alert: Unauthorized login attempt. Confirm your identity https://update-info.com.	1
12	Dear user, your account will be suspended unless you verify it https://update-info.com.	1
13	Security alert: Unauthorized login attempt. Confirm your identity https://secure-login.com.	1
14	Security alert: Unauthorized login attempt. Confirm your identity https://secure-login.com.	1
15	You've won a prize! Click https://secure-login.com to claim it now.	1
16	New company policy updates available on the intranet.	0
17	Don't forget to complete your timesheet by Friday.	0
18	Get your refund by submitting your details now at https://update-info.com.	1
19	New company policy updates available on the intranet.	0
20	Urgent: Your payment was declined. Update details here: https://update-info.com.	1
21	Urgent: Your payment was declined. Update details here: https://claim-now.com.	1
22	Security alert: Unauthorized login attempt. Confirm your identity https://claim-now.com.	1
23	Don't forget to complete your timesheet by Friday.	0
24	Security alert: Unauthorized login attempt. Confirm your identity https://update-info.com.	1
25	You've won a prize! Click https://update-info.com to claim it now.	1

Text_phishing_dataset2

Figure 1: Dataset Sample

Data Preprocessing

During the data preprocessing phase, we first clean the collected dataset by removing irrelevant entries like duplications and noise from the dataset. This is done to improve the quality of the dataset. After the cleaning of the dataset, other text preprocessing task that was done includes the conversion of all text to lowercase, removing punctuations and removing common stop words. We further generate frequency distribution with 20 most frequent words during exploratory analysis an shown in Figure 2, and the word cloud of frequent words shown in Figure 3. The class distribution is displayed in Figure 4, which shows that the class distribution is slightly imbalance. The class imbalance was addressed by computing class weights that was applied during the model training.

For CNN-LSTM-Attention model, the cleaned dataset was further tokenized and converted into numerical sequence, which were padded to a fixed length to create a shape that is uniform and compactable with deep learning layers. While for BERT model, we utilized the BERT tokenizer in the conversion of text into tokens, and corresponding attention mask was generated to enable model to focus on the important parts of the input during the model training.

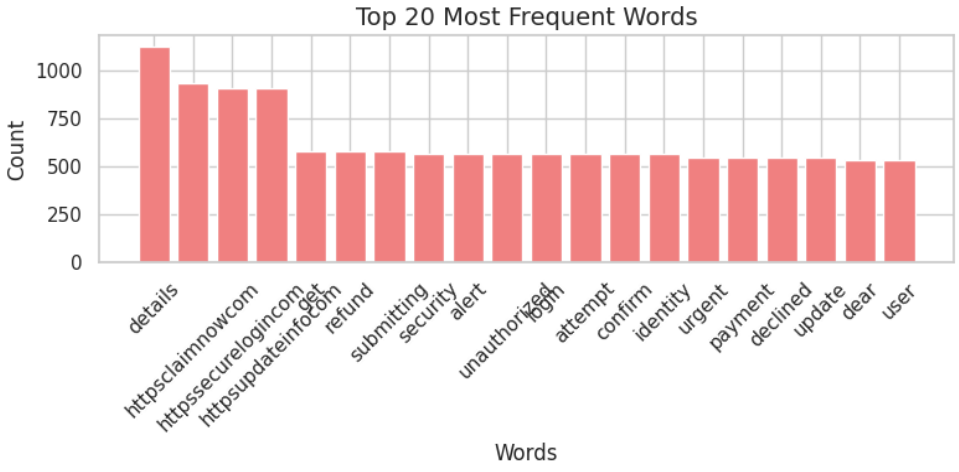

Figure 2: Top 20 Most Frequent Words

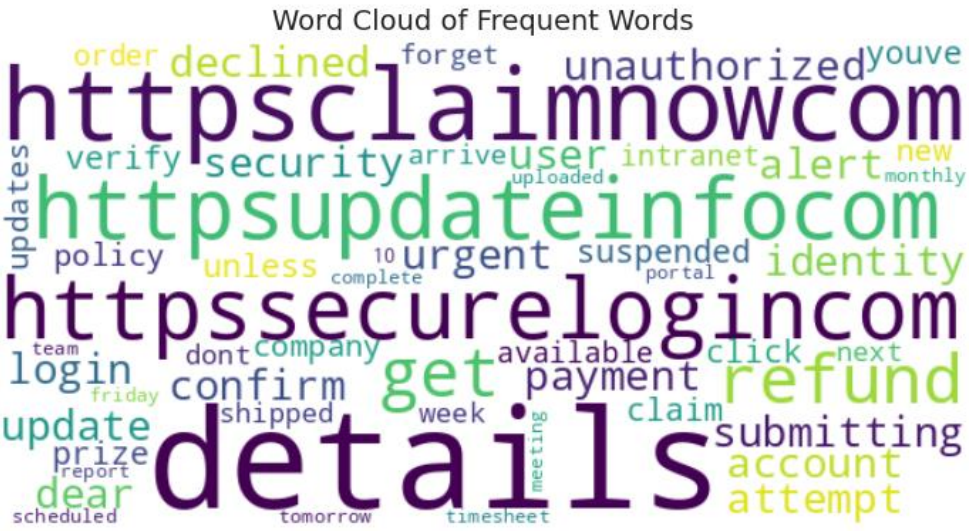

Figure 3: Word Cloud of Frequent Words

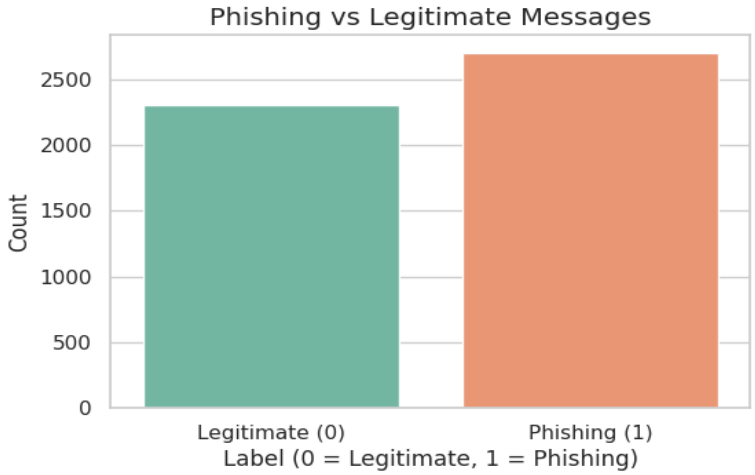

Figure 4: The Class Distribution of Phishing Versus Legitimate Messages

Model Development

The CNN-LSTM-Attention and the BERT models were both developed to detect phishing attempt in email. We used a layered architecture that is composed of convolution layers, LSTMs and an attention mechanism implemented with a dense layer for the CNN-LSTM-Attention. In a similar way, the BERT was fine-tuned with the use of a classification head built on top of the pre-trained BERT base. The model summary for the CNN-LSTM-Attention and the BERT is presented in figure 5 and Figure 6 respectively.

Model: "functional_1"

Layer (type)	Output Shape	Param #
input_layer_1 (InputLayer)	(None, 100)	0
embedding_1 (Embedding)	(None, 100, 128)	1,280,000
conv1d_1 (Conv1D)	(None, 96, 64)	41,024
lstm_1 (LSTM)	(None, 96, 64)	33,024
attention_layer_1 (AttentionLayer)	(None, 64)	160
dropout_1 (Dropout)	(None, 64)	0
dense_1 (Dense)	(None, 1)	65

Total params: 1,354,273 (5.17 MB)
Trainable params: 1,354,273 (5.17 MB)
Non-trainable params: 0 (0.00 B)

Figure 5: CNN-LSTM-Attention Model Summary

Model: "functional_1"

Layer (type)	Output Shape	Param #	Connected to
input_ids (InputLayer)	(None, 100)	0	-
attention_mask (InputLayer)	(None, 100)	0	-
tf_bert_layer_1 (TFBertLayer)	(None, 768)	0	input_ids[0][0], attention_mask[0…
dense_1 (Dense)	(None, 1)	769	tf_bert_layer_1[…

Total params: 769 (3.00 KB)
Trainable params: 769 (3.00 KB)
Non-trainable params: 0 (0.00 B)

Figure 6: BERT Model Summary

Model Training

The CNN-LSTM-Attention and the BERT models were both trained on the proposed dataset. Both model was trained over 10 eparches. The training process for the CNN-LSTM-Attention and the BERT models are shown in Figure 7 and Figure 8 respectively.

```
Epoch 1/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 8s 76ms/step - accuracy: 0.9157 - loss: 0.2985 - val_accuracy: 0.9025 - val_loss: 0.3273
Epoch 2/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 19s 159ms/step - accuracy: 0.9305 - loss: 0.2617 - val_accuracy: 0.9025 - val_loss: 0.3207
Epoch 3/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 13s 134ms/step - accuracy: 0.9325 - loss: 0.2552 - val_accuracy: 0.9025 - val_loss: 0.3204
Epoch 4/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 9s 90ms/step - accuracy: 0.9146 - loss: 0.2976 - val_accuracy: 0.9025 - val_loss: 0.3361
Epoch 5/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 7s 73ms/step - accuracy: 0.9303 - loss: 0.2618 - val_accuracy: 0.9025 - val_loss: 0.3208
Epoch 6/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 9s 88ms/step - accuracy: 0.9214 - loss: 0.2780 - val_accuracy: 0.9025 - val_loss: 0.3214
Epoch 7/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 8s 83ms/step - accuracy: 0.9221 - loss: 0.2836 - val_accuracy: 0.9025 - val_loss: 0.3227
Epoch 8/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 9s 71ms/step - accuracy: 0.9179 - loss: 0.2931 - val_accuracy: 0.9025 - val_loss: 0.3258
Epoch 9/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 9s 91ms/step - accuracy: 0.9199 - loss: 0.2864 - val_accuracy: 0.9025 - val_loss: 0.3237
Epoch 10/10
100/100 ━━━━━━━━━━━━━━━━━━━━ 7s 71ms/step - accuracy: 0.9277 - loss: 0.2658 - val_accuracy: 0.9025 - val_loss: 0.3211
```

Figure 7: CNN-LSTM-Attention Learning Progress

```
Epoch 1/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 31s 126ms/step - accuracy: 0.6784 - loss: 0.6509 - val_accuracy: 0.6640 - val_loss: 0.6545
Epoch 2/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 35s 102ms/step - accuracy: 0.6742 - loss: 0.6416 - val_accuracy: 0.6640 - val_loss: 0.6456
Epoch 3/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 41s 103ms/step - accuracy: 0.6697 - loss: 0.6324 - val_accuracy: 0.6640 - val_loss: 0.6377
Epoch 4/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 26s 103ms/step - accuracy: 0.6773 - loss: 0.6221 - val_accuracy: 0.6640 - val_loss: 0.6304
Epoch 5/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 25s 102ms/step - accuracy: 0.6773 - loss: 0.6161 - val_accuracy: 0.6640 - val_loss: 0.6230
Epoch 6/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 46s 123ms/step - accuracy: 0.6558 - loss: 0.6146 - val_accuracy: 0.6640 - val_loss: 0.6163
Epoch 7/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 36s 103ms/step - accuracy: 0.6784 - loss: 0.5965 - val_accuracy: 0.7420 - val_loss: 0.6108
Epoch 8/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 46s 123ms/step - accuracy: 0.7356 - loss: 0.5904 - val_accuracy: 0.6640 - val_loss: 0.6033
Epoch 9/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 36s 103ms/step - accuracy: 0.7579 - loss: 0.5783 - val_accuracy: 0.7420 - val_loss: 0.5988
Epoch 10/10
250/250 ━━━━━━━━━━━━━━━━━━━━ 26s 102ms/step - accuracy: 0.7655 - loss: 0.5754 - val_accuracy: 0.7420 - val_loss: 0.5913
<keras.src.callbacks.history.History at 0x7a8d540fbe10>
```

Figure 8: BERT Learning Progress

Performance Evaluation

After the model training, the model performance was further evaluated based on accuracy, precision, recall, F1-scores, And AUC-curve. Bothe modes were evaluated individually with the use of these evaluation metrics, providing insight on the effectiveness of the proposed phishing detection models. The ROC curve for the CNN-LSTM-Attention and BERT models are presented in Figure 9 and Figure 10 respectively.

The ROC curve of the BERT model presented in figure 9 shows that the model achieves an AUC value of 0.817, indicating a fair classification performance. As seen in the figure we observed that the curve rises above the random guess line, without maintaining any steep climb towards the top-left corner, this reflect a moderate discriminatory power between phishing and legitimate emails. This ROC result shows that the BERT model is able to detect phishing attempts with some reliability but underperformed compared to the hybrid CNN-LSTM-Attention model.

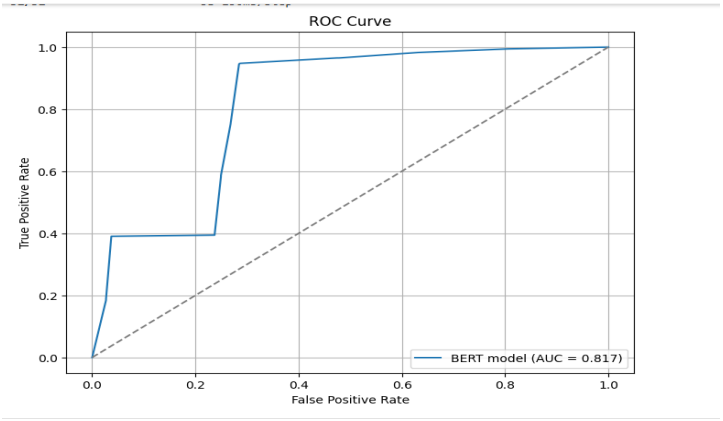

Figure 9: ROC Curves for BERT

Figure 9 present the ROC curve for the CNN-LSTM-Attention model, which outperformed the compared BERT model with a superior performance of AUC value of 0.93. as shown in the image, we observed that the curve sharply rises toward the top-left corner, which shows a strong ability to differentiate phishing from legitimate emails. This shows that the hybrid deep learning approach is more effective as compared to the pre-trained BERT approach The robust classification power reflected in the ROC curve validates the strength of combining CNN, LSTM, and attention mechanisms for phishing detection.

RESULTS AND DISCUSSION

Experimental Results

The experimental result of the proposed models is presented in Table1. The table reflects the effectiveness of both the CNN-LSTM-Attention model and the BERT mode, in terms of accuracy, precision, recall, F1-Scores, and AUC-values.

Table 1: Performance Comparison of CNN-LSTM-Attention and BERT Models

Metric	CNN-LSTM-Attention Model	BERT Model
Accuracy	92.77%	76.55%
Precision	93.00%	74.00%
Recall	92.00%	73.00%
F1-Score	92.00%	75.00%
AUC Score	93.00%	81.70%

From the experimental result, we observed that the CNN-LSTM-Attention model outperform the BERT model across all the five evaluation metrics used. The superior performance of the hybrid deep learning model indicates that the hybrid deep learning model was more reliable when used for text based phishing classification. The BERT model on the other hands, underperform in most of the evaluation metrics used, but has its highest performance of 81.70% AUC-values. These slightly higher AUC indicate that the BERT model has a better capability to distinguish between classes across different decision thresholds, which may be due to the model's deep contextual understanding despite its low performance. This result indicates that the CNN-LSTN-Attention model is more effective in the classification of text based phishing attempt in real-world scenario.

Comparative Analysis with the Baseline Paper

The study result was further compared with the baseline paper (Mehndiratta et al. 2023),who developed a phishing detection model using KNN and a malicious URL features. Mehndiratta et al. (2023) study shows that the KNN model developed achieved 90% precision when used to classify phishing URLs. Table 2 shows the summary of the comparison of this study with (Mehndiratta et al. 2023)'s study.

Table 2: Comparison of Key Results with the Baseline Paper

Study	Precision	Detection Type	Approach
Mehndiratta et al. (2023) (baseline paper)	90%	URLs-based phishing	Machine Learning
CNN-LSTM-Attention (This Study)	93%	Text-based phishing	Hybrid Deep Learning with Attention Mechanism
BERT Model (This Study)	74%	Text-based phishing	Transformer-based (BERT)

Improvements

When comparing this study with the baseline paper, it was observed that the study's CNN-LSTM-Attention model was able to outperform the benchmarked KNN model interms of precision. The CNN-LSTM-Attention model was able to achieve the highest precision of 93%, while the benchmarks KNN model achieved 90% precision, indicating the hybrid model superior performance. Also the benchmarked paper utilized the URLs, while this study focused on textual message, which offers complementary detection strategy that enhances model's robustness, especially for phishing attempts embedded in text bodies rather than URLs. The CNN-LSTM-Attention model also achieved high performance when evaluate with other evaluation metrics with F1-score (92.00%) and accuracy (92.77%), this shows the model's robustness across all evaluation metrics used.

CONCLUSION

This study focused on email text-based phishing attempt detection model using an hybrid of CNN-LSTM-Attention

and a pre-trained BERT model. The models were trained on a public dataset and the result was evaluated using evaluation metrics like accuracy, precision, recall, f1-scores and AUC. The result from this study shows how effective deep learning is, in text-base phishing detection. Although the two models show good performance, but the CNN-LSTM-Attention model outperform the BERT model across all the evaluation metrics used, achieving 92.77% accuracy, 93.00% precision, 92.00% recall, 92.00% F1-scores, and 93% AUC, while the BERT model had average performance with 76.55% accuracy, 74.00% accuracy, 75.00% precision, 73% recall, 75.00%, F1-scores, and 81.70% AUC. The ability of the CNN-LSTM-Attention model's to capture local features and sequential dependencies in this study make it suitable for detecting deceptive textual patterns. This study compares its result with the baseline paper which focused on URL-based features, while this study address a more nuanced challenge and expands the understanding of text-based phishing detection in email. This study provides scalable solution of cyber security applications in real-world setting. Future studies can focus on model deployment, multilingual support, and the integration of user behavior features to enhance phishing detection systems.

REFERENCES

Abed, L. H., Mohammed, H. J., & Yaseen, Y. S. (2023). Phishing identification through up-to-date features generation and exploration. *International Journal on Technical and Physical Problems of Engineering*, *15*(3).

Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R.-E. -, & Hossain, S. (2020). Phishing attacks detection using machine learning approach. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 1173–1179. https://doi.org/10.1109/icssit48917.2020.9214225

Alanezi, M. (2021). Phishing detection methods: a review. *Technium: Romanian Journal of Applied Sciences and Technology*, *3*(9), 19–35. https://doi.org/10.47577/technium.v3i9.4973

Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. A. (2023). A deep learning-based innovative technique for phishing detection in modern security with uniform resource Locators. *Sensors*, *23*(9), 4403. https://doi.org/10.3390/s23094403

Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. *Electronics*, *12*(1), 232. https://doi.org/10.3390/electronics12010232

APWG. (2024). Phishing activity trends report. Phishers combining tactics and resources in attacks. https://docs.apwg.org/reports/apwg_trends_report_q2_2024

Atawneh, S., &Aljehani, H. (2023). Phishing email detection model using deep learning. *Electronics*, *12*(20), 4261. https://doi.org/10.3390/electronics12204261

Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Nuñez-Agurto, D., & Rodríguez-Galán, G. (2023). A phishing-attack-detection model using natural language processing and deep learning. *Applied Sciences*, *13*(9), 5275. https://doi.org/10.3390/app13095275

Etuh, E., S. Bakpo, F., & A.H, E. (2021). *Social Media Network Attacks and their Preventive Mechanisms: A Review*. https://doi.org/10.5121/csit.2021.112405

Feng, J., Zou, L., Ye, O., & Han, J. (2020). Web2Vec: Phishing Webpage Detection Method Based on Multidimensional Features Driven by Deep Learning. *IEEE Access*, *8*, 221214–221224. https://doi.org/10.1109/access.2020.3043188

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., &Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers and Security*, *139*. https://doi.org/10.1016/j.cose.2023.103671

Geest, R. J., Cascavilla, G., Hulstijn, J., & Zannone, N. (2024). The applicability of a hybrid framework for automated phishing detection. *Computers & Security*, *139*, 103736. https://doi.org/10.1016/j.cose.2024.103736

Ige, T., Kiekintveld, C., &Piplai, A. (2024). Deep learning-based speech and vision synthesis to improve phishing attack detection through a multi-layer adaptive framework. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.17249

Jayaraj, R., Pushpalatha, A., Sangeetha, K., Kamaleshwar, T., Udhaya Shree, S., & Damodaran, D. (2024). Intrusion detection based on phishing detection with machine learning. *Measurement: Sensors*, *31*, 101003. https://doi.org/10.1016/j.measen.2023.101003

Mehndiratta, M., Jain, N., Malhotra, A., Gupta, I., & Narula, R. (2023). Malicious URL: Analysis and Detection using Machine Learning. *Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023*.

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2). https://doi.org/10.1080/23311916.2023.2272358

NajwaAltwaijry, Isra Al-Turaiki, Alotaibi, R., &Alakeel, F. (2024). Advancing phishing email detection: a comparative study of deep learning models. *Sensors*, *24*(7), 2077–2077. https://doi.org/10.3390/s24072077

Osemwegie, E. E., & Amadin, F. I. (2023). Student dropout prediction using machine learning. *FUDMA Journal of Sciences, 7*(6), 347–353. https://doi.org/10.33003/fjs-2023-0706-2103

Prasad, A., & Chandra, S. (2024). PhiUSIIL: A diverse security profile empowered phishing URL detection framework based on similarity index and incremental learning. *Computers and Security*, *136*. https://doi.org/10.1016/j.cose.2023.103545

Rashid, J., Mahmood, T., Nisar, M. W., & Nazir, T. (2020). *Phishing Detection Using Machine Learning Technique*. IEEE Xplore. https://doi.org/10.1109/SMART-TECH49988.2020.00026

Saha, I., Sarma, D., Chakma, R. J., Alam, M. N., Sultana, A., & Hossain, S. (2020). *Phishing Attacks Detection using Deep Learning Approach*. IEEE Xplore. https://doi.org/10.1109/ICSSIT48917.2020.9214132

Sultan Asiri, Xiao, Y., Alzahrani, S., & Li, T. (2024). PhishingRTDS: A Real-time Detection System for Phishing Attacks Using a Deep Learning Model. *Computers & Security*, *141*, 103843–103843. https://doi.org/10.1016/j.cose.2024.103843