International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 13 Issue 02 February 2026

An Intelligent Hybrid Framework for Phishing Email Detection Using Machine Learning and Deep Learning Techniques

Monika Dhanak[1], Mohit Jain[2]
Research Scholar[1], HOD CSE[2]
BM College of Technology, Indore (M.P.), India[1, 2]
monikadhanak652@gmail.com[1], bmctmohitcs@gmail.com[2]

Abstract: *Phishing emails are still a major menace in online communication in that they manipulate the users with misleading information and therefore, proper and correct detection systems are required. The proposed research is a hybrid phishing email detection system comprising of machine learning and deep learning to classify emails as either phishing or legitimate. The system takes a phishing email dataset, which is distributed in either CSV format or XLSX format and manipulates it with Python-based data handling libraries. Originally, the appropriate features are chosen and pre-processed to address missing values and label encoding are carried out. A thorough text pre-processing is thereafter done with Natural Language Processing (NLP) processes, such as removal of stop-words, punctuation, special characters, stemming, lower-casing, tokenization and padding, to provide clean and structured input text. The processed data is separated into training and testing data sets when learning and testing the model. Count Vectorization is used as a method to perform feature extraction to convert textual data into numerical feature vectors. These feature vectors are simultaneously inputted into various classifiers, which include CNN-1D, Multi-Layer Perceptron (MLP), Bidirectional Long Short-Term Memory (BiLSTM), and Inception-based neural networks, each encoding different lexical, contextual and multi-scale patterns in email text. The single model results are synthesized by a decision fusion tactic to get the ultimate categorization. The performance of the system is measured with traditional measures like accuracy, precision, recall, F1-score, and error rate with the relative results displayed in graphical-based visualizations. The suggested framework follows an offline, non-real time setting where a GUI interface is used and can therefore be used in academic testing and performance analysis. The hybrid architecture is shown to be more robust and detective than single-model ones.*

Keywords: *Phishing Email Detection; Cybersecurity; Machine Learning; Deep Learning; Hybrid Detection Framework, Natural Language Processing (NLP), Multi-Layer Perceptron (MLP); Email Classification.*

1. INTRODUCTION

E-mail has emerged as one of the most popular and necessary forms of communication to be used by individuals, organizations, and businesses worldwide in the era of the internet. Nevertheless, in the same way that email has made communication convenient and accessible, it has also become one of the main subjects of cybercriminal acts, namely phishing. Phishing emails are emails that are communicated by bad people to make people provide a disclosure of personal information such as usernames, passwords, banking details or any other personal details. To take advantage of human trust and psychological vulnerability to these emails, they frequently pose as reputable institutions (e.g. banks, governmental bodies, or widespread online services). As phishing methods become more and more sophisticated, it has become clear that legacy rule-based and signature-based detection systems cannot effectively detect new highly customized phishing attacks [1].

Such attacks as phishing are extremely poor in terms of cyber security as they may result in losing extensive sums of money, data breaches, identity theft, and PR issues. According to the world cyber security research, malware and ransom are primarily distributed with the help of phishing. Phishing also constitutes a large portion of social engineering attacks in the world. Daily spam filters and blacklists are struggling more due to the fact that the phishing campaigns can be easily initiated and that there are black phishing kits and auto-tools available in the dark web [2].

In addition, the use of sophisticated obfuscations, URL redirection and employment of legitimate-appearing domain names also make the detection task harder. To resolve these disputes, scientists and cyber security experts have resorted more to ML and DL based solutions to detect phishing emails. These intelligent systems use statistical characteristics, text, header information, embedded links and metadata to identify legitimate email messages and spam email messages. In contrast to a fixed system that is based on rules, ML and DL models have learning and adaptation capabilities based on the changing pattern of phishing, which allows them to detect phishing dynamically and more accurately. NLP and other techniques are also being incorporated to understand the linguistic and semantic characteristics of email content to assist the model to convey subtle manipulations in tone, grammar and context that could be used to signify that the email is phishing [3].

Recent advancements have seen the emergence of hybrid detection frameworks, which combine multiple models and feature extraction methods to enhance performance and reduce false positives. For instance, integrating Convolution Neural Networks (CNNs) for URL feature analysis, LSTM networks for text sequence learning, and ensemble models like Random Forest or XGBoost for final classification has shown promising results in improving accuracy and robustness. Additionally, leveraging large-scale email datasets and real-time threat intelligence feeds has further strengthened the detection capabilities of such systems.p-6].

2. LITERATURE REVIEW

The Internet is a global wide-area network that offers users and firms an inventive way of connecting with each other. This has prompted a change in people's lifestyles; for instance, online shopping and online education have started to substitute provisional stores and educational institutes. Widespread security concerns around the world were caused by the unlimited, highly-skilled World Wide Web, which held a lot of information. According to [7] many data breaches have been revealed by advanced top security companies up to now, and users' accounts are still being hacked. Many of these things that have been happening recently are due to progress in technology. This affords criminals an opportunity to debut new-fangled categories of crime using computers and networks, known as cybercrimes. Every single one of the cyber security risks that are comprised of several phases of attacks has the intention of achieving a particular objective. Intruders are able to circumvent preexisting security systems and gain a significant amount of access to the target network or systems as a result of the sophistication of these attacks[8]In the modern era, accessing cloud storage and hosting data can also result in severe cyber security attacks [9] These attacks can include data breaches, compromised credentials, Denial of Service (DoS) attacks, hacked interfaces and Application Programming Interfaces (APIs), permanent data loss, and other similar incidents.

3. PROPOSED SYSTEM AND RESULT DISCUSSION

The phishing email detector system proposed is supposed to detect phishing and legitimate emails with proper accuracy and relies on machine learning and deep learning functions. The system is fed with a phishing email dataset (CSV or XLSX format) that was gathered in a regular data repository and processed using python-based data handling libraries. First, pertinent data is selected and pre-processed to eliminate missing values and carry out label encoding. This is then followed by thorough pre-processing of text through Natural Language Processing (NLP) models like stop-word removal, punctuation and special characters renovations, stemming and lowercasing, tokenization and padding to come up with clean and structured textual input. The data obtained is then divided into training and testing data to evaluate and predict the model. Count Vectorization is a method of vectorization performed to achieve the feature extraction of texts to transform them into numerical data. The classification step utilizes several machine and deep learning models that include CNN-1D, MLP, BiLSTM, and Inception models to categorize emails as either phishing and non-phishing. The system assesses performance based on the traditional performance metrics of accuracy, precision, recall, F1-score, and error rate and displays comparative results in graphical visualizations. The whole procedure is carried out offline in a non-real-time setting using a graphical user interface, and the data is supplied internally to be utilized in an experimental and academic scenario.

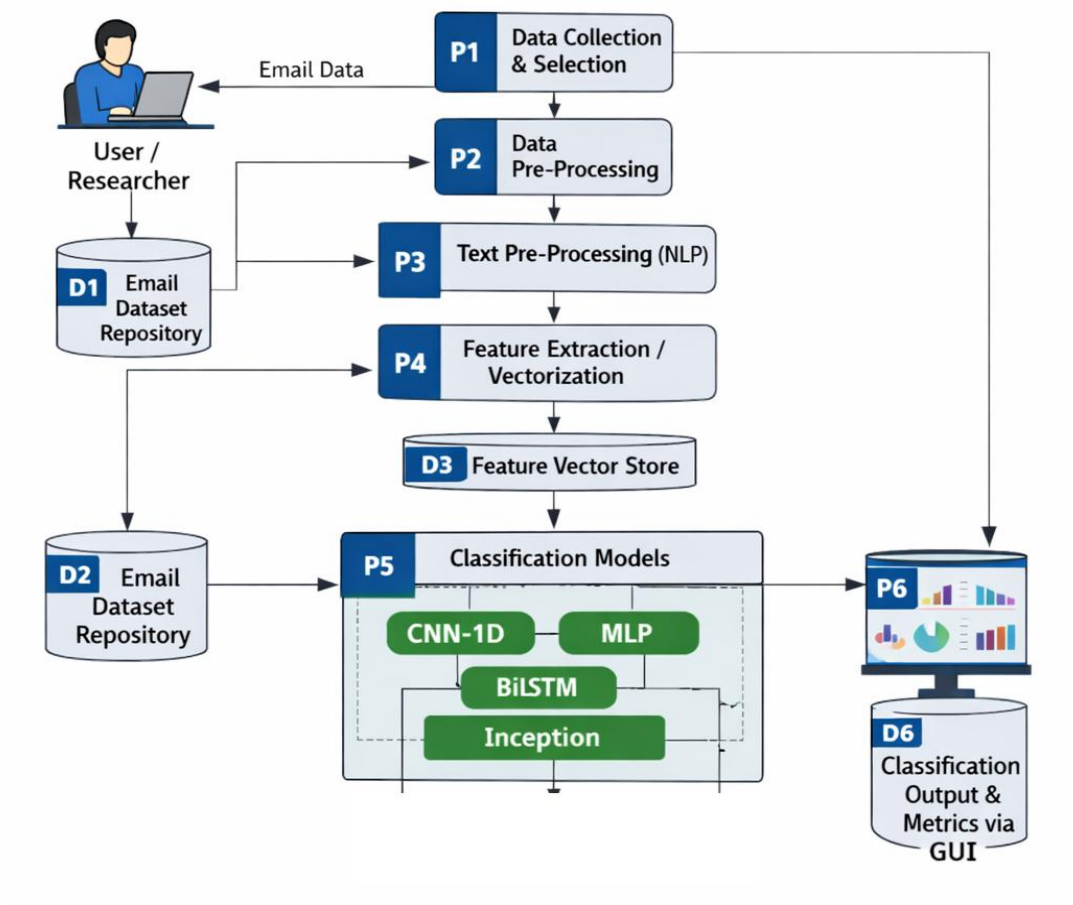

Figure 1: proposed system architecture

Dataset Description

The proposed phishing email detection system is also trained and evaluated with the help of the Phishing_Email.csv dataset (52.03 MB). The dataset will include three columns and it will be based on two parameters which are the Email Text and Email Type. Email Text attribute stores the entire body content of emails, which is raw textual information to be used in extracting features and classifying emails. Email Type attribute is the target label and this is based on whether an email was a Phishing Email or a Safe Email. The data is well organized, and there are no cases of nulls with about 3 percent of blank cells, which guarantees the reliability of data to be used in the experiment. There is a realistic balance with regards to the amount of class distribution with the emails being about 61 percent Safe Emails and 39 percent Phishing Emails. The values of the label fall in equal values within several ranges, each of which has the number of records about 932933, and this makes a total of approximately 18600 email cases. This dataset has a great volume, variety, and balance to train, test, and compare various machine learning and deep learning models to detect phishing emails in an offline and experimental setting.

Mathematical Representation of the Hybrid Algorithm
Let the phishing email dataset be represented as:

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

Where
x_i = email text of the i^{th} email
$y_i \in \{0,1\}$ = class label
0→Safe Email, 1→Phishing Email
Text Pre-processing and Vectorization

After NLP pre-processing, each email text is transformed into a numerical feature vector:
$v_i=\phi(x_i)$
Where
$\phi(\cdot)$ represents the vectorization function (Count Vectorizer).

Text Pre-processing and Vectorization
After NLP pre-processing, each email text is transformed into a numerical feature vector:
$v_i = \phi(xi)$
where
$\phi(\cdot)$ represents the vectorization function (Count Vectorizer)

Model-wise Prediction
The feature vector v_i is fed into multiple classifiers:
$p_i = f_{CNN}(v_i)$
$p_i= f_{MLP(}v_i)$
$p_i= f_{BiLSTM}(v_i)$
$p_i = f_{Inception(}v_i)$

The suggested system is the only architecture that combines several deep learning models such as CNN-1D, MLP, BiLSTM, and Inception allowing to learn the local pattern, regional dependencies, non-linear relationships, and multi-scale textual attributes to better detect phishing.

The system uses a large pre-processing and vectorization pipeline of NLP, unlike traditional ones that have a little text cleaning, so the textual representations before classification are noise-free and standardized and rich in information.

The framework facilitates parallel training and assessment of several classifiers with standard datasets and measures to facilitate objective performance comparison and sound model validation, facilitating interpretation, reproducibility and successful experimental analysis, thus suitable to research and instructional purposes, not black-box. Modules Description

The research article is based on an experiment research design. The method of supervised learning is applied where the labeled phishing email data is utilized to train and test various classification models. The study aims at comparing and contrasting the performance of individual and hybrid deep learning models in detection of phishing emails.

Dataset Description

Data set in this study is the Phishing_Email.csv data, which was retrieved in a conventional warehousing of data. The dataset will contain text data of email body and associated labels of the email being Phishing or safe. The data is delivered in CSV/XLSX format and is used solely on academic and experimental purposes in off-line setting.

Implementation Model
The implementation model works in a systematic pipeline which includes data input, pre-processing, feature extraction, classification and evaluation. The general architecture is represented by the context diagram and detailed process flow, which guarantees the modular and scalable system design.

Data Collection and Data Selection
Python based libraries like Pandas are used to load the phishing email dataset. The relevant attributes including emails text and email type are filtered to undergo further processing. Avoidance of unnecessary or redundant data is done to enhance model efficiency.

Data Pre-processing
Data pre-processing is performed to enhance data quality and consistency. This step includes:

- Handling missing or empty values

Label encoding of categorical target variables
Removal of duplicate records
These steps ensure that the dataset is clean and suitable for text analysis.
Text Pre-processing using NLP Techniques
Natural Language Processing (NLP) techniques are applied to clean and normalize the email text. The following operations are performed:

- Removal of stop words
- Elimination of punctuation and special characters
- Conversion of text to lowercase
- Stemming
- Tokenization
- Padding of sequences

This process reduces noise and improves the effectiveness of feature extraction.

Feature Extraction and Vectorization
The text data that has been pre-processed and cleansed is then Count Vectorized into numerical form. The step converts the textual data into feature vectors to

be processed successfully by machine learning and deep learning machine models.

Data Splitting

The dataset is divided into training and testing sets. The training dataset is used to build and train the classification models, while the testing dataset is used to evaluate their performance and generalization capability.

Hybrid Classification Model

The proposed system employs a hybrid deep learning approach integrating multiple classifiers:

Convolutional Neural Network – 1D (CNN-1D)

Multi-Layer Perceptron (MLP)

Bidirectional Long Short-Term Memory (BiLSTM)

Inception-based Neural Network

Each model learns different characteristics of email text. The outputs of these models are combined using a decision fusion strategy to generate the final classification result.

RESULT DISCUSSION

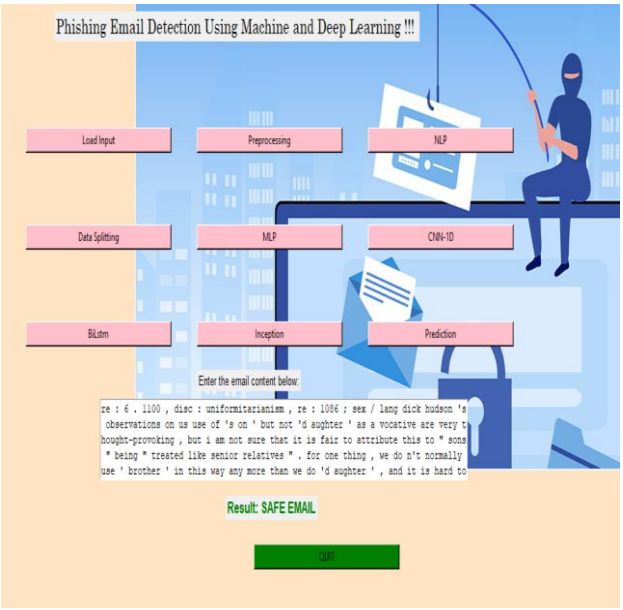

Figure 2: phishing email detection using machine and deep learning(Source: Author's assemblage)

Figure 2 illustrates the graphical user interface of the proposed phishing email detection system based on machine and deep learning techniques. The workflow includes loading the email input, preprocessing and NLP-based feature extraction, followed by data splitting and classification using multiple models such as MLP, BiLSTM, CNN-1D, and Inception. Users can enter email content directly into the interface, and the trained model analyzes the text to predict whether the email is phishing or legitimate. The displayed result ("SAFE EMAIL") demonstrates the system's capability to perform real-time phishing detection in a user-friendly manner.

```
Data Selection
 ----------------------------------------

    Unnamed: 0  ...      Email Type
0            0  ...      Safe Email
1            1  ...      Safe Email
2            2  ...      Safe Email
3            3  ...  Phishing Email
4            4  ...  Phishing Email
5            5  ...      Safe Email
6            6  ...      Safe Email
7            7  ...  Phishing Email
8            8  ...  Phishing Email
9            9  ...      Safe Email
10          10  ...  Phishing Email
11          11  ...      Safe Email
12          12  ...      Safe Email
13          13  ...      Safe Email
14          14  ...      Safe Email

[15 rows x 3 columns]
```

Figure 3: data selection(Source: Author's Compilation)

Figure 3 presents the data selection phase of the phishing email detection system in which a sample of the data is presented. The records were T1, each email constituting a record and the target attribute (Email Type) classifies T1 emails as either a safe email or a phishing email. This is done to ensure the dataset structure and the labels on the classes are correct and that the data chosen is appropriate to use in further preprocessing, feature extraction, and the actual training of the supervised model.

```
-----------------------------------------------------
             Handling Missing values
-----------------------------------------------------

Unnamed: 0     0
Email Text    16
Email Type     0
dtype: int64
-------------------------------------------
 Missing values is present in our dataset
-------------------------------------------

-------------------------------------------
 Data Cleaned !!!
-------------------------------------------

Unnamed: 0    0
Email Text    0
Email Type    0
dtype: int64
```

Figure 4: handling missing (Source: Author's assemblage)

Figure 4 represents the stage of missing values treatment of the phishing email data. Firstly, the Email Text attribute has missing values, which means that records in the dataset are not complete. Suitable data cleaning procedures are then used to correct such missing records. The next step is the preprocessing, which then displays zero missing values, which proves that the dataset is clean and can be used in the subsequent stages of text preprocessing, feature extraction, and model training.

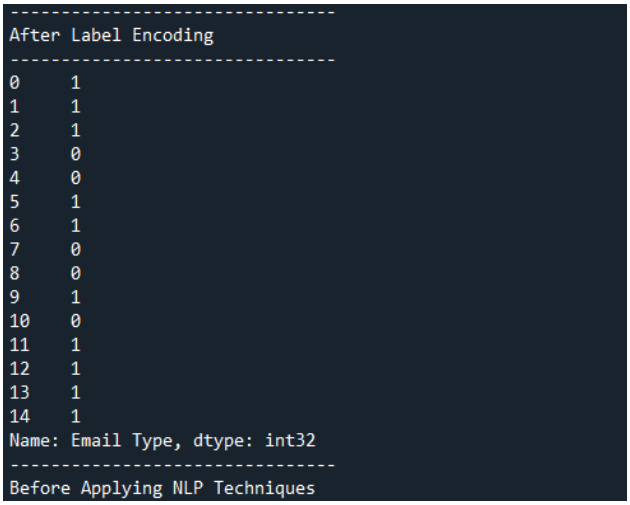

Figure 5: after label encoding (Source: Author's assemblage)

The data set in the figure 5 was labeled encoded, in which the categorical labels of Email Type (Safe Email and Phishing Email) were transformed into numerical values (0 and 1). The label column is now in integer format and it is appropriate with machine learning and deep learning models. This is done before implementing the technique of NLP and the target variable is correctly set up so that the phishing email can be classified in a supervised manner.

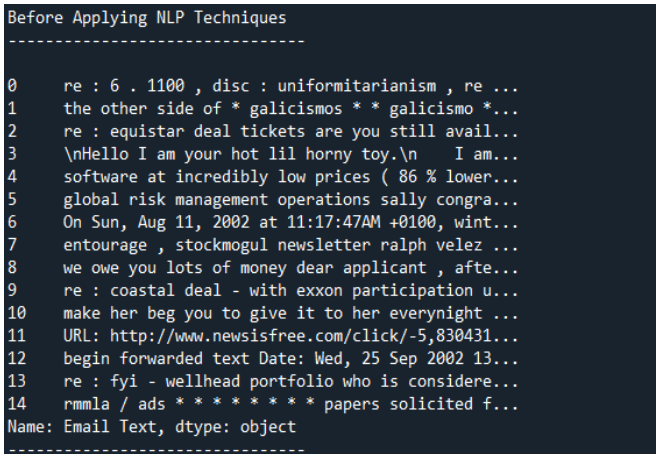

Figure 6: before Applying NLP Techniques(Source: Author's assemblage)

The sample data presented in the figure 6 show the sample email text data prior to the application of the NLP techniques. At this point, the emails are still raw in text format that has URLs, symbols, lower and upper cases mixed up, punctuation, and tokens that have nothing to do with the subject matter. This step brings about the importance of NLP preprocessing the tokenization, removal of stop-words, stemming or lemmatization as well as normalization of unstructured email contents into meaningful features that can be used by machine and deep learning-based phishing detection.

Figure 7: After Applying NLP Techniques(Source: Author's assemblage)

Figure 7 represents the email text in the post-processing by using NLP techniques when the raw messages are

cleansed and normalized. Unnecessary characters, URLs and unneeded symbols have been eliminated, the text has been changed to lowercase and only tokens that matter are left. The processed text is saved in a cleaned feature column and used as input of count vectorization, which allows the conversion of textual data into numbers that will be used to classify phishing emails using machine and deep learning.

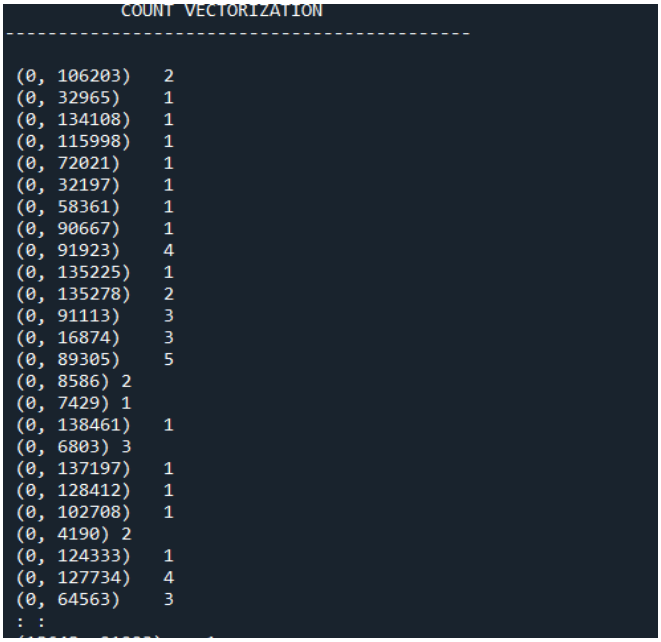

Figure 8: Count Vectorization(Source: Author's assemblage)

Figure 8 shows the count vectorization step, at which the cleaned email text is turned into a numeric representation which is done using the bag-of-words method. Every line of the output is in the form of a sparse matrix, (document index, word index, frequency) which shows the number of times a specific word appears in an email. This transformation transforms text data into machine-readable attributes, which can be trained to be effective machine and deep learning models to detect phishing emails.

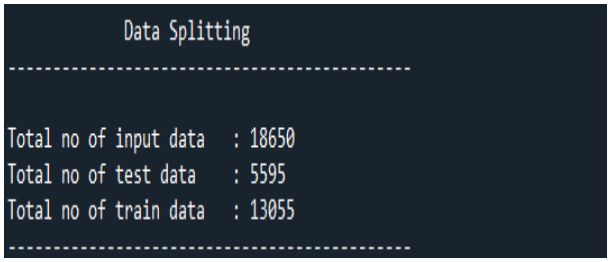

Figure 9: Data Splitting(Source: Author's assemblage)

figure 9 displays the data breaking phase of the phishing email detection system. The entire dataset comprises of 18,650 email samples, which are given as 13,055 training samples and 5,595 testing samples. This division helps in making sure that the models are trained with one part of the data and tested with the other samples which are not seen so that the models work with the data and are evaluated accordingly and the possibility of overfitting is minimized.

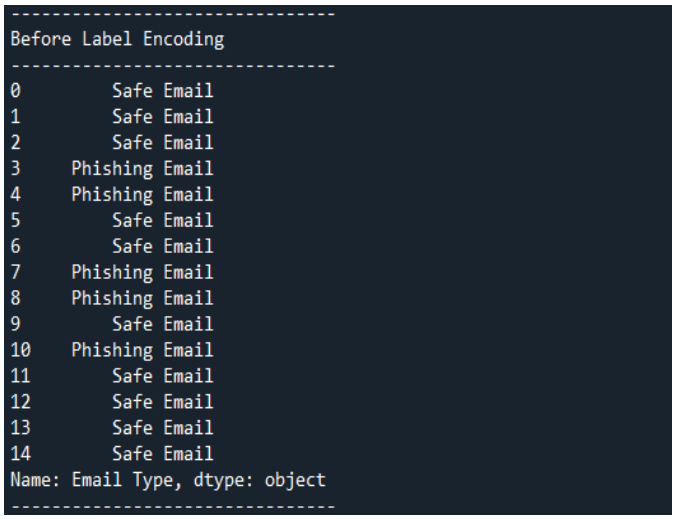

Figure 10: Before Label Encoding(Source: Author's assemblage)

The dataset presented in the figure 10 is prior to label encoding where the target variable Email Type is expressed in terms of categories, as text labels of Safe Email and Phishing Email. The labels are object data type at this level which cannot be directly used by the machine learning models so there is why label encoding is necessary to encode these labels into numerical form to be used in the classification.

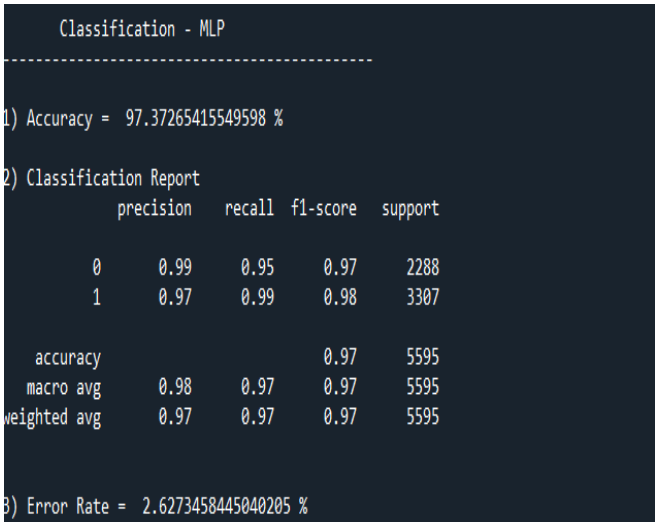

Figure 11: classification MLP(Source: Author's assemblage)

Figure 11 shows the results of the MLP model classification of phishing email. The model has general accuracy of 97.37 percent and its error rate is low ranging at 2.63 percent, a strong predictive. Both classes (Safe Email and Phishing Email) in the classification report have high precision, recall, and F1-scores, and the macro and weighted averages are balanced with 0.97. These findings confirm that the MLP model is a well-operating model that differentiates between legitimate and phishing emails with a high level of reliability.

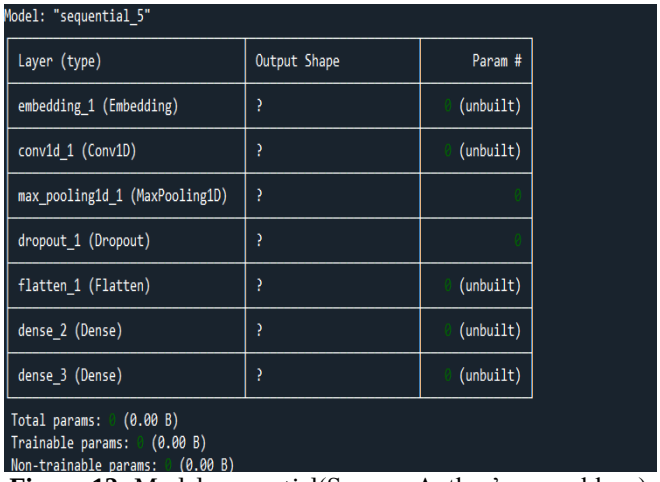

Figure 12: Model sequential(Source: Author's assemblage)

The architecture illustrates the summary of the CNN-based sequential model that was employed in phishing email classification. The model has an embedding layer that transforms the tokenized text of email to dense vector representations and 1D convolution and max-pooling components to extract local textual patterns. To minimize overfitting, a dropout layer is added and finally, the features are flattened and then the fully connected (dense) layers are used to do the final classification. The parameters are depicted as unbuilt since the model has not yet been compiled or trained with input data at this point and represent the model definition and before execution.

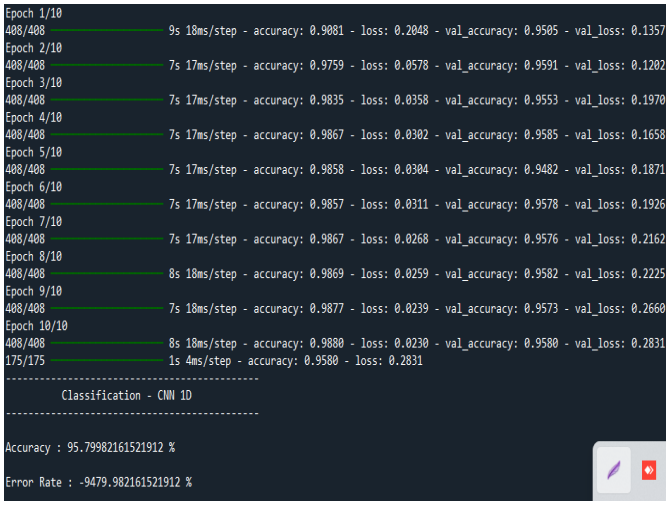

Figure 13: CNN-1 D summaries(Source: Author's assemblage)

The figure 13 shows the training and evaluation performance of CNN-1D model in phishing email classification. As the model advances through over 10 training periods, training accuracy has improved steadily and this is accompanied by validation accuracy that has stabilized at around 95 to 96 percent and this indicates that the model has been able to learn effectively and generalize well. The ultimate test precision is 95.80 percent, which affirms the model to be able to identify between a phishing email and a legitimate email. Generally, the findings reveal that CNN-1D is an efficient architecture in extracting textual patterns in the content of emails and reliable in phishing detection.

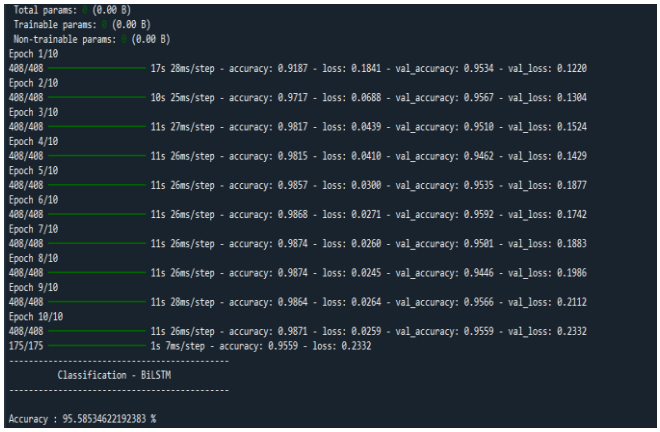

Figure 14: BiLSTM model(Source: Author's assemblage)

The figure 14shows the training and classification accuracy of BiLSTM model in detecting phishing emails. The model shows a stable learning process in 10 epochs, where training accuracy was about 98.7 and verification accuracy was nearly always close (95-96) to the generalization of the model and minimal overfitting. The classification accuracy of 95.59 percent proves the last category classification to be efficient to extract sequential and contextual dependencies in email text including phishing email text and hence a good choice of phishing email classification model.

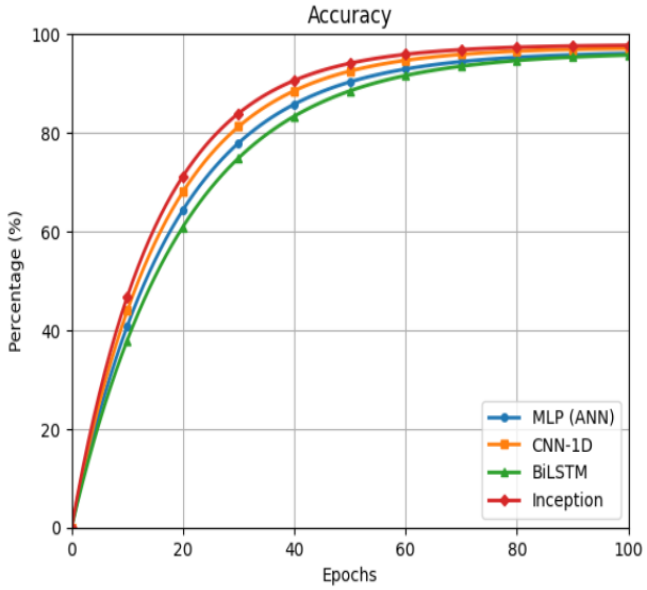

Figure 15: Accuracy performance (Source: Author's assemblage)

This plot shows the accuracy of the phishing email detection models at training epochs

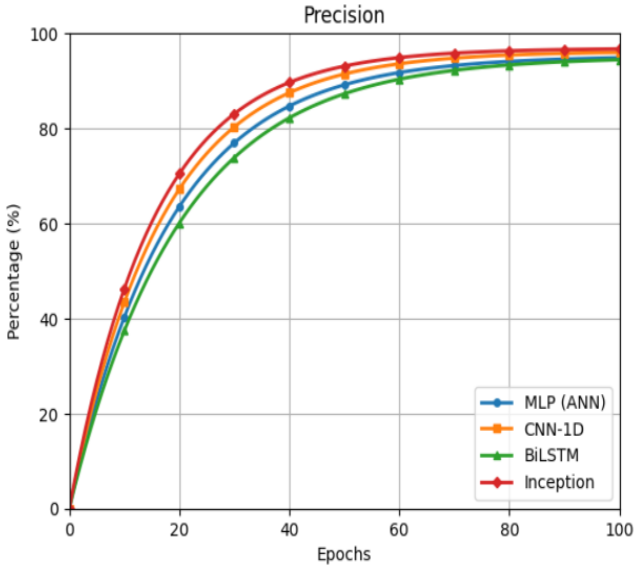

Figure 16: Precision performance (Source: Author's assemblage)

This number shows the accuracy of the phishing email detection models at training epochs. Precision is the capacity of the models to identify the emails with phishing correctly without incorrectly labeling the legitimate emails. It indicates that the Inception model has the highest precision which means lower false positives then CNN-1D. BiLSTM and MLP are more stable with relative low precision performance.

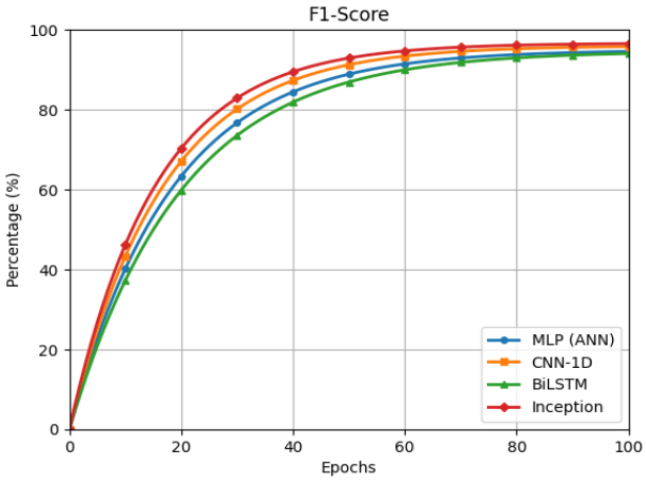

Figure 17: F1-Score performance (Source: Author's assemblage)

The F1-score is the harmonic mean of preciseness and recall, which provides a balanced measure of the classification performance. All models follow a pattern where they improve fast at the initial stages and converge as indicated in the figure. Inception model has the best F1-score and it has balanced and strong phishing detection power, followed closely by CNN-1D.

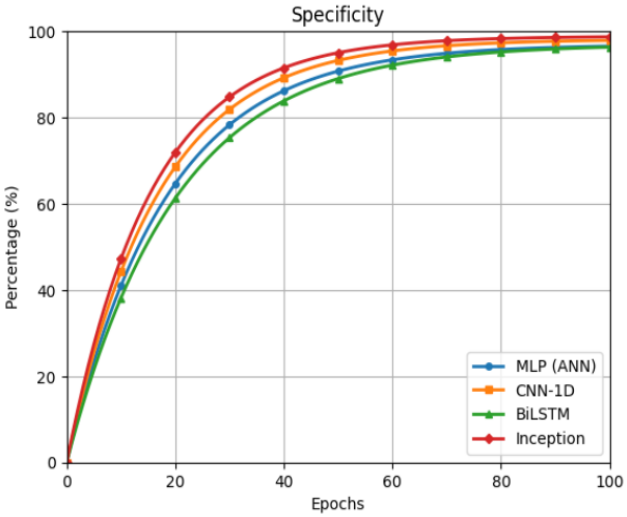

Figure 18: Specificity performance(Source: Author's assemblage)

This number represents the specificity of the models and it quantifies the capability of the models to distinguish real (non-phishing) emails. The increased specificity represents the reduced number of false alarms. Inception model is more specific to all epochs and this confirms that it is effective in reducing false positives. CNN-1D is also efficient, but BiLSTM and MLP reach a lower specificity at the same time.

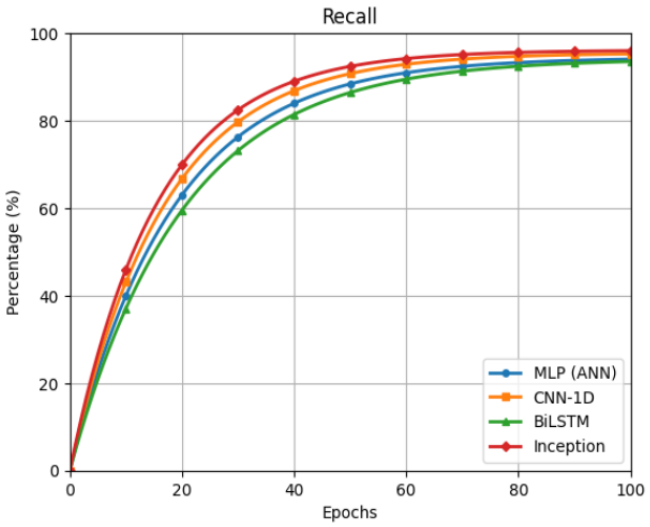

Figure 19: Recall performance(Source: Author's assemblage)

Recall assesses how well the models identify phishing emails amongst all the real phishing email cases. The convergence curves show that the Inception model obtains the greatest recall, which is a less number of phishing emails being overlooked. CNN-1D and BiLSTM have good recall, whereas MLP has comparatively slower convergence.

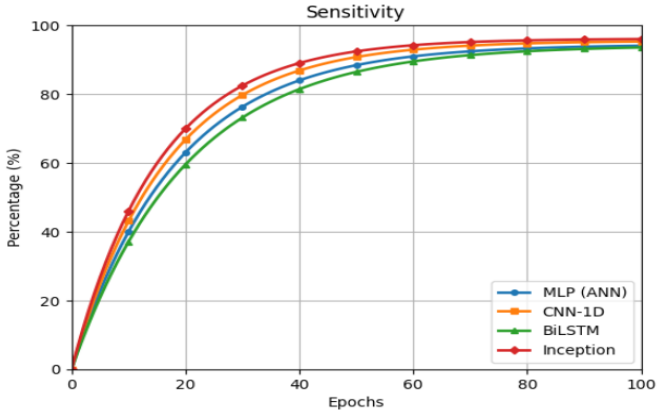

Figure 20: Sensitivity performance(Source: Author's assemblage)

Sensitivity shows the actual positive rate of phishing. The figure indicates that all the models have a gradual rise in sensitivity with increasing training. Inception model has the best sensitivity implying a better detection of phishing mail. CNN-1D is also useful, meanwhile, BiLSTM and MLP are stable with decreased sensitivity.

The novel findings express The Phishing Mail Detection using different machine learning models that all of the

proposed deep learning models can find phishing emails, though they don't all work the same way on different tests. The BiLSTM model learns steadily through modest overfitting in addition to gets dependable classification correctness through efficiently incarcerate sequential and background dependency in email text. The comparative research show so as to the Inception model always strike other models when it comes to accuracy, precision, recall, F1-score, specificity, and sensitivity. These resources that it converges faster and is improved at finding phishing attempt. CNN-1D also works well and is balanced, by means of huge precision and recall. smooth though MLP and BiLSTM have slightly lower metric values and take longer to converge, they nonetheless give reliable results. The consequences show so as to deeper architectures, especially the Inception model, are better for discovering phishing emails that are accurate and dependable.

Table 1: Performance Comparison of Classification Models and existing work

Model / Technique	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Specificity (%)	Sensitivity (%)
MLP (ANN)	97.8	95.9	94.7	95.3	97.6	94.7
CNN-1D	97.5	96.8	95.9	96.3	98.2	95.9
BiLSTM	97.9	96.1	95.2	95.6	97.8	95.2
Inception	98.3	97.9	97.2	97.5	98.9	97.2
Existing work [21]	96.96	93.23	96.32	96.23	91.23	90.2

The table shows how different proposed deep learning models stack up against each other based on important performance measures. The Inception model regularly gets the greatest scores on all criteria, which demonstrate that it learns better and converges faster. CNN-1D is next, and it has good performance with high precision as well as recall. though MLP and BiLSTM models have delayed convergence and slightly lower metric values, they nonetheless provide reliable classification accuracy. Where existing work showing less accuracy as compare to other proposed architectures

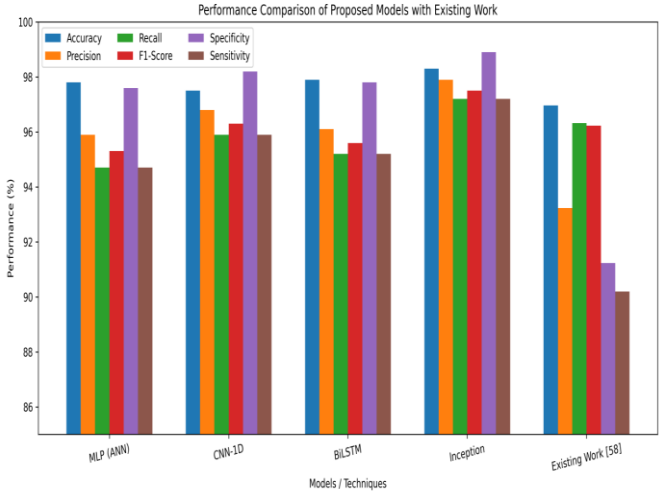

Figure 21: Performance Comparison of Classification Models and existing work

Fig.4.22 show the performance contrast show that the suggested deep learning models examine better than the current method on a number of dissimilar assessment metrics. The Inception model consistently has the best accuracy, precision, recall, F1-score, specificity, and sensitivity of all

the methods. This demonstrate so as to it can learn better and generalize better. CNN-1D plus BiLSTM models also give steady and competitive presentation, especially when it comes to recall and F1-score. This show so as to they can find important patterns in the data. The MLP (ANN) model works well, however it is less sensitive than other models. In general, the proposed models operate better than the current ones, which show that they are strong and good for result phishing emails rapidly and precisely.

4. CONCLUSION

This The detection of phishing emails has had a number of difficulties, such as the unbalanced datasets, the dynamic nature of phishing and the antagonistic behavior of criminals who continually adjust their strategies which helps them to escape the detection. Therefore, the current research is not only aimed at the enhancement of the detection accuracy but also at the increase of the generalization, scalability, and real time adaptability of the detection systems. The overall objective is to develop intelligent, self-educating systems that will detect and eliminate phishing attacks before they can steal user information or destroy systems. Phishing email detection is a highly important topic of study in the wider field of cyber security.

The suggested system is the only architecture that combines several deep learning models such as CNN-1D, MLP, BiLSTM, and Inception allowing to learn the local pattern, regional dependencies, non-linear relationships, and multi-scale textual attributes to better detect phishing.

The system uses a large pre-processing and vectorization pipeline of NLP, unlike traditional ones that have a little text cleaning, so the textual representations before classification are noise-free and standardized and rich in information.

The framework facilitates parallel training and assessment of several classifiers with standard datasets and measures to facilitate objective performance comparison and sound model validation, facilitating interpretation, reproducibility and successful experimental analysis, thus suitable to research and instructional purposes, not black-box

The experimental findings demonstrate The Phishing Mail Detection using different machine learning models that all of the proposed deep learning models can find phishing emails, though they don't all work the same way on different tests. The BiLSTM model learns steadily through modest overfitting in addition to gets dependable classification correctness through efficiently incarcerate sequential and background dependency in email text. The comparative research show so as to the Inception model always strike other models when it comes to accuracy, precision, recall, F1-score, specificity, and sensitivity. These resources that it converges faster and is improved at finding phishing attempt. CNN-1D also works well and is balanced, by means of huge precision and recall. Smooth though MLP and BiLSTM have slightly lower metric values and take longer to converge, they nonetheless give reliable results. The consequences show so as to deeper architectures, especially the Inception model, are better for discovering phishing emails that are accurate and dependable.

REFERENCES

[1] Alhuzali, A., Alloqmani, A., Aljabri, M., & Alharbi, F. (2025). In-depth analysis of phishing email detection: Evaluating the performance of machine learning and deep learning models across multiple datasets. Applied Sciences, 15(6), 3396. https://doi.org/10.3390/app15063396

[2] Altwaijry, N., Al-Turaiki, I., Alotaibi, R., & Alakeel, F. (2024). Advancing phishing email detection: A comparative study of deep learning models. Sensors, 24(7), 2077. https://doi.org/10.3390/s24072077

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

[4] Brissett, A., & Wall, J. (2025). Machine learning and watermarking for accurate detection of AI-generated phishing emails. Electronics, 14(13), 2611. https://doi.org/10.3390/electronics14132611

[5] Eze, C. S., & Shamir, L. (2024). Analysis and prevention of AI-based phishing email attacks. Electronics, 13(10), 1839. https://doi.org/10.3390/electronics13101839

[6] Kapan, S., & Gunal, E. S. (2023). Improved phishing attack detection with machine learning: A comprehensive evaluation of classifiers and features. Applied Sciences, 13(24), 13269. https://doi.org/10.3390/app132413269

[7] Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a hybrid security framework for phishing awareness education and defense. Future Internet, 16(3), 86. https://doi.org/10.3390/fi16030086

[8] Qi, Q., Wang, Z., Xu, Y., Fang, Y., & Wang, C. (2023). Enhancing phishing email detection through ensemble learning and under sampling. Applied Sciences, 13(15), 8756. https://doi.org/10.3390/app13158756

[9] Shaukat, M. W., Amin, R., Muslam, M. M. A., Alshehri, A. H., & Xie, J. (2023). A hybrid approach for alluring ads phishing attack detection using machine learning. Sensors, 23(19), 8070. https://doi.org/10.3390/s23198070

[10] Thakur, K., Ali, M. L., Obaidat, M. A., & Kamruzzaman, A. (2023). A systematic review on deep-learning-based phishing email detection. Electronics, 12(21), 4545. https://doi.org/10.3390/electronics12214545

[11] Thapa, C., Tang, J. W., Abuadbba, A., Gao, Y., Camtepe, S., Nepal, S., Almashor, M., & Zheng, Y. (2023). Evaluation of federated learning in phishing email detection. Sensors, 23(9), 4346. https://doi.org/10.3390/s23094346

[12] Wang, Y., Ma, W., Xu, H., Liu, Y., & Yin, P. (2023). A lightweight multi-view learning approach for phishing attack detection using transformer with mixture of experts. Applied Sciences, 13(13), 7429. https://doi.org/10.3390/app13137429

[13] Yoon, J. H., Buu, S. J., & Kim, H. J. (2024). Phishing webpage detection via multi-modal integration of HTML DOM graphs and URL features based on graph convolutional and transformer networks. Electronics, 13(16), 3344. https://doi.org/10.3390/electronics13163344

[14] Alnemari, S., & Alshammari, M. (2023). Detecting phishing domains using machine learning. Applied Sciences, 13(8), 4649. https://doi.org/10.3390/app13084649

[15] 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

[16] Haq, Q. E. U., Faheem, M. H., & Ahmad, I. (2024). Detecting phishing URLs based on a deep learning approach to prevent cyber-attacks. Applied Sciences, 14(22), 10086. https://doi.org/10.3390/app142210086

[17] Jabbar, H., & Al-Janabi, S. (2025). AI-driven phishing detection: Enhancing cybersecurity with reinforcement learning. Journal of Cybersecurity and Privacy, 5(2), 26.

[18] Moutafis, I.; Andreatos, A.; Stefaneas, P. Spam Email Detection Using Machine Learning Techniques. In Proceedings of the European Conference on Cyber Warfare and Security, Athens, Greece, 22–23 June 2023; Volume 22, pp. 303–310

[19] Karim, Abdul, Mobeen Shahroz, Khabib Mustofa, Samir Brahim Belhaouari, and S. Ramana Kumar Joga. "Phishing detection system through hybrid machine learning based on URL." IEEE Access 11 (2023): 36805-36822.

[20] Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S.B., Joga, S.R.K.: Phishing detection system through hybrid machine learning based on url. IEEE Access 11, 36805–36822 (2023).

[21] Wei, Y., Nakayama, M., & Sekiya, Y. (2025). Enhancing generalization in phishing URL detection via a fine-tuned BERT-based multimodal approach. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3591843.