IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

A Multi-Feature Hybrid DistilBERT Model for Phishing Email Detection Incorporating Header and Attachment Analysis

Mrs. Anuja Phapale, Devika Mule, Om Korhale, Anuja Kale
Department of Information Technology
AISSMS Institute of Information Technology, Pune, India
anuja.phapale@aissmsioit.org, devikamule8@gmail.com,
omkorhale3@gmail.com, kaleanuja211@gmail.com

Abstract: *Phishing emails have been known to pose a great cybersecurity threat globally. Phishing emails are a tactic that attackers employ to deceive the users to illegally leak or share their personal and financial data. This information can be misused by the attackers, violating and exploiting the user's privacy. It is highly essential to identify such phishing emails promptly and efficiently to help safeguard the users. Existing methods, including rule-based, traditional machine learning, and deep learning methods have focused on the textual content of the emails and the URL-based characteristics of the emails. Other attributes like email header and attachments, however, have been comparatively less emphasized even though they can offer valuable contextual information to make efficient phishing detection. This analysis integrates text and URL data of the emails with header and attachment-like aspects.*

Semantic representations which are extracted from email content are combined with attachment, URL and structured metadata characteristics in a hybrid architecture by the proposed Multi-Feature Hybrid DistilBERT Model. To determine the impact of different combinations of features three independent experiments are conducted. The expanded model is seen to increase the recall to 99.42%, which enhances the phishing detection ability whereas the base model has an accuracy of 98.82% and an F1 score of 99.23%. The model that is optimized has 99.42% accuracy which brings out the trade-off between the sensitivity of the detection and the false positives. The results show that the multi-dimensional characteristics can result in the increased detection strength of the model making the proposed approach eligible to real-world cybersecurity applications.

Keywords: Cybersecurity, Phishing Email Detection, Deep Learning, DistilBERT, Hybrid Model, Feature Engineering, Email Header Analysis, Attachment-Based Features, Natural Language Processing (NLP)

I. INTRODUCTION

E-mail is a fundamental application-layer service based on the working of TCP/IP protocol stack. It has emerged as one of the most important ways of communication in today's digital era. Through emails, we are able to easily move information across borders and time zones and this is advantageous to individual users and massive international companies. Cyber attackers and hackers have however, targeted it as a major target because it is widely used. Phishing is a very common and costly threat, which uses well-designed emails to lure naive users into providing their personal information such as password, personal identification number or bank account details [1]. Phishing email is a well-known tactic of fooling individuals into acting in a rush and being careless by instilling a sense of urgency, authority or familiarity. A phishing email's threat surface is far beyond its textual content; attackers deliberately include malicious

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

signals into a variety of email elements like the body text, hyperlinks, header fields and file attachments, each of which presents a unique deceptive opportunity [1].A more specific type of spear-phishing, where messages are tailored to individuals or organizations, makes them appear more believable and successful, thereby being more dangerous and raising concerns [1]. It has been estimated worldwide that the financial losses to phishing are in the billions of dollars annually and with the techniques to carry out such attacks becoming more intricate, there is an urgent requirement of smart and versatile detection procedures.

Attempts to automatically detect phishing emails have gone through three phases over the last few decades. Early detection systems used blacklist filtering techniques and rule-based logic to compare incoming communications to manually maintained lists of flagged domains and suspicious linguistic patterns, like odd header structures or high-risk keywords [2]. Despite the fact that these technologies were fast and convenient, they were quite inactive. Nevertheless, even the slightest alteration in the text, a newly created lookalike site or a minor structural shift in the mail [1][2] may make a phishing message seem invisible to such filters.

The second phase involved the introduction of machine learning by replacing the data-driven models that are able to learn discriminative patterns by using labeled samples with hard-coded rules. Significantly higher identification rates were shown by classifiers such Support Vector Machines, Random Forest, and Logistic Regression that were trained using TF-IDF feature representations of email text [3]. Incorporating stylometric cues by capturing writing style, linguistic behavior, and lexical content in stacked ensemble pipelines, researchers also learned to achieve higher scores of over 2.2% higher than purely text-vectorized baselines and F1-scores up to 0.9843 on balanced datasets [4]. Nevertheless, these advances did not increase the semantic ceiling of these methods as, although they could identify statistically frequent patterns, they could not decode tone, context, or the intent behind phishing language that was skillfully written [3].

The third and ongoing step is the transformer architecture and deep learning. GRU-based recurrent neural network-based models, with metaheuristic parameter optimization, demonstrated up to 99.72% detection accuracy [5]. This frontier has been further advanced by transformer-based models. To model sequentially, BERT was employed with LSTM, where the model attained 99.61% accuracy with a good generalization capacity of both training and testing conditions [6].These results indicate the significance of attention-related contextual representations in understanding the intricate language of lying. When the malicious purpose of a phishing email is hidden in a well-coded URL, that email will be able to pass a detection model that only scans the message content. On the other hand, URL-only systems may ignore the phishing attacks where the text is manipulative yet the hyperlinks appear to be safe. Semantic textual cues and URL-based structural cues have to be analyzed jointly to be effectively detected, but only a very small fraction of existing systems can achieve a real feature-level fusion [2][4].Although the primary focus of most of the existing methods is on textual content and URL-based features, other important attributes such as email headers and attachments have been relatively underresearched, although they can provide valuable information. Inconsistencies in sender identification and routing paths can be found in email headers, and suspicious file types or malicious payloads can be found in attachments—both of which are clear signs of phishing attempts.

This paper bridges this gap by using both textual and URL data combined with header and attachment based features. A hybrid architecture is proposed to enhance the detection performance by combining textual embeddings with DistilBERT with structured features representation. To systematically evaluate the impact of different combinations of features, three distinct experiments are conducted:(1) a baseline model which uses textual and URL features; (2) an extended model which uses header and attachment features; and (3) an optimized model which uses fine-tuning in architectural tuning as well as feature selection. The experimental results indicate that as much as textual features explain most of the overall accuracy, the structural features added to it enhances the detection sensitivity particularly in terms of recall and this makes the model more viable in real-life phishing detection scenarios.

The remainder of this paper is as follows: In Section 2, we will review relevant research on phishing detection; in Section 3, we will describe the proposed technique; in Section 4, we will present the results of the experiment and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

compare them with the existing levels of knowledge concerning the subject matter; and in Section 5, we will provide the conclusion and recommendations on future research.

II. LITERATURE SURVEY

In the field of cybersecurity, phishing email detection has been thoroughly investigated, resulting in the creation of numerous methods, such as rule-based systems, traditional machine learning models, and deep learning techniques. Over time, research has evolved to go beyond depending on heuristic rules and handcrafted features by data-driven and context-sensitive models that are capable of detecting complex patterns within email messages. This paragraph will overview the pros and cons of existing phishing detection methods and provide the foundations of the proposed strategy.

1. **Survey Spear phishing attacks detection and prevention: an in-depth survey (Birthriya SK, Ahlawat P, Jain AK · Computers & Security, 2025)[7]:**

In this study, a thorough fundamental survey of phishing detection and prevention methods at multiple layers is introduced. It speaks of the creation of more advanced methods that should stop more advanced spear-phishing attacks by traditional list-based filters, like blacklisting. The paper highlights the importance of dynamic and adaptive detection methods since blacklisting, though helpful as a preliminary filter, cannot be effective in dealing with obfuscated or recently created malicious domains. It forms a critical beginning point to understanding of the development and limitations of phishing defenses.

2. The Phishing Email Detection on Binary Search Feature Selection (Sonowal G. · SN Computer Science, 2020)[8]:

To identify phishing emails, this work proposes a binary search-based feature selection algorithm that embodies the rule-based paradigm where categorization is done using preset structural clues such as header anomalies, suspicious phrases and URLs patterns. The work demonstrates that the systematic selection of features can yield competitive results, but it also emphasizes the inherent limitation of rule-based systems, that is, they use pre-programmed signatures, which attackers can avoid exploiting by making minor structural or content modifications. This study is a clear motivation to switch to adaptive, learning detection algorithms.

3. Phishing Email Detection by machine learning algorithms (Murti YS, Naveen P. · Journal of Logistics, Informatics and Service Science, 2023)[9]:

The paper utilizes a real-world Kaggle dataset comprising of true percentages of valid and phishing e-mails in order to conduct an in-depth comparison analysis of the traditional machine learning classifiers like Naive Bayes, SVM, Random Forest, Decision Tree, and KNN. Exploratory data analysis (EDA) is used to perform preprocessing and ROC and AUC measures are employed to assess performance of the model. Random Forest and Decision Tree classifiers show the best precision, recall, and F1-scores, which confirms that tree-based ensembles are suitable to structured email feature spaces. The paper also highlights the necessity of deep learning methods because of the scale effect and the inability of conventional models to get deeper semantic context.

4. Improving the Phishing Email Detection using Stylometric Features and Classifier Stacking (Chanis I, Arampatzis A. · International Journal of Information Security, 2025)[10]:

Through simple TF-IDF vectorization with stylometric features, which are authorship and writing style indicators, under a classifier stacking ensemble method, this work broadens content-based phishing detection. The balanced and imbalanced datasets are tested in different stacking configurations, with F1-scores of 0.9843 and 0.9656, respectively, which outperform the baselines of vectorization-only by over 2.2%. The findings indicate that the inclusion of lexical features to non-textual stylometric features in a multi-classifier pipeline has a remarkable impact on detection performance, which in turn promotes feature-level hybrid approaches that integrate both textual and structure data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

5. Smart Phishing Email Detection and Classification by Deep Learning Based Cybersecurity Phishing Email Detection and Classification (Brindha R, Nandagopal S, et al. · Computers, Materials & Continua, 2023)[11]:
This paper proposes the ICSOA-DLPEC model, a combination of Intelligent Cuckoo Search (CS) optimization method to tune autonomous hyperparameters and a Gated Recurrent Unit (GRU) deep learning classifier. The CS algorithm is capable of determining the optimum GRU configuration, and this allows effective binary classification of emails as either phishing or legal. The proposed model has very high precision of 99.72% when tested against a conventional dataset. The paper contributes to the future of DL-based phishing detection by demonstrating that recurrent deep learning architectures with metaheuristic optimization result in significant performance benefits compared to static deep learning environments.

6. Phishing Email Detection Model based on Deep Learning (Atawneh S, Aljehani H. · Electronics, 2023)[12]:
Various deep learning models, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Recurrent Neural Networks (RNN) and BERT, are implemented and evaluated in this paper based on a collection of phishing and authentic emails that were subjected to NLP-based feature extraction. The highest accuracy of 99.61 is obtained using the best combination of BERT and LSTM after the consistent training and testing results indicate that this method has low overfitting and great generalization. This paper openly promotes the integration of BERT-based contextual representations with structural metadata into subsequent hybrid systems and outlines the possibilities of transformer-based embeddings in combination with sequential models in real-time phishing identification.

7. A Feature-Based Hybrid Model of an Automated Phishing Email Detection(Ayesha Saman, & Saad Rasool. (2025)[13]:
This paper proposed a hybrid deep learning model, which is a variant of DistilBERT, that uses a mix of URL-based features and semantic representations of email texts. This combined approach has a high accuracy of 99.1, precision of 98, and recall of 99 using the structural indicators and contextual language understanding. Although it is effective, the model does not attach much importance to other helpful properties such as email headers and attachments to concentrate on textual and URL elements. To bridge such a gap, the present implementation extends the framework to include the features of header and attachment based functionality which will enable a more comprehensive and reliable phishing detection system.

III. METHODOLOGY

A. Overview

This paper applies both text and structured metadata features to offer a hybrid deep learning-based phishing email detector. Through integration of multiple information sources, including email body text, URLs, header data and attachment properties, the overall objective is to enhance detection ability. The methodology includes three stages of an experiment:(1) Experiment 1: Baseline model (textual and URL) model; (2) Experiment 2: Extended model with both attachment and header functions; (3) Experiment 3: An improved feature selection model that
has been optimized.
This step-by-step design allows conducting a methodical evaluation of the impact of the additional features on model performance. Three models were designed to systematically determine the impact of additional features and architectural enhancements: a baseline model, an extended model and an optimized model.

B. Dataset description & Preprocessing:

Email samples classified into four categories—AI phishing, legitimate emails, manual spam, and Nigerian scams—make up the dataset used in this study. This issue is defined as a binary job of classification in order to conduct this study with legitimate emails being 0, and malicious emails (phishing, spam, and scams) being 1. The email subject and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

the body are combined into one text input to increase context awareness. In order to be consistent, empty values are filled with empty strings.

C. Feature Engineering

To obtain various attributes of phishing emails, several types of features are obtained:

1 Textual Features:

The primary source of information is the email content that is composed of the subject line and the body text. These two parts are joined together to form one textual input:

Subject + Body of email = combined text.

This will ensure that contextual cues present in both regions are recorded simultaneously. The DistilBERT tokenizer, which transforms unprocessed text into numerical representations (tokens) appropriate for deep learning models, is then used to tokenize the combined text. The tokenizer performs:

(1) Lowercasing;

(2) Padding (to guarantee a consistent length of sequence)

(3) Truncation (to limit to 128 tokens).

This processed text is then fed into the DistilBERT model to obtain contextual embeddings.

2 URL-Based Features:

The URLs in emails are one of the indicators of the phishing activity. Attackers often use malicious or deceptive links in order to deceive consumers. To capture this behavior, URL features are extracted out of the HTML text of the email using regular expressions. The characteristics listed below are derived:: (1) URL Count: The total number of URLs in the email; (2) URL Presence: Binary indicator of the presence of at least one URL. These characteristics assist us in measuring the level of link utilization, which is found to be frequently more in phishing emails.

3 Header Features:

Email headers contain details of an email origin, routing, and authentication. The phishing emails often misrepresent or modify the data in the headers. To gain access to valuable properties and detect structural anomalies that cannot be detected in the email body, the header data is saved in structured JSON format and decoded:(1) From-Reply-To Mismatch: Recognizes attempts at spoofing based on differences between the sender and reply addresses; (2) Return-Path Inconsistency: finds differences in the return path that could indicate a fake sender identity; (3) Number of Received Fields: shows the number of mail servers involved in routing; a high number may imply doubtful routing.

4 Attachment Features:

Attachments are often used to deliver malicious payloads, such as executables or compressed files. The characteristics below are borrowed off the attachment field and provide information regarding potential risks associated with attachments. The number of attachments depicts how many files are attached. Executable File Indicator (.exe): Indicates attachments that can be harmful. Packaged payloads that are frequently used to get around filters are detected by the Compressed File Indicator (.zip).

D. Feature Normalization:

StandardScaler is employed to normalize all the structure (non-textual) features to ensure that scaling is done similarly across all. This prevents dominance of features with wide ranges of numbers in the learning process.All the structured characteristics (URL, header, and attachment features) are normalized with StandardScaler to give them a zero mean and unit variance. This step is essential to ensure that all features are equal contributors to the learning process and to make sure that the features with bigger sizes do not dominate in the learning process.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

E. Model Architecture:

The proposed model follows a hybrid architecture which combines deep contextual embeddings along with structured feature representations.

1) Text Processing Module (DistilBERT):

The textual input is fed through an already trained DistilBERT model that produces contextual embeddings of each token. Based on the output obtained, the embedding of the [CLS] token is then extracted. The vector is a concise embodiment of semantics of the whole email. Advantages of using DistilBERT model are that it is lightweight and faster than BERT, retains ~97% of BERT's performance and is very suitable for resource-constrained environments.

2) Structured Feature Processing Module:

The Structured features are processed with the aid of a special feedforward neural network. This module studies patterns on its own, which are specific to the metadata of textual data that is received. The architecture consists of: a Fully connected layer, a ReLU activation and Dropout to regularize it. This separation takes care that the structured features are not overshadowed by high-dimensional textual embeddings.

3) Feature Fusion Mechanism:

The features of Text module (768-dimensional embedding) and Structured feature module are joined together to create a single feature. This integration allows the model to integrate semantic knowledge of the text with structural knowledge and therefore account for the intricate interactions among the different types of features.

4) Classification Layer:

The fused representation is then passed through the fully connected layers, which is followed by a sigmoid activation function, that produces a probability score for binary classification such that if output is 1 it classifies as a phishing email, whereas if the output is 0 it classifies as a legitimate email.

F. Experimental Setup:

1) Problem Formulation:

In the original dataset that we have used, there are various categories of emails. To simplify the task to a binary classification problem, in this paper, Legitimate emails are classed as 0 and phishing, spam and scam emails are malicious and thus classified as 1. This problem formulation is in line with the real world phishing detection systems where phishing emails are of varying types.

2) Data Splitting:

The dataset will be divided into 80% Training Data, 20% Testing Data. This is to make sure that there is a fair test on generalization of models.

3) Training Configuration:

The model is trained with the following parameters:

Loss Function: Binary Cross-Entropy Loss.

Optimizer: Adam / AdamW

Learning Rate: 2e-5

Batch Size: 8 (Training on large datasets with Batch-wise training is both efficient and it prevents overloading of the GPU memory)

Epochs: 3–4

4) Evaluation Metrics:

To comprehensively evaluate performance of the model, the following metrics are used:

Accuracy: Refers to the general accuracy of forecasts.

Precision: To measure correctness of phishing predictions

Recall: To measure ability to detect phishing emails

F1 Score: Harmonic mean of precision and recall.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Particular attention is paid to recall because it is possible to have dire consequences in case of not receiving phishing emails.

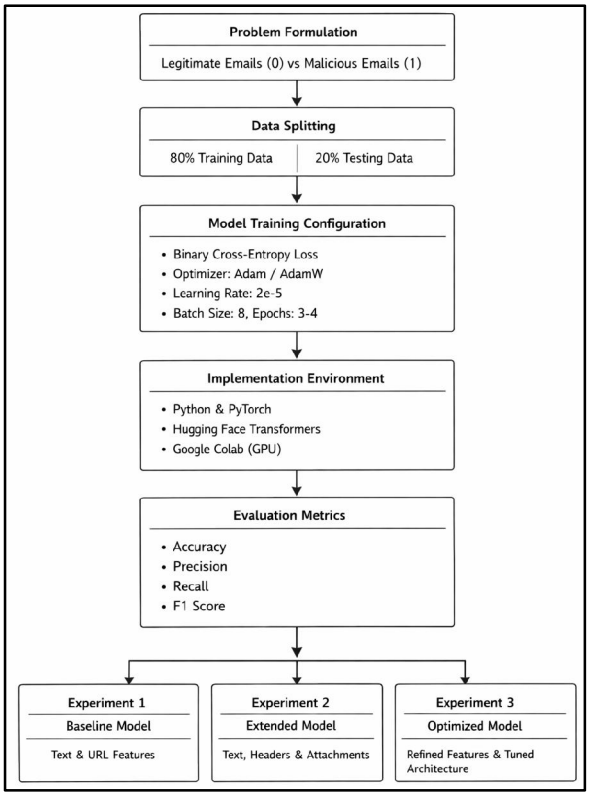

Figure 1. Experimental Setup

5) Experimental Design Strategy:

Three experiments are carried out to determine the effect of various sets of features and their combinations:

Experiment 1: Baseline Model

Only textual and URL features of the email are used in the model in this experiment. This model basically reproduces the model in the paper by Saman, Ayesha, and Saad Rasool[14].

Experiment 2: Extended Model

In this experiment, we have added header and attachment features also to the model. This is done in order to evaluate the impact of additional metadata which is the main aim of our research.

Experiment 3: Optimized Model

We have optimized the feature selection process and fine-tuned the model structure to achieve increased accuracy and recall in this experiment.

G. System Architecture:

1) Overview of the System:

The proposed system is a hybrid phishing email detection system consisting of deep learning-based textual analysis and structured feature processing. This architecture follows a multi-stage pipeline which transforms raw email data into meaningful predictions. The following are the key components of the proposed system. These components play a major role in ensuring accurate and robust phishing detection:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Input Layer
Preprocessing Module
Feature Extraction Module
Hybrid Model (Text + Structured Processing)
Classification Layer
Output Layer

2) System Pipeline:

The overall workflow of the system can be described as following:
Email Data → Preprocessing → Feature Extraction → Hybrid Model → Prediction

3) Input Layer:

The system accepts raw email data as input, that includes following features:
Email body (text)
Subject line
HTML content
Metadata (email headers)
Attachment information
This multi-modal input facilitates the system to examine the content and structural properties of emails.

4) Preprocessing Module:

This step involves cleaning and preparing the raw input to be used in the feature extraction process.The omitted values are filled with the null replacement technique, the subject and the body are merged into a text input, the labels are transformed into a binary form (phishing vs legitimate). This preprocessing of data ensures consistency and improves model's performance.

5) Feature Extraction Module:

There are two kinds of features that are extracted by the system:
Textual Features: They are sent through the DistilBERT tokenizer and then token embeddings are obtained. It simply extracts semantic content of email messages.
Structured Features: These cover URL features (count, presence), Attachment features (file types, count) and Header features (mismatch indicators, routing information). All these organized features are regularised and then submitted to the model to be further assessed.

6) Hybrid Model Architecture:

The very essence of the suggested system is a hybrid neural network, which contains two parallel processing arms:
1. Text Processing Branch:This branch is responsible for capturing the deep semantic patterns in email content. It comprises of adhering to:
Input: Text in email format, tokenized.
Output: contextual embedding (token) 768-dimensional.
2. Structured Feature Branch: This branch deals with capturing the behavioral and metadata patterns. It is composed of following:
Input: Designed numerical characteristics.
Model: Feedforward neural network.
Output: Structured representation learnt.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

The result of the two of these branches is then concatenated in an attempt to create a combined feature vector in the following way:

[Text Embedding (768)] + [Structured Features Representation.]

This combination enables the model to utilize semantic and structural information at the same time.

7) Classification Layer:

The combined feature vector is passed through the fully connected layers, which are followed by the Sigmoid activation function which gives outputs in the form of a probability score which is between 0 and 1.

8) Output Layer:

The last result obtained is the classification like 1 is a Phishing email and 0 is a Legitimate Email. A threshold which is typically 0.5 is used to make the final decision.

The suggested system has numerous benefits- It can be used to combine deep learning and feature engineering, it discovers both semantic and structural patterns of an email, it can be extended and modified to a higher level of flexibility and can detect a wider range of cases (better recall).

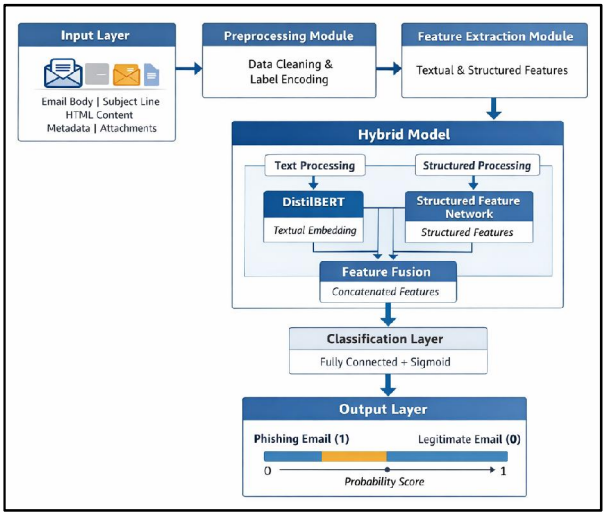

Figure 2. System Architecture

IV. RESULTS & DISCUSSION

Three separate experiments were done to determine the success of the hybrid phishing detection framework proposed. Each of the experiments used a variation of the model to examine the effect of adding extra features of an email like URLs, email headers and attachments. Each model is tested based on four typical measures, which include Accuracy, Precision, F1 Score and Recall.

Experimental Results:

The table below summarizes the quantitative results of the three experiments.

Table 1. Comparative Performance of Three Experimental Models

Metric	Exp. 1	Exp. 2	Exp. 3
Accuracy	98.82%	98.67%	98.23%
Precision	99.61%	98.85%	99.42%
Recall	98.85%	99.42%	98.27%
F1 Score	99.23%	99.14%	98.84%

DOI: 10.48175/IJARSCT-32847

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Analysis:

Experiment 1 (Baseline Model): The overall best performer was the baseline model, which considers textual features, and URL-based data, and achieved the best accuracy (98.82) and F1 score (99.23). This indicates that the DistilBERT is effective at identifying semantic trends in emails and that text is highly informative when it comes to detecting phishing. The high level of the model performance shows that in most cases, language-based signals are sufficient to achieve high classification accuracy.

Experiment 2 (Extended Model): To allow representing email data in a more complete way, the second experiment uses additional attributes, which are extracted out of email headers and attachments. The model has the highest recall (99.42) of any of the studies, although with a slight drop in overall accuracy.The much lower accuracy can be attributed to the emphasis of the base model on textual features, which make the classification most accurate. Our proposed model incorporates additional header and attachment properties, which raise recall and accuracy, but bring about a minimal degree of variability. This increases the effectiveness of the model in detecting phishing in the real world. This is an indication that the model is effective in reducing the number of false negatives (phishing emails that were missed) and becomes more responsive to phishing activities.This is very desirable from a cybersecurity standpoint since, while false alarms are comparatively less serious, missing a phishing email can have serious repercussions. Thus, although there is no significant improvement in total accuracy, Experiment 2 demonstrates that the addition of structural features enhances the detection abilities.

Experiment 3 (Model Optimization): In order to increase productivity and decrease redundancy, feature selection and architectural improvements were used in the third trial. Recall and accuracy of the model were slightly lower, but its precision was high (99.42%). This implies that the model will minimize false positives and be more conservative in its predictions, but some phishing emails may be missed. Based on the results, aggressive feature selection can remove valuable information, which would diminish the detection sensitivity.

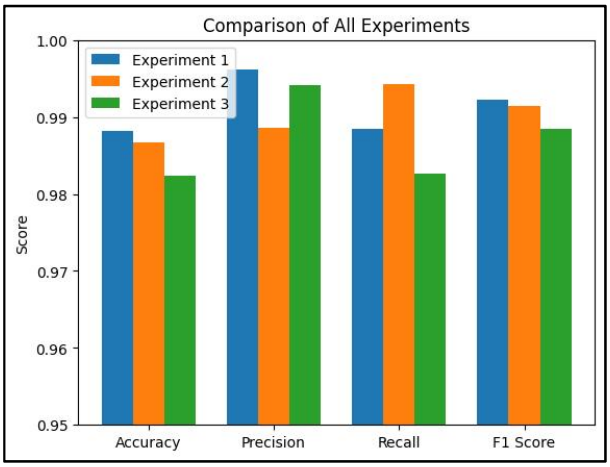

Figure 3. Comparison of Performance metrics of all 3 experiments

Comparative analysis of all three experiments conducted show that a significant trade-off exists between the performance measures::

Trade-off between Precision and Recall is observed as follows:

Experiment 1: Balanced performance

Experiment 2: High recall (greater detection)

Experiment 3: Accurate (low false alarms)

This highlights an important fact: The combinations of features influence the behavior of models, leading to trade-offs between detection sensitivity and prediction accuracy. The results sufficiently demonstrate that: (1) overall perfor-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

mance is dominated by textual elements; (2) recall is enhanced by structural elements (headers, attachments); (3) the process of feature selection must be well-balanced to avoid losing valuable information.

V. CONCLUSION

The paper proposed a composite deep learning-based phishing email detection system that incorporates structured feature engineering with URLs, email header, and attachments and language analysis with DistilBERT. The idea was to find out whether semantic and structural information can be combined to improve phishing detection performance. Three experiments were conducted to systematically investigate the input of different feature sets.

The baseline model was effective in all measures of evaluation, which indicates that textual features are highly effective. The proposed hybrid model that incorporated attachment and header functionalities enhanced recall significantly implying that the phishing email detection capability would be enhanced. Following the optimization, the proposed model showed the trade-off between accuracy and recall by exploring further in terms of feature selection and architecture modification.

Based on the experimental findings, structural characteristics make the model more sensitive to harmful patterns, but overall the accuracy is dominated by textual embeddings. This leads to a more accurate detection mechanism and particularly where missing phishing emails can be highly detrimental. Moreover, the proposed technique proved to be effective and relevant in practice because it achieved the same accuracy with higher precision, recall, and F1 score, compared to the original Hybrid DistilBERT model[]. The proposed hybrid architecture proposes a scalable and efficient phishing detection system with potential applications in modern cybersecurity systems.Generally, our work has emphasized the need to incorporate intelligent features in phishing detection with the aim of balancing sensitivity and reliability of detection, as opposed to focusing on making phishing detection as accurate as possible.

Although the proposed model could be effective, various enhancements could be explored to enhance its effectiveness, including incorporating multi-class categorization, Explainable AI, or real-time deployment. To increase generalization and resilience, the model can also be trained on bigger and more varied datasets.

REFERENCES

[1] S. K. Birthriya, P. Ahlawat, and A. K. Jain, “Detection and prevention of spear phishing attacks: A comprehensive survey,” Computers & Security, vol. 140, 2025.

[2] G. Sonowal, “Phishing email detection based on binary search feature selection,” SN Computer Science, vol. 1, no. 6, pp. 1–13, 2020.

[3] Y. S. Murti and P. Naveen, “Machine learning algorithms for phishing email detection,” Journal of Logistics, Informatics and Service Science, vol. 10, no. 4, pp. 1–15, 2023.

[4] I. Chanis and A. Arampatzis, “Enhancing phishing email detection with stylometric features and classifier stacking,” International Journal of Information Security, 2025.

[5] R. Brindha, S. Nandagopal et al., “Intelligent deep learning based cybersecurity phishing email detection and classification,” Computers, Materials & Continua, vol. 75, no. 1, pp. 1123–1138, 2023.

[6] S. Atawneh and H. Aljehani, “Phishing email detection model using deep learning,” Electronics, vol. 12, no. 3, p. 3262, 2023.

[7] Birthriya, Santosh Kumar, Priyanka Ahlawat, and Ankit Kumar Jain. "A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies." *Journal of Applied Security Research* 20.2 (2025): 244-292.

[8] Sonowal, Gunikhan. "Phishing Email Detection Based on Binary Search Feature Selection: G. Sonowal." *SN Computer Science* 1.4 (2020): 191.

[9] Murti, Yoga Shri, and Palanichamy Naveen. "Machine learning algorithms for phishing email detection." *Journal of Logistics, Informatics and Service Science* 10.2 (2023): 249-261.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

[10] Chanis, Ilias, and Avi Arampatzis. "Enhancing phishing email detection with stylometric features and classifier stacking." *International Journal of Information Security* 24.1 (2025): 15.

[11] Brindha, R., et al. "Intelligent deep learning based cybersecurity phishing email detection and classification." *Computers, Materials, & Continua* 74.3 (2023): 5901.

[12] Atawneh, Samer, and Hamzah Aljehani. "Phishing email detection model using deep learning." *Electronics* 12.20 (2023): 4261.

[13] Saman, Ayesha, and Saad Rasool. "A feature-level hybrid model approach for automated phishing email detection." *Journal of Computing & Biomedical Informatics* 9.01 (2025).

[14] Saman, Ayesha, and Saad Rasool. "A feature-level hybrid model approach for automated phishing email detection." *Journal of Computing & Biomedical Informatics* 9.01 (2025).