Transfer Learning Models for E-mail Classification

Muatamed Abed Hajer[1,*], Mustafa K. Alasadi[2], Ali Obied[3]

[1]Faculty of computer science and Information Technology University of Sumer, Thi-Qar. Iraq

[2]Faculty of Computer Science and Information Technology, University of Sumer, Rifai, Iraq

[3]Dept. of computer science, college of comp &IT, university of Al-Qadisiyah, Iraq

Emails: m.hajer@uos.edu.iq; mustafa.kamil@uos.edu.iq; Ali.obied@qu.edu.iq

Abstract

Phishing and spam are examples of unsolicited emails, result in significant financial losses for businesses and individuals every year. Numerous methodologies and strategies have been devised for the automated identification of spam, yet they have not demonstrated complete predictive precision. Within the spectrum of suggested methodologies, ML and DL algorithms have shown the most promising results. This article scrutinizes the outcomes of assessing the efficacy of three transformation-based models - BERT, AlBERT, and RoBERTa - in scrutinizing both textual and numerical data. The proposed models achieved higher accuracy and efficiency in classification tasks, which was a notable improvement above traditional models such as KNN, NB, BiLSTM, and LSTM. Interestingly, in several criteria the Roberta model achieved almost perfect accuracy, suggesting that it is very flexible on a variety of datasets.

Keywords: Spam E-mail; BERT; ALBERT; Roberta; Machine learning; Deep learning

1. Introduction

The effective exchange of a wide range of information via email is still possible. Email plays vital role in international business communication because to its ability to send messages, files, media, and hyperlinks with great flexibility. Email is a convenient and affordable solution, even with its asynchronous nature (messages stay in the recipient's inbox until they are opened) and ease of distribution to several recipients at once. However, there are a lot of obstacles due to the increasing number of unsolicited emails, or spam. Online communication is becoming a necessary component of our everyday lives due to the rapid expansion of social media and internet usage. Email has emerged as a popular venue for official and commercial correspondences due to its accessibility, speed, and dependability [1]. As email's popularity grows, spam emails have expanded rapidly, inundating people with unwanted ads such as debt relief offers, quick-money schemes, online dating proposals, health-related product endorsements, and so on. To solve this issue, novel neural programming and machine learning approaches have emerged [2]. Natural Language Processing (NLP) is used to identify and classify spam emails. NLP is responsible for converting unstructured email content into structured data, which helps in text analysis and ultimately increases the accuracy of the model. Multiple machine learning methods can be used to filter emails. [3]. Recent models have demonstrated in the field of transfer learning, especially those that use pre-trained models for a variety of natural language processing tasks. The BERT model outperformed other techniques. BERT is used to generate word embeddings that take into account important contextual information from preceding and following words, resulting in different semantic representations of a given word depending on its context. Ongoing research efforts focus on investigating BERT-based models for automated spam detection and evaluating these systems using new methodologies on publicly available datasets containing spam and unsolicited email. [4, 5]. The contributions of this paper can be listed in the following points:

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

1. *Efficacy Assessment*: The article demonstrates the ability of three transfer learning models, BERT, AlBERT and RoBERTa to examine text data along with numerical values.
2. *Highly Accurate and Efficient*: Our models showed very high accuracy and efficiency over common tradition methods (e. g., KNN, NB, BiLSTM, LSTM) in classification tasks
3. *Strong Performance of RoBERTa*: The base RoBERTa model was among the best at nearly everything and reached almost perfect scores on some criteria, which demonstrates its degree of generalization across datasets.
4. *Improved over traditional models*: We show that compared to traditional models, transformation-based modalities work well in dealing with complex data types.

2. Background

This section shows briefly background about transfer learning that used in this paper.

2.1. Transformer Model

The transformer model is popular because it incorporates a self-attention mechanism that aids in understanding the context represented by serial inputs. Its primary benefit is its capacity to properly handle large-scale interactions between input components, allowing for parallel processing and surpassing standard neural networks. Transformers stand out due to their influence on natural language processing and capacity to adapt to a wide range of data sources. New advancements have resulted in the development of transformer-based systems, such as BERT models.

2.1.1. BERT

BERT (Bidirectional Encoder Representations from Transformers) is a popular model developed by Google for natural language processing tasks. Known for its efficiency and simple structure, BERT differs from traditional transformers by utilizing only the encoder part and discarding the decoder part Trained on extensive data from Book Corpus and English Wikipedia, BERT produces two outputs used for language translation, sentiment analysis, fake news detection, and spam detection The model's versatility allows for various applications like text classification, named entity recognition, and question answering, making it suitable for tasks like spam message classification BERT's pre-trained base uncased model, when fine-tuned, proves effective in detecting spam emails with high accuracy and F1 scores[6]. Unlike traditional feature-based methods, BERT follows the fine-tuning approach where the model is pre-trained on unlabeled data before being fine-tuned for specific tasks During fine-tuning, two sentences are combined, and the special token [CLS] at the beginning represents the sequence pair BERT is known for its effectiveness in capturing complex features like syntax and semantics for sequences of any length, leading to state-of-the-art results in various sentence-level tasks The representation by BERT focuses on tokens within a sequence rather than individual sequences, which can lead to limitations in handling different granularities of text[7-8]

2.1.2. Albert

ALBERT (A Lite BERT) is a model designed for self-supervised learning of language representations based on BERT, utilizing multi-layer Transformers It is pre-trained and fine-tuned for specific tasks, such as similarity classification In the research paper, ALBERT was explored for Mathematical Answer retrieval, surpassing other models in performance The model It uses a sentence-order prediction (SOP) loss to model inter-sentence coherence effectively ALBERT models have much smaller parameter size compared to BERT models with comparable hyper parameter settings The ALBERT architecture backbone is similar to BERT, using a transformer encoder with GELU nonlinearities Increasing the number of layers in the ALBERT model can significantly improve performance, but there are diminishing returns after a certain point To enhance ALBERT's efficiency, methods like sparse attention and block attention can be used to speed up training and inference[9]

ALBERT's design aims to match the semantics of text rather than just their tokens, enhancing its capabilities in various natural language processing tasks through pre-training on Mathematics
Stack Exchange data and fine-tuning for Mathematical Answer Retrieval, calculates the similarity score between two text snippets, like a question and an answer ALBERT demonstrated strong mathematical post modeling capabilities [10]

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

2.1.3. Roberta

RoBERTa is a pre-trained Encoder model that builds on BERT's language masking strategy, with modifications such as larger minibatches and learning rates It was trained on significantly more data than BERT and for a longer duration, leading to better generalization to downstream tasks
RoBERTa stands for robustly optimized BERT approach, which is an improved version of BERT pretraining RoBERTa is a robust language representation model used for various natural language processing tasks, exhibiting state-of-the-art performance in text classification datasets

The RoBERTa model is utilized in the research paper for predicting labels such as Facts, Ruling, Argument, Statue, Precedent, Ratio of decision, and Ruling by present court In the study, three different systems were developed based on RoBERTa with varying epochs, where the system trained for 15 epochs achieved the highest ranking with a Macro-F score of 0.468 The output of the RoBERTa model is passed through a bidirectional LSTM, followed by a dense layer, global_max_pooling_1D layer, and a softmax layer to obtain the desired output [11]

Modifications in RoBERTa include training with dynamic masking, using full sentences without the next sentence prediction loss, employing large mini-batches, and implementing a larger byte-level BPE The RoBERTa model is trained following the BERT LARGE architecture, with specific parameters (L = 24, H = 1024, A = 16) and a total of 355 million parameters RoBERTa pretraining involves training for 100K steps over a dataset combining Book-Corpus and Wikipedia data using a large number of GPUs for approximately one day [12]

RoBERTa is an artificial neural network based on transformers with 6 layers, focusing on large-scale byte and batch increments It uses WordPiece tokenization and masked layer modeling (MLM) and next sentence prediction (NSP) during training RoBERTa eliminates the NSP method, making modifications to the pre-training section of BERT, and uses the ByteLevelBPE tokenization method derived from GPT-2 The RoBERTa model aims to improve final project performance by training with dynamic masking without losing NSP, showing promising results in natural language generation for question-answering tasks in English and French[14].

2.2. Related Work

The issue of spam detection has drawn the attention of several researchers, and various methods have been put out in the literature. This section reviews some earlier research that employed BERT models, deep learning methods, and machine learning approaches to detect and classify spam.

Hassanpur et al. [15] used the word2vec package to convert emails to vectors rather than rule-based techniques. Vector representations are given into the learning model, a neural network (NN). In comparison to typical machine learning techniques, their approach delivers more than 96% accuracy.

Egozi et al. [16] endeavored to validate the efficacy of utilizing NLP methodologies in identifying phishing emails through the analysis of email sample contents and extraction of characteristics emphasizing word frequencies, occurrences of stop words, instances of punctuation, and uniqueness metrics. A total of 26 features were derived and employed in the training of a composite learning framework utilizing a linear kernel Support Vector Machine (SVM), resulting in the accurate classification of more than 80% of phishing emails and 95% of legitimate emails.

Shajideen,N.M.et al [17] The goal of this paper is to compare how well machine learning classifiers perform in accurately distinguishing between emails. The SVM model has shown high accuracy in classifying messages. Methods used include training SVM, Naive Bayes (NB) and J48 machine learning algorithms

Saab et al. [18] The study focuses on distinguishing between "ham" (legitimate emails) and "spam" (unsolicited emails) to improve email filtering processes.Support Vector Machines (SVM) are employed as one of the classification algorithms due to their mathematical foundation in statistical learning theory They achieved an accuracy of 93.57%

Anshumaanmishra et al. [19] The paper focuses on using advanced techniques such as deep learning to identify and classify spam emails. The study used different deep learning models such as RNN, LSTM and BLSTM to classify spam messages.Evaluate the proposed method and compare it with other existing models based on loss curve history, precision and accuracy. Based on the results, the Bi-LSTM model proposed in the paper produced higher accuracy their study achieved an accuracy of up to 97% using the Bi-LSTM model.

Farkhund Iqbal [20] the research proposes four categories – normal, fraudulent, threatening and suspicious emails – as new ways to analyze email. The best strategy was discovered by conducting an examination of the

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

transformers and machine and deep learning. The transformers achieved the highest accuracy compared to previous works, with an accuracy rate of 98%.The research also discussed issues such as data privacy concerns and the need for continuous model updates to combat new spam techniques.

Isra'a AbdulNabi and Qussai Yaseen[21] Presented the approach of using deep learning techniques to detect spam emails. In the context of deep learning model training, this research specifically focused on automatically embedding words into classification and feature extraction as part of the deep learning model training process. Understanding text context using attention layers allows the pre-trained BERT model to be improved for its detection. The proposed approach achieved a high accuracy of 98.67%. Dense layers and BiLSTM are compared to the basic DNN architecture.

Malhotra, P., & Malik, S. [22] the research uses spam dataset and Natural Language Processing (NLP) to distinguish between spam and non-spam (Ham) emails. The research paper focuses on applying deep learning and machine learning algorithms to detect spam emails using various classifiers such as Logistic Regression, Naive Bayes, and SVM, Random Forest, LSTM, and Bi-Map. LSTM and transformers as well. By using encoding and transformation from natural language processing as well as pre-processing. The accuracy of Bi-LSTM random classification was 97.30%. It outperformed previous models

Table 1: summary of related works

Authors	**Classifier**	**Accuracy**	**Data Set**
Hassanpur et al. [15]	Neural Network (NN)	over 96% accuracy	Open dataset
Egozi et al. [16]	Linear Kernel SVM	80% phishing, 95% legitimate	IWSPA competition dataset: Training - 3865 ham, 735 phishing; Testing - 3824 ham, 475 phishing. Sources: Wikileaks, SpamAssassin, Nazario, university IT websites, Dada engine-generated.
[17] Shajideen,N.M.et al. 2018	SVM, NB and J48.	94% accuracy achieved by SVM	3762 spam, 5172 ham.
[18] Saab et al. 2014	SVM, NB, LMSVM, Decision tree, ANN.	93% accuracy achieved by SVM	Spam base dataset of 4597
[19] Anshumaanmishra.et	RNN,LSTM, Bi-LSTM	97% accuracy achieved by Bi-LSTM	The dataset comprises 5171 valid and spam samples, with 75% utilized for training and 25% for testing. Approximately 3878 samples for training the model, and 1293 samples for testing.
[20] FARKHUND IQBAL,	BERT Unfreeze + LSTM	96%	The dataset contains benign and malicious emails, such as those from the Enron Corpora 2
[21] Isra'a AbdulNabi and Qussai Yaseen	BERT with BiLSTM	97.30%	Public datasets containing SPAM and HAM emails [23][24]
[22] Malhotra, P., & Malik, S.	LSTM, Bi-LSTM	98.5% accuracy achieved by SVM	Kaggle Spam Email Dataset[25]

3. The Proposed methodology

This section presents the proposed method and data collection and pre-processing.

3.1 Proposed Method

The method in this paper suggest to implement three transfer learning models such as; BERT, ALBERT, and RoBERTa, after amend them and prepare them for data set.

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

Figure (1) shows the general structure of the proposed method is as follows. Two sets of data were uploaded, one digital and the other textual, and they were processed and balanced in the pre-processing stage. Three models are used in this paper: BERT, ALBERT, and RoBERTa, and each of them was explained in the figure, where the challenge of digital data was addressed by converting it into text and then conducting training on it. This treatment achieved good results compared to previous work.

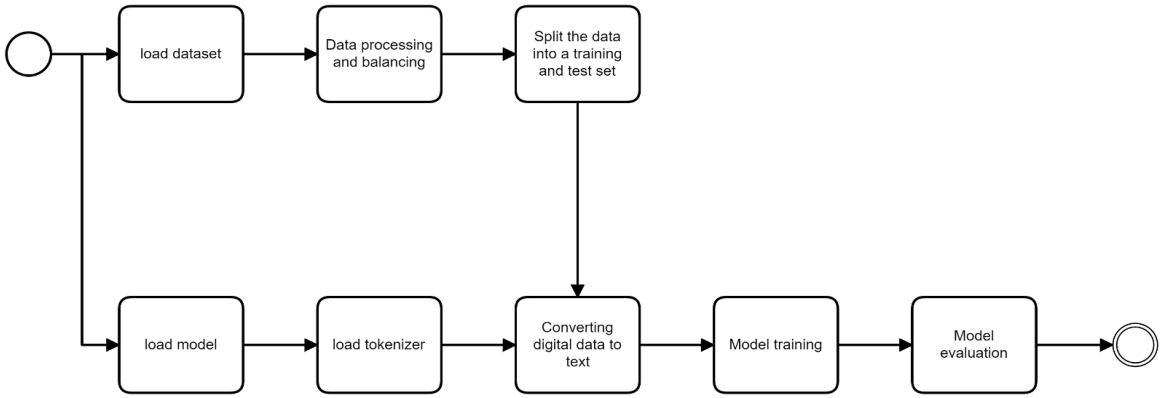

Figure 1. Shows those stages. Hence, in this work

3.2 Data Collection and Pre-Processing

Three open source datasets were used in this study, each consisting of two columns: the body text of emails and their corresponding category labels, either "spam" or "pork". The first dataset is obtained from the Spam base dataset, an open source available in the UCI Machine Learning Repository, which includes 5569 emails, of which 745 are classified as spam [23]. The second dataset is derived from the Kaggle spam filter dataset, which contains 5728 emails, of which 1368 are classified as spam [24]. When exploring the distribution of spam categories and garbage categories within the first and second datasets, it is clear that they are unbalanced, with spam being the minority category. To mitigate bias towards the majority class (pork), a balanced training dataset is created by processing and digitizing text data with the same number of features.

The first dataset consists of features of the text that were previously extracted, and to merge them with the second dataset, which is in text format, we have converted the text into features with the same number and order of features as the first dataset, and then we have balanced them .

The third dataset employed in this study originates from the Spam Email dataset on Kaggle, accessible at https://www.kaggle.com/datasets/venky73/spam-mails-dataset. This dataset encompasses 5171 messages, all tagged as either legitimate or non-legitimate [25].

Also, the third set of data was used, but it is not weighted, as ham = 3672, spam=1499 to solve the problem of imbalance in the third data set, use the down sampling method. Some records from the ham category are deleted so that they match the number of the minority category, i.e. spam. Thus, the data set consists of ham=1499 and spam=1499.

During the pre-processing stage, three sets of data, one numerical and one textual, underwent uploading, processing, and harmonization. To address the predicament associated with the textual data within the second set, it was digitized and subsequently amalgamated with the first set, which is numerical, while considering the quantity and configuration of attributes, following which the models were subjected to training.

4. Results and Discussion

This section presents results to evaluate the performance of transfer learning models on the datasets. In this paper, it has been used three transformation-based models (BERT, AlBERT, and RoBERTa). Also, it has been compared their performance with models (KNN, NB, BiLSTM, LSTM).

The datasets were divided into training and testing with different proportions to evaluate the performance of each set.

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

4.1 First and Second Dataset

We find that the proposed models performed better in almost measures when compared to the deferent models that used the same dataset. Table (2) and Fig. 2 show these results.

Table 2: Comparison results

Dataset	Model	Precision	Recall	F1-Measure	Accuracy
First and second dataset 70/30 %	[21] KNN	____	____	0.9081	0.9310
	[21] NB	____	____	0.9408	0.9540
	[21] BiLSTM	____	____	0.9556	0.9650
	[21]BERT with BiLSTM	____	____	0.9696	0.9730
	Proposed model BERT	**0.95**	**0.93**	**0.94**	**0.98**
	Proposed model AlBERT	**0.93**	**0.93**	**0.93**	**0.98**
	Proposed model RoBERTa	**0.98**	**0.94**	**0.93**	**0.98**

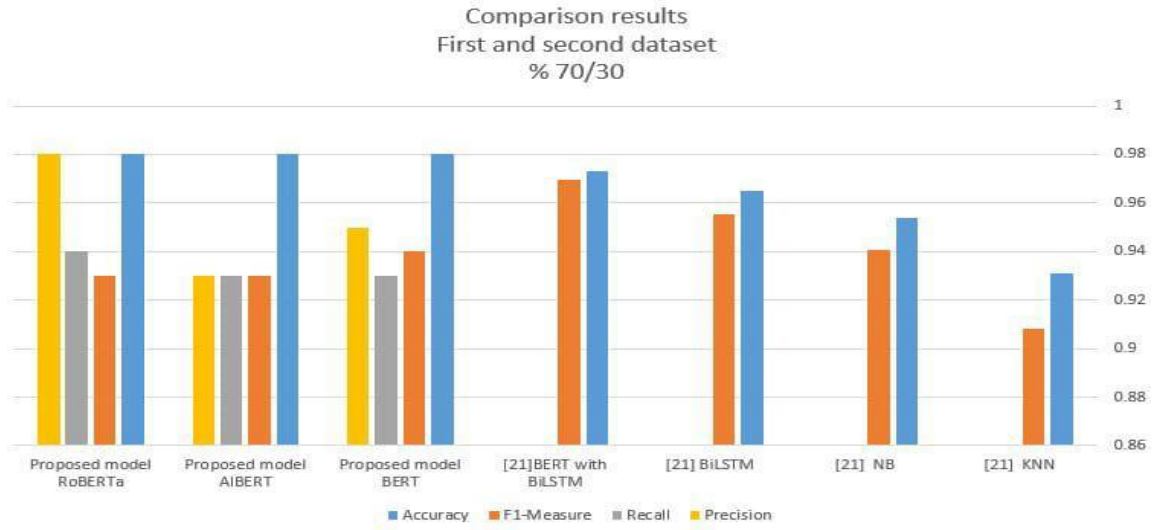

Figure 2. Comparison results first and second dataset

4.2 Third Dataset

The suggested models perform much better than traditional models on the majority of measures, according to a comparison with these models that used the same dataset. An explanation of the comparison is given in Table (3) and Fig. 3.

Table 3: Comparison results

Dataset	Model		Precision	Recall	F1-Measure	Accuracy
Third Dataset 80/20 %	[22] LSTM	Ham	0.98	0.92	0.95	0.983
		Spam	0.93	0.98	0.95	
	[22] BiLSTM	Ham	0.98	0.94	0.96	0.985
		Spam	0.94	0.94	0.96	
	Proposed model BERT		**0.99**	**0.99**	**0.99**	**0.990**
	Proposed model AlBERT		**0.99**	**1.0**	**0.99**	**0.991**
	Proposed model RoBERTa		**1.0**	**0.99**	**1.0**	**0.995**

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

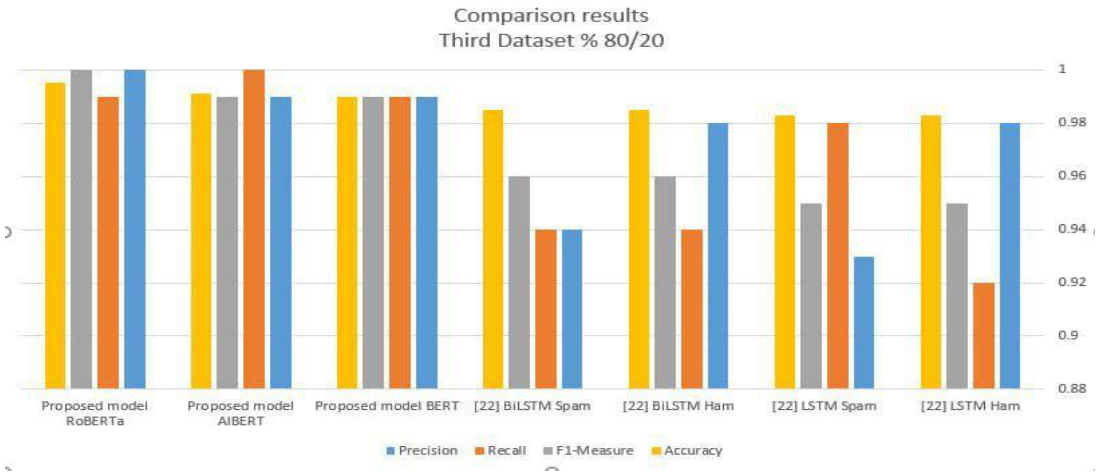

Figure 3. Comparison results third dataset

4.3 Overall Evaluation Results

Table (4) and Fig. 4 present the accuracy of various models on different datasets used for spam detection. Each model's performance is evaluated based on its accuracy, reflecting its ability to correctly classify spam and non-spam emails.

Table 4: Comparison with different Datasets

Model	Dataset	Accuracy
Neural Network (NN)[15]	Open dataset	96%
Linear Kernel SVM [16]	IWSPA competition dataset: Training - 3865 ham, 735 phishing; Testing - 3824 ham, 475 phishing. Sources: Wikileaks, SpamAssassin, Nazario, university IT websites, Dada engine-generated.	80% phishing, 95% legitimate
SVM[17]	3762 spam, 5172 ham.	94%
SVM[18]	Spam base dataset of 4597	93%
Bi-LSTM[19]	The dataset comprises 5171 valid and spam samples, with 75% utilized for training and 25% for testing. Approximately 3878 samples for training the model, and 1293 samples for testing.	97%
BERT Unfreeze + LSTM [20]	The dataset contains benign and malicious emails, such as those from the Enron Corpora 2	96%
BERTwith BiLSTM [21]	dataset is from the UCI Spam Base, with 5569 emails (745 spam), the Kaggle spam filter dataset, with 5728 emails (1368 spam)	97.30%
BiLSTM [22]	the Spam Email dataset from Kaggle [25].	98.5%
proposed model BERT	First and second dataset: dataset is from the UCI Spam Base, with 5569 emails (745 spam), the Kaggle spam filter dataset, with 5728 emails (1368 spam) .	98%
proposed model AlBERT		98%
proposed model RoBERTa		98%
proposed model BERT	Third dataset the Spam Email dataset from Kaggle [25].	99%
proposed model AlBERT		99.1%
proposed model RoBERTa		99.5%

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

The results demonstrate that transformer-based models (BERT, AlBERT, RoBERTa) exhibit the highest accuracy, particularly RoBERTa, which achieves 99.5%. Traditional machine learning models such as Naive Bayes and SVM also perform well but generally achieve lower accuracy compared to deep learning models.

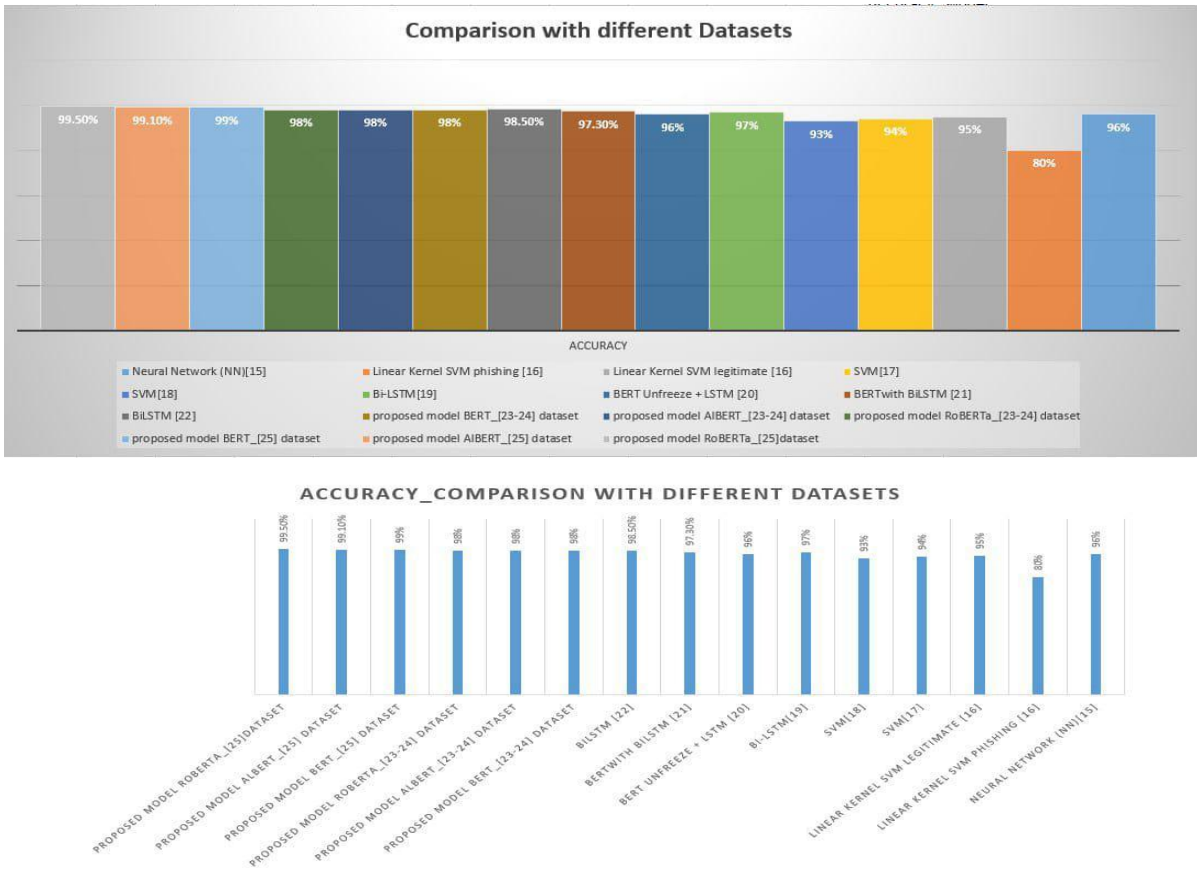

Figure 4. Comparison with different Datasets

In conclusion, while traditional models provide solid performance, the advanced deep learning and transformer-based models significantly enhance spam detection accuracy, demonstrating the ongoing evolution and improvement in this field.

5. Conclusion

This research shows that transformation-based models such as BERT, AlBERT, and RoBERTa are more successful when it comes to textual data when compared to traditional models such as KNN, NB, BiLSTM, and LSTM. It refers to the ability of modern models to understand complex data through contextual embedding and significantly improve performance on data sets, whether textual or converted to digital format. Modern models excel in most metrics such as Precision, Recall, F1-Measure and Accuracy. By addressing the challenges of converting digital data to text and using advanced techniques, significant improvements in classification accuracy and effectiveness can be achieved. The study recommends further research into improving these models and using them in various practical applications to achieve better results. The investigation indicates that the use of transformation-based models has the potential to yield significant improvements in classification accuracy and context understanding, thereby recommending additional research in this area to apply these models to a wider range of datasets and applications.

Funding: "This research received no external funding"

Conflicts of Interest: "The author declare no conflict of interest."

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

References

[1] Mohammed, M.A., Ibrahim, D.A. and Salman, A.O., 2021. Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language. Journal of Intelligent Systems, 30(1), pp.774-792.

[2] Source of the provided text is an article titled "The Evolution of Email: From Simple Communication to Spam Combat," published on TechCrunch on March 15, 2023.

[3] Belinkov, Yonatan, and James Glass. "Analysis methods in neural language processing: A survey." Transactions of the Association for Computational Linguistics 7 (2019): 49-72.

[4] Devlin, Jacob, et al. "BERT: Pre-training of deep bidirectional transformers for language understanding." arXiv preprint arXiv: 1810.04805 (2018).

[5] Raffel, Colin, et al. "Exploring the limits of transfer learning with a unified text-to-text transformer." Journal of Machine Learning Research 22.140 (2021): 1-67

[6] Tida, V. S., & Hsu, S. (2022). Universal Spam Detection using Transfer Learning of BERT Model. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2202.03480

[7] Li, Y., & Zhao, H. (2020). BURT: BERT-inspired Universal Representation from Twin Structure. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2004.13947

[8] Li, Y., & Zhao, H. (2020). BURT: BERT-inspired Universal Representation from Twin Structure. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2004.13947

[9] Lan, Z., Chen, M., Goodman, S., Gimpel, K., Sharma, P., & Soricut, R. (2019). ALBERT: A lite BERT for self-supervised learning of language representations. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1909.11942

[10] Reusch, A., Thiele, M., & Lehner, W. (2021). An ALBERT-based Similarity Measure for Mathematical Answer Retrieval. Virtual Event, Canada. https://doi.org/10.1145/3404835.3463023

[11] Majumder, S., & Das, D. (2020). Rhetorical role labelling for legal judgements using ROBERTA. https://www.semanticscholar.org/paper/Rhetorical-Role-Labelling-for-Legal-Judgements-Majumder-Das/483a39b7953a88494d2ec65f53acaea91ae76eb0

[12] Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). ROBERTA: A robustly optimized BERT pretraining approach. https://www.semanticscholar.org/paper/RoBERTa%3A-A-Robustly-Optimized-BERT-Pretraining-Liu-Ott/077f8329a7b6fa3b7c877a57b81eb6c18b5f87de

[13] Pritzkau, A. (2021). NLytics at CheckThat! 2021: Multi-class fake news detection of news articles and domain identification with RoBERTa - a baseline model. https://www.semanticscholar.org/paper/NLytics-at-CheckThat!%C2%A02021%3A-Multi-class-fake-news-a-Pritzkau/898d3560f7d36dc84d8355ed7439c78c32068380

[14] Suwarningsih, W., Pramata, R. A., Rahadika, F. Y., & Purnomo, M. H. A. (2022). RoBERTa: language modelling in building Indonesian question-answering systems. Telkomnika, 20(6), 1248. https://doi.org/10.12928/telkomnika.v20i6.24248

[15] R. Hassanpour, E. Dogdu, R. Choupani, O. Goker, and N. Nazli, “Phishing e-mail detection by using deep learning algorithms,” in Proceed-ings of the ACMSE 2018 Conference, 2018, pp. 1–1.

[16] G. Egozi and R. Verma, “Phishing email detection using robust nlp techniques,” in 2018 IEEE International Conference on Data Mining Workshops (ICDMW), IEEE, 2018, pp. 7–12

[17] Shajideen, N.M., Bindu, V. (2018). Spam filtering: A comparison between different machine learning classifiers. 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 1919-1922. https://doi.org/10.1109/ICECA.2018.8474778

[18] Saab, S. A., Mitri, N., & Awad, M. (2014). Ham or Spam? A comparative study for some content-based classification algorithms for email filtering. Proceedings of MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference (pp. 339-343)

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024

[19] Anshumaanmishra, N., & VigneshwaranPandi, N. (2022). Classifications of E-MAIL SPAM using deep learning approaches. In Advances in parallel computing. https://doi.org/10.3233/apc220058

[20] Iqbal, F., Javed, A. R., Jhaveri, R. H., Almadhor, A., & Farooq, U. (2023). Transfer learning-based forensic analysis and classification of E-Mail content. ACM Transactions on Asian and Low-resource Language Information Processing. https://doi.org/10.1145/360459

[21] AbdulNabi, I., & Yaseen, Q. (2021). Spam email detection using deep learning techniques. Procedia Computer Science, 184, 853–858. https://doi.org/10.1016/j.procs.2021.03.107

[22] Malhotra, P., & Malik, S. (2022). Spam email detection using machine learning and deep learning techniques. Social Science Research Network. https://doi.org/10.2139/ssrn.4145123

[23] D. Dua and C. Graff, UCI machine learning repository, 2017. [Online]. Available: http://archive.ics.uci.edu/ml.

[24] karthick veerakumar, Spam filter, 2017. [Online]. Available:https://www.kaggle.com/karthickveerakumar/spam-filter.

[25] V. Metsis, I. Androutsopoulos and G. Paliouras, "Spam Filtering with Naive Bayes - Which Naive Bayes?" Proceedings of the 3rd Conference on Email and Anti-Spam (CEAS 2006), Mountain View, CA, USA, 2006. Available: https://www.kaggle.com/datasets/venky73/spam-mails-dataset

DOI: https://doi.org/10.54216/JCIM.150127
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 14, 2024