International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1195-1202
Journal homepage: http://iieta.org/journals/ijsse

Classification Model of Spam Emails Based on Data Mining – Deep Learning Techniques

Fryal Jassim Abd Al-Razaq[1*], Sura J. Mohammed[1], Mehdi Ebady Manaa[1,2], Safa Saad A. Al-Murieb[1], Hussein A.A. Al-Khamees[3]

[1] College of Information Technology, University of Babylon, Babel 51001, Iraq
[2] Intelligent Medical System Department, College of Sciences, Al-Mustaqbal University, Babel 51001, Iraq
[3] Computer Techniques Engineering Department, College of Engineering and Technologies, Al-Mustaqbal University, Babel 51001, Iraq

Corresponding Author Email: mahdi.ebadi@uomus.edu.iq

https://doi.org/10.18280/ijsse.140416

Received: 31 May 2024
Revised: 20 July 2024
Accepted: 1 August 2024
Available online: 30 August 2024

Keywords:
deep learning, spam emails, feature selection, machine learning, accuracy rate

ABSTRACT

Spam emails are unsolicited, unwanted emails that are usually sent in large quantities by advertisers and scammers. They are often sent for the purpose of promoting a product or service or for phishing, which is the attempt to obtain sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity in an electronic communication. Deep learning algorithms can be used to identify spam emails by analyzing large datasets of email messages and learning to recognize patterns and trends that are indicative of spam. For example, a deep learning algorithm could be trained on a dataset of spam and non-spam emails and then be able to identify spam emails with a high degree of accuracy based on the patterns and trends it has learned from the training data. For the current work, machine learning by using the random tree is used to determine the best features with the leading deep learning hybrid Deep Neural Network Convolution Neural Network (DNN-CNN) techniques in the field of disclosure of incidental messages (spam and non-spam). The results showed that a high accuracy rate (99.8%) was obtained comparing with minimum false positive rate to the other works.

1. INTRODUCTION

Electronic publications, digital libraries, electronic books, emails, news articles, and websites all contribute to the growing body of available electronic text content. The enormous increase in electronic documents necessitates the automatic classification or control of documents [1]. The practice of assigning a document to one or more predetermined classifications based on the content (text) of the document is known as categorizing. The need for tools to assist people in finding, sorting, and managing these materials is growing. As a result, academic research on the automatic categorization of text document collections is significant [2].

Historically, the early detection techniques of spam emails filtering have evolved early from rule-based systems to more advance machine learning techniques. Machine learning considers a computational model and the basic of the extract useful information from raw data. Machine learning techniques are classified into three main categories: classification, clustering, and association rules, used in spam emails detection. Classification models use various features of emails, including certain keywords, structure of the message, and sender information to classify emails to ham or spam. Emails are a popular choice for private and technical communications because they are an effective form of online communication that conserves resources and reduces communication time. Data mining plays an integral role in many fields, such as spam emails. Data mining is used to extract knowledge from raw data by using models, both supervised and unsupervised [2-4].

However, the proliferation of email has led to an increase in spam emails in recent years. A lot of emails are spam, which causes a number of issues when dealing with them. The biggest is the number of messages that are flooded with the incoming messages [5]. Scripts and other executable files found in spam may contain malware that can damage a user's machine [6]. Spam messages have a number of drawbacks, including decreased productivity, reduced mailbox space, the spread of viruses, Trojan horses, and resources that may contain information that is harmful to some users, the compromise of the stability of mail servers, and the need for users to spend time sorting through and deleting unwanted mail. Because individuals receive such a large volume of spam email, it poses a hazard to organizations in addition to its being an annoyance [7]. A spam classification system that can discriminate between spam and non-spam messages will be created to solve this issue [8]. Numerous strategies, such as data mining with deep learning techniques, will be used in our proposed system for spam classification. The objective of the proposed work is to classify the emails received by implementing data mining with deep learning techniques. Objectives can be divided into the following [9]:

1. To classify large sets of emails.

2. To implement a hybrid method based on deep learning DNN-CNN.
3. To save bandwidth consumption and make secure online communication.
4. To find out a good performance information of accuracy.

2. RELATED WORKS

A significant study in spam emails detection has been conducted. The spam dataset from the email machine learning repository [10] is used in this study to analysis various categorization methods using data mining and deep learning [11].

To choose the pertinent characteristics of classification in this job, feature selection must first be completed [12]. Fifteen alternative classification techniques are chosen for evaluation after feature extraction [13]. Different features are taken into account when determining the best spam filtering algorithm in this evaluation procedure [14]. The best and optimal classifier for spam emails is chosen after careful analysis of the different categorization techniques [15]. Therefore, deep learning algorithms can be a powerful tool for identifying spam emails, and they can be used in conjunction with other data mining techniques to more effectively filter spam emails and protect individuals and organizations from unwanted and potentially harmful emails. The most related works in terms of classification of spam emails based on data mining and deep learning techniques have been discussed and reviewed as follows:

Hassan and Mtetwa [16] employed NB and SVM machine learning techniques, in conjunction with distinct feature extraction methods, to implement two supervised machine learning classifiers. The classifiers are then assessed using four performance metrics on two publicly available spam email datasets, with the aim of enhancing spam filtering. The importance of accurately pairing feature extraction and classifiers has been emphasized.

Ohnishi and Yoshida [17] used spam email categorization techniques such as: NB, TF-IDF, K-NN, and SVM by applying many machine learning techniques to different parts of spam email categorization in terms of performance accuracy. The primary aim of this study is to integrate the TF-IDF and NB techniques to attain optimal categorization accuracy. The study determined that the integration of diverse learning algorithms resulted in an accuracy rate of 90%.

The data mining ontology was utilized for the purpose of eliminating spam and unsolicited bulk email from the system, as it was specifically designed for this task [18]. The employed classifiers include a neural network (NN), support vector machine (SVM), Naive Bayes (NB), and J48 classifiers. The results indicated that a high level of accuracy was achieved when utilizing a dataset consisting of 1,000 tuples. The J48 classifier yielded an accuracy of 95.80%, while the NN classifier achieved 93.50% accuracy, the SVM classifier achieved 92.70% accuracy, and the NB classifier achieved the highest accuracy of 97.20%.

Yu and Xu [19] proposed a framework of using four different classifiers for spam classification: NB, NN, SVM, and relevance vector machine (RVM). They highlighted the potential effectiveness of these approaches for identifying spam emails, where experimental results showed that, as a spam rejection tool, the NN classifier is unsuitable for use on its own.

Different algorithms are used, such as: ID3, J48, Simple CART, and alternating decision trees [20] to classify the spam email dataset. Classification accuracy is used as the basis for comparison between the four algorithms. ID3, CART, and AD tree are outperformed by the J48 classifier in terms of classification accuracy.

A random boost method is applied to compare the performance of small-number-of-examples-trained robust and efficient spam detection filters [21]. TREC and CEAS are used as challenging spam application domains. The results showed that the random boost method, in comparison to the Logit Boost algorithm, dramatically improved the performance of the spam filter.

A comprehensive survey of text classification algorithms is done, including support vector machines (SVMs), decision trees, and rule-based classifiers [22]. In this survey, the authors discussed the various approaches that have been developed for text classification and highlighted the strengths and weaknesses of each approach.

Deep neural networks for spam email classification are implemented by using independent classifiers for analyzing both the text and images in an email message and then, combining the results of these classifiers using two hybrid multi-modal architectures [23].

The artificial neural network was used to predict whether an email is spam or not, and the overall results showed an accuracy rate of 85.31% [24]. This study demonstrated the effectiveness of the use of artificial neural networks in the classification of e-mails.

The performance of many different classifiers was compared, the authors included random forest (RF), artificial neural networks (ANN), logistic regression, support vector machine (SVM), random tree, K-nearest neighbor (KNN), decision table, Bayes net, Naive Bayes (NB), radial basis function (RBF), using 10-fold mutual verification to evaluate their accuracy [25]. The results showed that the random forest classifier was the best with an accuracy of 95.45%. The accuracy of other classifiers ranged from 82.6% (RBF) to 95.4% (RF). In this research, they suggested that the jungle random classifier is an excellent option for classifying spam email and that it surpassed other classifiers in terms of accuracy.

The integration of the random forest algorithm with deep neural networks (DNNs) for classifying spam was discussed in the study [26]. The random forest algorithm was used to rank the importance of various features, and then train a deep neural network classifier using the features with the highest rating. The results showed that the combination of the random forest algorithm and deep neural networks achieved an accuracy of 88.59% for classifying spam, which is better than other classifiers such as: K-nearest neighbours (KNN) and support bus machine (SVMs). In general, their work suggested that this approach represented a promising direction for future research in the spam classification.

The proposed approach explored the practical applications of deep learning techniques using spam filtering, malware detection and adult content filtering [27]. Long-Short-Term-Memory (LSTM) and Deep Neural Network (DNN) are used for spam filtering in an effective manner. The results achieved an Area Under the ROC curve (AUC) greater than 0.94 for spam filtering. DNN neural network employed high accuracy for malware detection. CNN combined with transfer learning techniques are utilized for content filtering highlighting the benefits of pre-trained models for image classification tasks.

The results performance in terms of cost and effectiveness is achieved by deep learning, which showed straightforward powerful solution for cybersecurity detection and spam email classification.

3. THE PROPOSED METHODOLOGY

The suggested system's design is made up of many steps that work together to provide a model for classifying emails. The flow chart in Figure 1 depicts the system architecture as well as the general processes to categories email. A dataset is an email that has been obtained from the Internet and is ready to be utilized in this work. To make the procedure easier in the next phases, the first stage marks the removal of the punctuation and the white space. The fourth stage, which includes split data for the training and testing sets, and the final stage is model extraction, where the neural network is trained to extract the classification system.

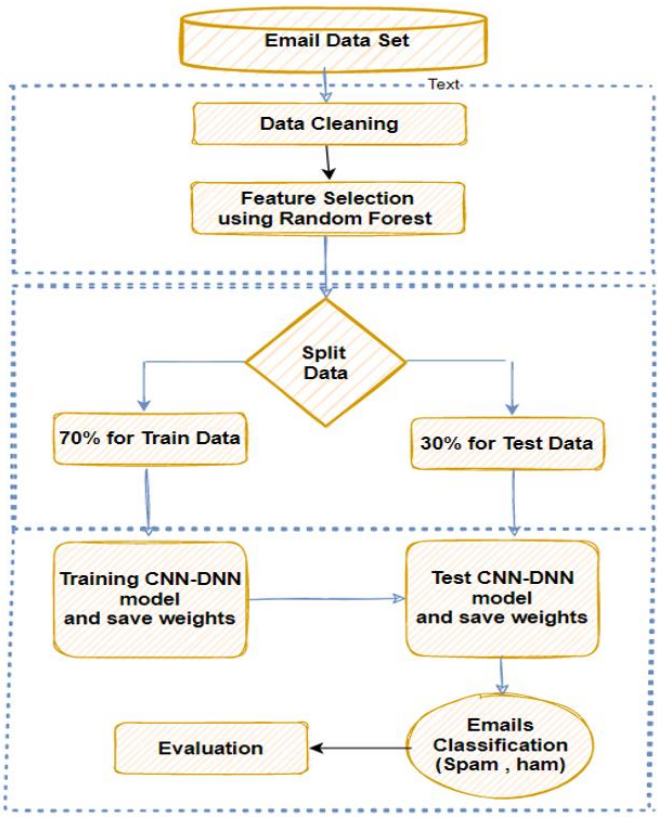

Figure 1. The proposed system of deep learning

3.1 Data set feature and description

Kaggle is a database for machine learning. The present study employed a dataset comprising a CSV file with 5,172 rows, where each row pertains to an email within the dataset. The sum of the features is 3,002. The initial column exhibits the nomenclature of the electronic mail. To ensure confidentiality, numerical identifiers have been used in lieu of personal names for the purpose of identification. The ultimate column of the dataset designates the prediction labels as either 1 for the spam or 0 for the non-spam (ham emails). The 3,000 features that remain represent the top 3,000 most commonly occurring words in all emails, following the removal of non-alphabetic characters and words. The dataset is comprised of a tabular structure where each row corresponds to a distinct email message and each column denotes a specific attribute of the email. The data can be scrutinized and manipulated efficiently as it is stored in a unified and condensed format. Consequently, the entirety of the 5,172 emails has been amalgamated into a solitary, condensed data frame, as opposed to being individually stored in separate emails.

Table 1 shows the snapshot distinct features for these numerical values of spam emails [28].

Table 1. The dataset feature escription

Email Name	Most Common Word#1 "the"	Most Common Word#2 "ect"	…	Most Common Word#3002 "dry"	Prediction Class (0 for Not Spam, 1 for Spam)
Email1	0	0	…	0	0
Email2	8	13	…	0	0
Email3	0	0	…	0	0
Email4	0	5	…	0	0
Email5	7	6	…	0	0
Email6	4	5	…	0	1
…	…	…	…	…	…
Email 5,172	22	24	…	0	0

Table 1 in above shows the main count for each distinct feature for each email. The last column shows the prediction class. Column #1 to column#3002 are used for training and testing of hybrid DNN-CNN deep learning.

3.2 Feature selection

There are some important steps in preparing the data for proper analysis. First, it is important to check the distribution of the data and make sure that it represents the target community. This may require data cleaning and removal of outliers or balanced sampling. Such actions help to obtain more reliable data for analysis. In this study, the dataset consisted of 3,000 features representing the most common words in emails. The random forest classification algorithm can be used to select the most important features, because it is able to detect patterns and trends in the data. Having identified the most important features, more accurate and efficient model can be built using only 500 features. The data set is divided into 70% for training and 30% for testing, weights are recorded and the model is memorized.

3.3 Deep learning

Neural networks can classify spam emails and do predictive analytics. They are particularly adept at learning complicated patterns and trends in data by adjusting the weights of neuronal connections based on input data [29]. Deep learning systems have outperformed the state-of-the-art on several machine learning tasks. An optimization approach is used to alter neuron weights to minimize the model's prediction error compared to the training data [30].

3.4 The components of DNN-CNN

The proposed model is designed by integrating two types of deep learning models characterized by their high ability in binary classification (DNN and CNN). The hybrid model consists of seven fully connected layers of the following sizes: (16, 32, 64, 128, 128, 64, 32, 64, 32) in three groups with size (0.2). The first four layers used to extract the best features from

the training data set of four-layer type "Conv1D" with 1D 32, 64, 32, 64, and 128 units. A global average pooling ID layer that down-samples the input by taking the maximum value as "dense" with 128, 64, 128, 64 and 32 units with the `ReLU` activation function, and finally the last layer is the output layer with 1 unit and the sigmoid activation function, which forecasts about the features. The architecture of the proposed hybrid model (DNN-CNN) is shown in Table 2.

Table 2. Summary of the proposed hybrid model (DNN-CNN)

conv1d_88 (Conv1D)	(None, 511, 16)	48
conv1d_89 (Conv1D)	(None, 510, 16)	528
max_pooling1d_44 (MaxPooling1D)	(None, 510, 16)	0
conv1d_90 (Conv1D)	(None, 509, 32)	1,056
conv1d_91 (Conv1D)	(None, 508, 32)	2,080
max_pooling1d_45 (MaxPooling1D)	(None, 508, 32)	0
conv1d_92 (Conv1D)	(None, 507, 64)	4,160
conv1d_93 (Conv1D)	(None, 506, 64)	8,256
max_pooling1d_46 (MaxPooling1D)	(None, 506, 64)	0
conv1d_94 (Conv1D)	(None, 505, 128)	16,512
conv1d_95 (Conv1D)	(None, 504, 128)	32,896
max_pooling1d_47 (MaxPooling1D)	(None, 504, 128)	0
flatten_11 (Flatten)	(None, 64512)	0
dense_42 (Dense)	(None, 128)	825,766 4
dropout_31 (Dropout)	(None, 128)	0
dense_43 (Dense)	(None, 64)	8,256
dropout_32 (Dropout)	(None, 64)	0
dense_44 (Dense)	(None, 32)	2,080
dropout_33 (Dropout)	(None, 32)	0
dense_45 (Dense)	(None, 1)	33

Algorithm 1. DNN-CNN model-training and testing
Input: df: Data of most relevant features
L: number of deep learning layers
Output: Trained DNNs Model
Begin
1 df= read (data)
2 For i =1 to L do
Create DNN-CNN (Create seven laters of deep neural networks)
3 Train the DNN-CNN on train-df and test-df
4 Evaluated DNN-CNN by calculating the confusion matrix parameters
5 Save train model DNN-CNN
End

Algorithm 2. The proposed system-training
Input: $\boldsymbol{f(xi)}$ // features vectors for features in email Data set
Output: Trained (DNN-CNN)
Begin
1 Let n number of Email groups in dataset
2 Call RandomForestClassifier (to choose the best features)
Call algorithm 1 // Create hybrid model (Create seven layers of DNN-CNN)
3 Split data to TRD(70%) and TED (30%) TRD split real training 70% and TSD validation 30%
4 Train the hybrid model (DNN-CNN) on email
5 Save weights hybrid model (DNN-CNN)
End

3.4.1 Training model and testing model

A hybrid deep neural network (CNN-DNN) is a model whose objective is to train the network to find a spam pattern to classify it. For network training, training data must be provided. Therefore, this model uses the email dataset. The model system's testing phase includes technical research and emails that are not labelled, as opposed to the emails used in the training phase. To save time, take up less memory, and produce better outcomes with high accuracy, the model system's key attributes are designed to work rapidly. Only one unlabeled email may be used during the testing phase before it is returned to the appropriate class. The main components and architecture of CNN-DNN can be found in algorithm 1, while algorithm 2 shows the deep neural network model training.

The last phase of this work includes six evaluation metrics that have been used for experimental results [31].

- Accuracy: It is a measure of the performance of a predictive model, and it is typically used to evaluate the ability of the model to correctly classify new data. To calculate the accuracy of the current model, we apply Eq. (1):

$$Accuracy = \frac{number\ of\ correct\ prediction}{total\ number\ of\ prediction} \quad (1)$$

- Recall: It is the model's genuine positive prediction rate compared to the dataset's actual positive cases. We use Eq. (2) to calculate model recall:

$$\text{Recall}= \frac{TP}{TP+FN} \quad (2)$$

- Precision: Correct positive results divided by the predicted number of positive results from the classifier. The exact computation can be seen in Eq. (3):

$$\text{precision}=\frac{TP}{TP+FP} \quad (3)$$

- F_1-score: It assesses a prediction model's accuracy and recall. It is the harmonic mean of accuracy and recall in classification problems. F_1-score is 0-1. The following Eq. (4) calculates a model's F_1-score:

$$\text{Recall}=\frac{2*precision*recall}{precision+recall} \quad (4)$$

- Detection rate (DR): It measures recognized positive (anomaly) cases from all positive ones, which is used in anomaly detection. Eq. (5) computes this measure:

$$\text{Detection rate (DR)}=\frac{TP}{TP+FN} \quad (5)$$

- False alert rate (FAR): Negative prediction percentage. Lower value is preferable. Eq. (6) computes this measure:

$$\text{False alert rate (FAR)}=\frac{FP}{FP+TN} \quad (6)$$

4. RESULTS AND DISCUSSION

The preprocessing phase is applied to the email dataset before the data is entered into the training phase of the proposed model. All emails entering the proposed system must go through the preprocessing phase, whether they are in the training phase or the testing phase. The output of this phase involves selecting the most important and best of those features to train the proposed deep model, and the Random Forest classifier is adopted for this task. After identifying the most important and best training features, the data set was divided into 70% for training and 30% for testing. The overall system performance is evaluated by the performance of the verification model based on the testing dataset. The metrics used to evaluate the verification model are confusion matric, accuracy, precision, recall, and F_1-measure, as described in formulas (1) to (6). Table 3 shows the main metrics for the proposed system with epochs number (25). Accuracy rate is of 96.25% after 25 epochs for training phase.

Figure 2 shows the training accuracy, loss function using CNN-DNN deep learning for 25 epochs.

Table 3. The performance metrics of the proposed system with epochs=25

Metric	Evaluate Results (%)
Accuracy	96.65
Precision	92.79
Recall	96.05
F1-score	94.39

Confusion matrix for training phase is presented in Table 4.

The training phase results are presented below for (50) epochs in Table 5. It is clearly shown that the accuracy rate is 95.55% and less false rate.

Figure 3 shows the training accuracy, loss function, and false alarm rate for training phase using CNN-DNN deep learning for 50 epochs.

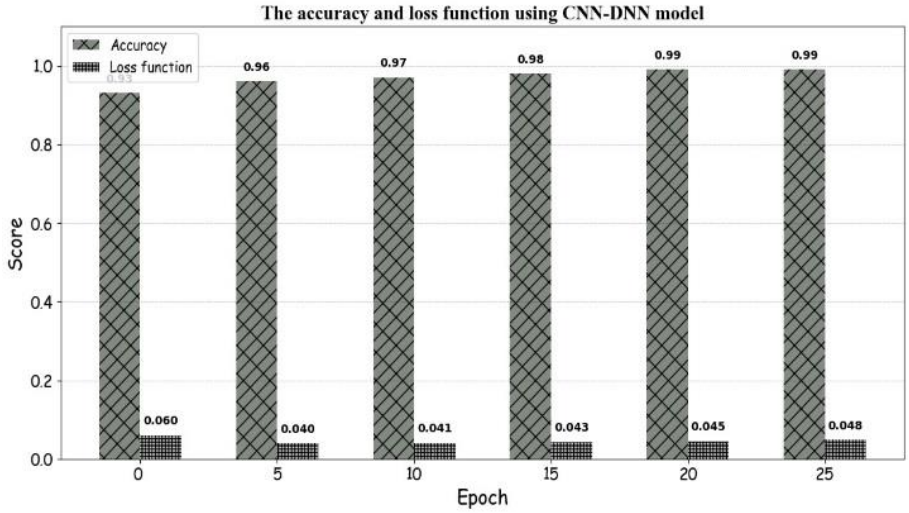

Figure 2. The training accuracy and loss function to the proposed model with 25 epochs

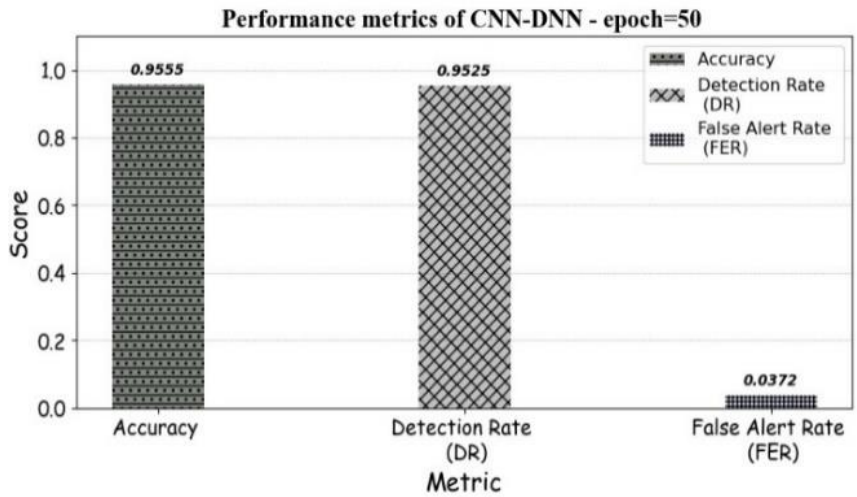

Figure 3. The training accuracy and loss function to the proposed model with 50 epochs

Table 4. Confusion matrix for spam/ham detection at 25 epochs using DNN-CNN

Confusion (Spam/Ham)	Predicted Spam	Predicted Ham
Actual spam	1,015	35
Actual ham	87	2,473

Table 5. The performance metrics of the proposed system with epochs=50

Metric	Evaluate Results (%)
Accuracy	95.55
Precision	89.41
Recall	96.27
F1-score	92.71

While Table 6 illustrates the confusion matrix for training phase.

Table 6. Confusion matrix for spam/ham detection at 50 epochs using DNN-CNN

Confusion (Spam/Ham)	Predicted Spam	Predicted Ham
Actual spam	1,004	46
Actual ham	113	2,447

The training phase results for (75) epochs are presented in Table 7.

Table 7. The performance metrics of the proposed system with epochs=75

Metric	Evaluate Results (%)
Accuracy	96.19
Precision	93.05
Recall	94.08
F1-score	93.56

Figure 4 shows the training accuracy, loss function and false alarm rate for training phase using CNN-DNN deep learning for 75 epochs.

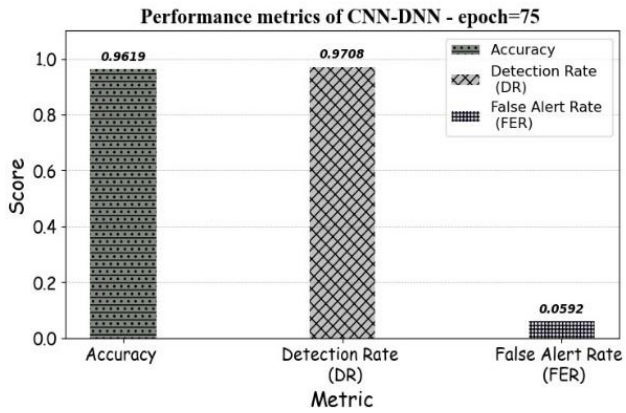

Figure 4. The training accuracy and loss function to the proposed model with 75 epochs

Confusion matrix for training phase with epochs 75 is presented in Table 8.

Table 8. Confusion matrix for spam/ham detection at 75 epochs using DNN-CNN

Confusion (Spam/Ham)	Predicted Spam	Predicted Ham
Actual spam	1,010	40
Actual ham	97	2,463

After finding the results of the models (epochs = 25, 50, and 75) and comparing them, we find that the good accuracy at epochs = 75 is more accurate in detecting spam. The proposed model reaches and records a classification accuracy of 99.8 in testing phase with minimum false alarm rate.

Confusion matrix for testing phase is presented in Table 9.

Table 9. Confusion matrix for spam/ham detection at 75 epochs using DNN-CNN for testing phase

Confusion (Spam/Ham)	Predicted Spam	Predicted Ham
Actual spam	1,048	2
Actual ham	5	2,555

However, the comparison of the performance of the proposed work with some other existing works using Kaggle datasets with different accuracy values is shown in Table 10.

Table 10. Comparison between verification accuracy of the proposed approach and other methods (testing phase)

Ref.	Technique	Accuracy (%)
[18]	NN	93.4
	SVM	90.87
	NB	96.47
	J48	97.56
[25]	RF	95.45
	ANN	92.41
	LR	92.41
	SVM	91.89
	Random tree	91.58
	K-NN	90.78
	Decision table	90.3
	Bayes net	89.8
	NB	89.85
	RBF	82.61
[26]	DL	88.59
[32]	LR	96.16
	CNN	96.39
	RF	88.69
	RNN	87.93
	LST	78.66
	DNN-BILSTM	98.69
[33]	NB	92.8
	DT	96.7
	LR	98.1
	AdaBoost	94.7
	K-NN	66.9
Our proposed system	RF + CNN +DNN hybrid classifier	**99.8**

From Table 10, we infer that the proposed model achieves the best accuracy with 99.8% that highlights in bold font. As a result, the proposed method outperforms the other works.

5. CONCLUSIONS

Spam emails are a pervasive problem in the digital age, often sent by advertisers and scammers for the purpose of promoting a product, service, or phishing. However, deep learning algorithms can be effectively utilised to identify and filter out spam emails by analysing patterns and trends in large datasets of email messages. The implication of this study using of random trees to determine the best features, in combination with leading deep learning techniques, has resulted in a highly accurate method for distinguishing between spam and non-spam emails thereby improving user experience and reducing the risks associated with phishing and other malicious

activities, with an accuracy rate of 99.8%. As such, deep learning algorithms offer a promising approach to combating the growing problem of spam emails and improving email communication for individuals and businesses alike, but with the limitation of dataset that may not fully represent the diversity of spam emails in real word. For future work, we need to incorporate more diverse and up-to date datasets which could enhance the model generalization.

ACKNOWLEDGMENT

The authors would like to express our deepest gratitude to the Al-Mustaqbal University and the College of Information Technology at the University of Babylon for their invaluable support in the publication of this paper.

REFERENCES

[1] Kadhim, A.I. (2019). Survey on supervised machine learning techniques for automatic text classification. Artificial Intelligence Review, 52(1): 273-292. https://doi.org/10.1007/s10462-018-09677-1

[2] Nicholas, N.N., Nirmalrani, V. (2024). An enhanced mechanism for detection of spam emails by deep learning technique with bio-inspired algorithm. e-Prime – Advances in Electrical Engineering, Electronics and Energy, 8: 100504. https://doi.org/10.1016/j.prime.2024.100504

[3] Hassan, K.F., Manaa, M.E. (2022). Detection and mitigation of DDoS attacks in Internet of Things using a fog computing hybrid approach. Bulletin of Electrical Engineering and Informatics, 11(3): 1604-1613. https://doi.org/10.11591/eei.v11i3.3643

[4] Qi, J., Du, J., Siniscalchi, S.M., Ma, X., Lee, C.H. (2020). Analyzing upper bounds on mean absolute errors for deep neural network-based vector-to-vector regression. IEEE Transactions on Signal Processing, 68: 3411-3422. https://doi.org/10.1109/TSP.2020.2993164

[5] Perazzini, S., Metulini, R., Carpita, M. (2023). Integration of flows and signals data from mobile phone network for statistical analyses of traffic in a flooding risk area. Socio-Economic Planning Sciences, 90: 101747. https://doi.org/10.1016/j.seps.2023.101747

[6] Dhivya, N., Banupriya, S. (2020). Network security with cryptography and steganography. International Journal of Engineering & Research Technology, 8(3): 1-4.

[7] Soomro, Z.A., Shah, M.H., Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2): 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[8] Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38: 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[9] Ayodele, T., Zhou, S., Khusainov, R. (2010). Email classification using back propagation technique. International Journal of Intelligent Computing Research, 1(1): 3-9. https://doi.org/10.20533/ijicr.2042.4655.2010.0001

[10] Lakshmi, R.D., Radha, N. (2010). Supervised learning approach for spam classification analysis using data mining tools. International Journal on Computer Science and Engineering, 2(8): 2760-2766.

[11] Souza, J.T.D., Francisco, A.C.D., Piekarski, C.M., Prado, G.F.D. (2019). Data mining and machine learning to promote smart cities: A systematic review from 2000 to 2018. Sustainability, 11(4): 1077. https://doi.org/10.3390/su11041077

[12] Dewangan, D.K., Gupta, P. (2018). Email spam classification using support vector machine algorithm. International Journal for Research in Applied Science and Engineering Technology, 6(6): 6-10. https://doi.org/10.22214/ijraset.2018.6002

[13] Ranjan, R., Sankaranarayanan, S., Castillo, C.D., Chellappa, R. (2017). An all-in-one convolutional neural network for face analysis. In 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), Washington, DC, USA, pp. 17-24. https://doi.org/10.1109/FG.2017.137

[14] Ruder, S. (2017). An overview of gradient descent optimization algorithms (arXiv:1609.04747). arXiv. https://doi.org/10.48550/arXiv.1609.04747

[15] Kingma, D.P., Ba, J. (2017). Adam: A method for stochastic optimization (arXiv:1412.6980). arXiv. https://doi.org/10.48550/arXiv.1412.6980

[16] Hassan, M.A., Mtetwa, N. (2018). Feature extraction and classification of spam emails. In 2018 5th International Conference on Soft Computing & Machine Intelligence (ISCMI), Nairobi, Kenya, pp. 93-98. https://doi.org/10.1109/ISCMI.2018.8703222

[17] Ohnishi, K., Yoshida, K. (2004). A constructive approach to creating a method for generating images. In Fourth International Conference on Hybrid Intelligent Systems (HIS'04), Kitakyushu, Japan, pp. 346-351. https://doi.org/10.1109/ICHIS.2004.2

[18] Youn, S., McLeod, D. (2007). Spam email classification using an adaptive ontology. Journal of Software, 2(3): 43-55. http://doi.org/10.4304/jsw.2.3.43-55

[19] Yu, B., Xu, Z. (2008). A comparative study for content-based dynamic spam classification using four machine learning algorithms. Knowledge-Based Systems, 21(4): 355-362. https://doi.org/10.1016/j.knosys.2008.01.001

[20] Sharma, A.K., Sahni, S. (2011). A comparative study of classification algorithms for spam email data analysis. International Journal on Computer Science and Engineering, 3(5): 1890-1895.

[21] DeBarr, D., Wechsler, H. (2012). Spam detection using random boost. Pattern Recognition Letters, 33(10): 1237-1244. https://doi.org/10.1016/j.patrec.2012.03.012

[22] Aggarwal, C.C., Zhai, C. (2012). A survey of text classification algorithms. In: Mining Text Data. Springer, Boston, MA, pp. 163-222. https://doi.org/10.1007/978-1-4614-3223-4_6

[23] Seth, S., Biswas, S. (2017). Multimodal spam classification using deep learning techniques. In 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Jaipur, India, pp. 346-349. https://doi.org/10.1109/SITIS.2017.91

[24] Alghoul, A., Al Ajrami, S., Al Jarousha, G., Harb, G., Abu-Naser, S.S. (2018). Email classification using artificial neural network. International Journal of Academic Engineering Research, 2(11): 8-14.

[25] Bassiouni, M., Ali, M., El-Dahshan, E.A. (2018). Ham and spam e-mails classification using machine learning

techniques. Journal of Applied Security Research, 13(3): 315-331. https://doi.org/10.1080/19361610.2018.1463136

[26] Jain, G., Sharma, M., Agarwal, B. (2019). Spam detection in social media using convolutional and long short term memory neural network. Annals of Mathematics and Artificial Intelligence, 85(1): 21-44. https://doi.org/10.1007/s10472-018-9612-z

[27] Miranda-García, A., Rego, A.Z., Pastor-López, I., Sanz, B., Tellaeche, A., Gaviria, J., Bringas, P.G. (2024). Deep learning applications on cybersecurity: A practical approach. Neurocomputing, 563: 126904. https://doi.org/10.1016/j.neucom.2023.126904

[28] Email Spam Classification Dataset CSV. Available: https://www.kaggle.com/datasets/balaka18/email-spam-classification-dataset-csv.

[29] Abbas Al-Khamees, H.A.A., Al-A'araji, N., Al-Shamery, E.S. (2023). Enhancing the stability of the deep neural network using a non-constant learning rate for data stream. International Journal of Electrical and Computer Engineering (IJECE), 13(2): 2123-2130. https://doi.org/10.11591/ijece.v13i2.pp2123-2130

[30] Alkhamees, H., Al-Jwaid, W., Al-Shamery, E. (2022). The impact of using convolutional neural networks in COVID-19 tasks: A survey. International Journal of Computing and Digital Systems, 11(1): 1157-1165. https://doi.org/10.12785/ijcds/110194

[31] Manaa, M.E., Hussain, S.M., Alasadi, S.A., Al-Khamees, H.A. (2024). DDoS attacks detection based on machine learning algorithms in IoT environments. Inteligencia Artificial, 27(74): 152-165. https://doi.org/10.4114/intartif.vol27iss74pp152-165

[32] Krishnamoorthy, P., Sathiyanarayanan, M., Proença, H.P. (2024). A novel and secured email classification and emotion detection using hybrid deep neural network. International Journal of Cognitive Computing in Engineering, 5: 44-57. https://doi.org/10.1016/j.ijcce.2024.01.002

[33] Adnan, M., Imam, M.O., Javed, M.F., Murtza, I. (2024). Improving spam email classification accuracy using ensemble techniques: A stacking approach. International Journal of Information Security, 23(1): 505-517. https://doi.org/10.1007/s10207-023-00756-1