Equilibrium Optimizer with Deep Learning Model for Detecting SMS Spam

Asma Ibrahim Gamar Eldeen, Ikhlas Saad Ahmed, Nahla O. A. Mustafa, Amel Mohamed Essaket Zahou, Amal Abdallah AlShaer

Department of Computer Science, Applied College, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia,
Email: aieldeen@iau.edu.sa

Abstract

Despite the proliferation of messages sent over the Internet, text messaging is still used as a communication service. Smartphone users often suffer from unwanted text messages that may contain fraudulent links. This study presents a novel approach that combines the Equilibrium Optimizer (EO) algorithm with a Deep Learning model for detecting SMS spam messages. The proposed method aims to enhance the performance of spam classification by leveraging the optimization capabilities of the EO algorithm and the powerful feature representation of Deep Learning models. The EO algorithm is utilized to optimize the training process of the Deep Learning model, enabling it to effectively learn and classify spam messages from legitimate ones. Experimental results on a real-world SMS spam dataset demonstrate the effectiveness of the proposed approach in achieving high accuracy and robust spam detection performance. The integration of the EO algorithm with Deep Learning models offers a promising solution for improving SMS spam detection systems and combating the increasing threat of spam messages in mobile communication networks.

Keywords: Equilibrium Optimizer; SMS Spam; Deep learning; Detecting; Artificial intelligence.

1. Introduction

The Short Message Service (SMS) provides a service for sending short text messages (160 characters) via phone. The Global System first used it for Mobile Communication (GSM). Due to the widespread use of mobile phones, the SMS service has grown due to its use by millions of mobile phone users. Spam has become a widespread problem that threatens users' privacy and the security of their data due to the risk of phishing and fraud[1]. Every day, more companies discover that the existence of a means that enables establishing a special relationship directly with the customer via mobile phone enables speedy communication from customers and speedy delivery of advertisements and offers.[2]. SMS has emerged as one of the most important wireless services. SMS is used in mobile marketing campaigns, which is profitable for phone companies and advertisers [3].

Spam is the process of spreading unwanted and irrelevant content, and it may be observed in many areas such as e-mail, SMS, websites, Internet telephony, etc.[4]

Spammers are people who want to make quick money who use the same spamming techniques until they are stopped by anti-spam software. They use different Internet addresses with different email accounts so they can bypass firewalls.[5]

2. Literature Review

2.1 AI studies

The study of [6] proposed a model for classifying e-mail messages using machine learning. Two data sets were used to test the model. The model showed satisfactory results in terms of accuracy compared to other recent models. The proposed model has three outputs a CSV file with the spam email IP addresses (of originating email servers), a map with their geolocation, as well as a CSV file with statistics about the countries of origin. In [7] they presented a mixed approach to classifying spam messages based on the Neural Network model Paragraph Vector-Distributed Memory (PV-DM). This approach is considered a more comprehensive candidate for classifying spam, as it showed results superior to the results of the filter PV-DM and the BOW email classification methods.

In [8] The Dense Network, Long Short-Term Memory (LSTM), and Bi-directional Long Short-Term Memory (Bi-LSTM) models were used to predict whether a text message was important or random. The results showed that the Dense Network model was the best because it gave a loss of 14.22%. and an accuracy of 95.63%. The study of [9] used Deep Machine Learning Techniques to create a model to classify SMS messages from a data set containing 5574 messages. Test results for the model showed an accuracy of up to 99.82.

The study [10] proposed a modified transformer model to detect spam. The model was evaluated on an SMS Spam Collection v.1 dataset and UtkMl’s Twitter Spam Detection Competition dataset, and the model achieved accuracy results on accuracy, recall, and F1-Score with the values of 98.92%, 0.9451, and 0.9613, respectively.

2.2 AI NN(RNN) studies

In the study [11]These messages are primarily intended to distribute emails for commercial or financial gain. This study proposes an approach that uses machine learning techniques to address spam SMS messages. The approach involves various components, including datasets, data cleaning, exploratory data analysis, and feature engineering. The ultimate goal of spam detection is to protect users from spam-related issues.

In this study [12] , extensive experiments were conducted on diverse datasets to evaluate the performance of the system across multiple metrics, including accuracy, precision, recall, and computational efficiency. The results demonstrate the effectiveness of the approach in accurately identifying spam messages while minimizing false positives. Moreover, the system is scalable and adaptable to dynamic spam techniques, making it suitable for real-time deployment. The study emphasizes the role of AI and machine learning in combating SMS spam, ensuring a secure and hassle-free communication environment for mobile users worldwide.

In this study[13] , a new method using RNN is proposed to classify spam and junk mail with sequences of varying lengths, despite using a fixed sequence length. The proposed study achieved a significant improvement, with an accuracy of 98.11.

In this study[14], the original SMS spam repository database was used, and after pre-processing and discrimination, specialized machine learning methods and algorithms were applied to the information base.

3. Proposed Model

In this paper, we proposed a model for identifying and classifying spam messages. The model includes three stages: the data preprocessing stage, the spam recognition stage, and finally the control stage.

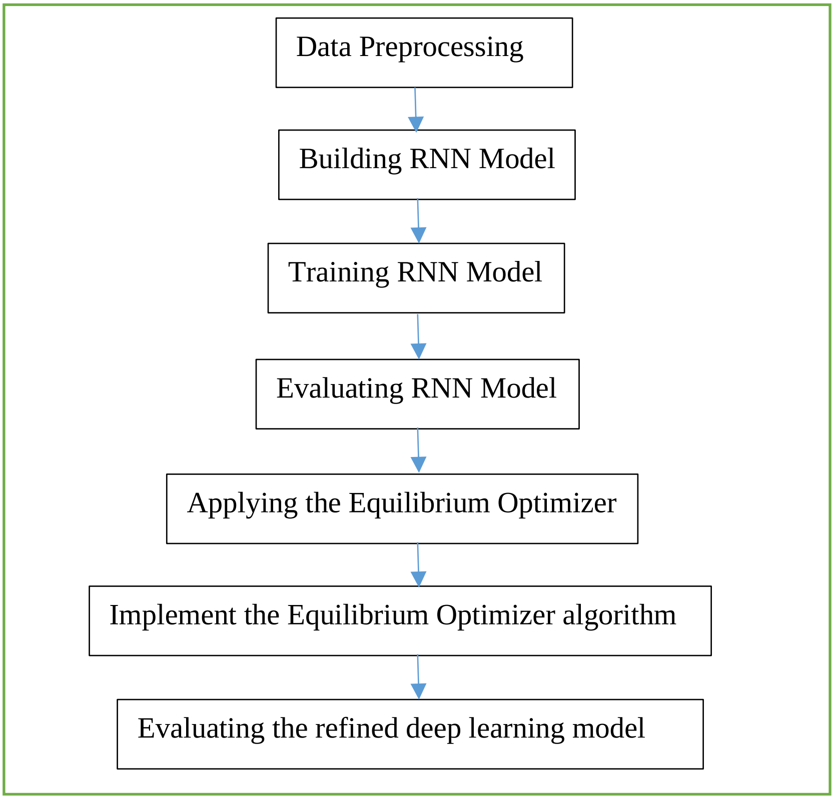

Data Preprocessing
Building RNN Model
Training RNN Model
Evaluating RNN Model
Applying the Equilibrium Optimizer
Implement the Equilibrium Optimizer algorithm
Evaluating the refined deep learning model

Figure.1 proposed model

3.1 Preprocessing the data:

Collect a labeled dataset of Android messages, where each message is labeled as either spam or not spam. Preprocess the data by performing tokenization, removing stop words, and vectorizing the messages to numerical representations.

a. Load the SMS dataset, which should contain a collection of labeled SMS messages (spam or non-spam).

b. Perform any necessary data preprocessing steps, such as removing stopwords, tokenizing the text, and converting it into numerical representations suitable for deep learning models.

c. Split the dataset into training and testing sets.

3.2 Building the deep learning model:

Choose a deep learning architecture suitable for text classification, such as a recurrent neural network (RNN), a convolutional neural network (CNN), or a combination of both (e.g., an LSTM-CNN model).

Define the layers of the model, including embedding layers, recurrent or convolutional layers, and fully connected layers.

Compile the model with an appropriate loss function (e.g., binary cross-entropy) and optimizer (e.g., Adam).

3.4 Training the deep learning model:

Fit the model to the training data, specifying the number of dataset and size. Monitor the training progress, including the loss and accuracy on the training set.

3.5 Evaluating the deep learning model:

Evaluate the trained model on the testing set to measure its performance.

Calculate metrics such as accuracy, precision, recall, and F1 score to assess the model's ability to classify spam and non-spam messages.

2. Equilibrium Optimizer:

Implement the Equilibrium Optimizer algorithm. The EO algorithm involves maintaining a population of candidate solutions and iteratively updating them based on the equilibrium concept. The algorithm aims to find the optimal solution by balancing exploration and exploitation.

3. Applying the Equilibrium Optimizer:

After training the deep learning model, you can apply the Equilibrium Optimizer algorithm to fine-tune the model's parameters further.

Initialize the Equilibrium Optimizer and specify the hyperparameters, such as the population size, maximum iterations, and convergence criteria.

Implement the Equilibrium Optimizer algorithm to optimize the model's parameters. This can involve adjusting the weights and biases of the deep learning model based on the Equilibrium Optimizer's search strategy.

Iterate the Equilibrium Optimizer algorithm until convergence or a specified number of iterations.

4. Evaluating the refined deep learning model:

After applying the Equilibrium Optimizer, evaluate the refined deep learning model on the testing set.

Compare the performance of the refined model with the original model to assess any improvements.

We used Accuracy, Precision, Recall, and F1 Score to evaluate the performance of the study model. Accuracy is the percentage of samples that the model was able to classify correctly.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \qquad (1)$$

Precision is the quality of a positive prediction made by the model

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \qquad (2)$$

Recall measures how many positive samples were correctly classified

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \qquad (3)$$

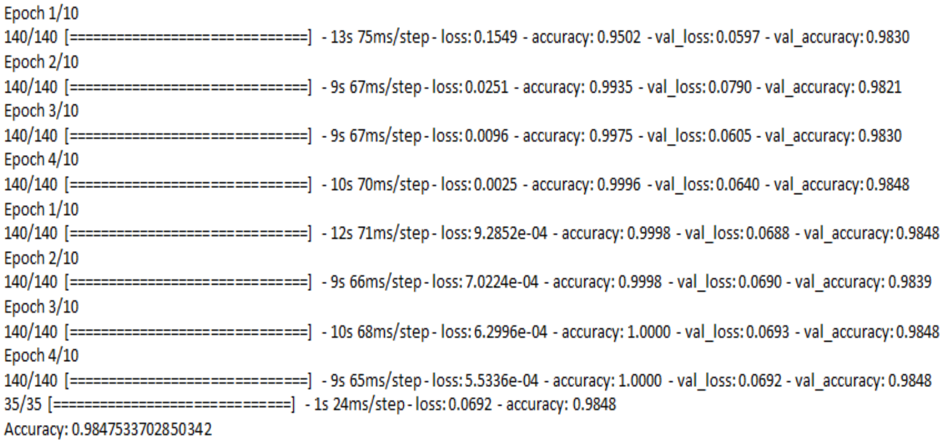
F1 Score integrates precision and recall into a single metric to gain a better understanding of model performance.

$$\text{F1} = \frac{2 \times \text{Percision} \times \text{Recall}}{(\text{Percision} + \text{Recall})} \qquad (4)$$

4. Result and Discussion

This study evaluates the performance of spam detection model and others models designed for SMS spam detection. The proposed model utilizes a comprehensive dataset features, and then underwent training and evaluation on the same dataset,

In Figure 3 and 4, an extensive comparison result of the proposed model is provided . The results indicate proposed model based on accuracy is 9847% whereas Naive Bayes Accuracy: 0.97847533632287, Multilayer Perceptron Accuracy: 0.979372197309417 and Decision Tree Accuracy: 0.9704035874439462



```
Epoch 1/10
140/140 [============================] - 13s 75ms/step - loss: 0.1549 - accuracy: 0.9502 - val_loss: 0.0597 - val_accuracy: 0.9830
Epoch 2/10
140/140 [============================] - 9s 67ms/step - loss: 0.0251 - accuracy: 0.9935 - val_loss: 0.0790 - val_accuracy: 0.9821
Epoch 3/10
140/140 [============================] - 9s 67ms/step - loss: 0.0096 - accuracy: 0.9975 - val_loss: 0.0605 - val_accuracy: 0.9830
Epoch 4/10
140/140 [============================] - 10s 70ms/step - loss: 0.0025 - accuracy: 0.9996 - val_loss: 0.0640 - val_accuracy: 0.9848
Epoch 1/10
140/140 [============================] - 12s 71ms/step - loss: 9.2852e-04 - accuracy: 0.9998 - val_loss: 0.0688 - val_accuracy: 0.9848
Epoch 2/10
140/140 [============================] - 9s 66ms/step - loss: 7.0224e-04 - accuracy: 0.9998 - val_loss: 0.0690 - val_accuracy: 0.9839
Epoch 3/10
140/140 [============================] - 10s 68ms/step - loss: 6.2996e-04 - accuracy: 1.0000 - val_loss: 0.0693 - val_accuracy: 0.9848
Epoch 4/10
140/140 [============================] - 9s 65ms/step - loss: 5.5336e-04 - accuracy: 1.0000 - val_loss: 0.0692 - val_accuracy: 0.9848
35/35 [============================] - 1s 24ms/step - loss: 0.0692 - accuracy: 0.9848
Accuracy: 0.9847533702850342
```

Figure.2 Proposed model Accuracy result

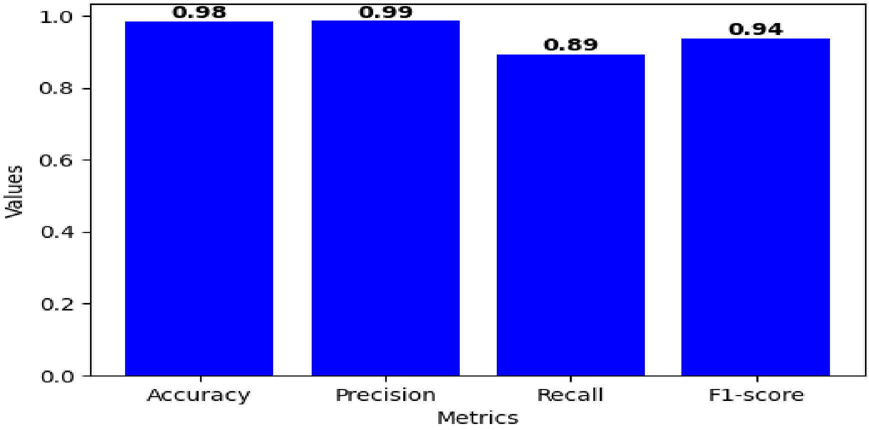


Figure.3 Evaluation measures comparison

Table 3 Evaluation measures comparison results of the proposed model for the detection of SMS spam

Techniques	Accuracy	Precision	Recall	F1 Score
Dataset	0.98	0.99	0.89	0.94

Table 4 Evaluation measures comparison results of the Naive Bayes Classification of SMS spam

Techniques	Accuracy	Precision	Recall	F1 Score
Data set	0.97	0.99	0.99	0.99

Table 5 Evaluation measures comparison results of the Multilayer Perceptron Classification of SMS spam

Techniques	Accuracy	Precision	Recall	F1 Score
Data set	0.97	0.98	1.0	0.99

Table 6 Evaluation measures comparison results of the Decision Tree of SMS spam

Techniques	Accuracy	Precision	Recall	F1 Score
Data set	0.97	0.98	0.99	0.98

5. Conclusion

In this study, we have introduced a novel approach that combines the Equilibrium Optimizer (EO) algorithm with a Deep Learning model for detecting SMS spam messages. By leveraging the optimization capabilities of the EO algorithm and the feature representation power of Deep Learning models, we have demonstrated promising results in enhancing the performance of SMS spam classification.

Our experimental results on a real-world SMS spam dataset have shown that the proposed approach achieves high accuracy and robust spam detection performance compared to traditional methods. The integration of the EO algorithm into the training process of the Deep Learning model has enabled the model to effectively learn and distinguish spam messages from legitimate ones.

The findings of this study underscore the potential of combining metaheuristic optimization algorithms such as the EO algorithm with Deep Learning models for improving SMS spam detection systems. This hybrid approach offers a promising solution for addressing the growing challenge of spam messages in mobile communication networks and can be further extended and applied to other text classification tasks.

Future research directions may include exploring the adaptability of the proposed approach to different types of spam messages, optimizing hyperparameters of the EO algorithm for improved performance, and investigating the scalability of the model to larger datasets. Overall, the Equilibrium Optimizer with Deep Learning Model presents a valuable contribution to the field of spam detection and holds potential for enhancing the security and efficiency of communication systems.

WORKS CITED

[1] D. A. Oyeyemi and A. K. Ojo, “SMS Spam Detection and Classification to Combat Abuse in Telephone Networks Using Natural Language Processing,” Journal of Advances in Mathematics and Computer Science, vol. 38, no. 10, pp. 144–156, Oct. 2023, doi: 10.9734/jamcs/2023/v38i101832.

[2] M. Gutiérrez-Colon Plana, P. Gallardo Torrano, and M. E. Grova, “SMS as a learning tool: an experimental study,” The EuroCALL Review, vol. 20, no. 2, p. 33, Sep. 2012, doi: 10.4995/eurocall.2012.11376.

[3] J. Brown, B. Shipman, and R. Vetter, “SMS: The short message service,” Computer (Long Beach Calif), vol. 40, no. 12, pp. 106–110, 2007, doi: 10.1109/MC.2007.440.

[4] Gothenburg, “SHORT MESSAGE SERVICE (SMS) IN FIXED AND MOBILE NETWORKS,” 2004.

[5] D. Nagamalai, B. C. Dhinakaran, and J. K. Lee, “An In-depth Analysis of Spam and Spammers,” 2008.

[6] I. Moutafis, A. Andreatos, and P. Stefaneas, “Spam Email Detection Using Machine Learning Techniques.” [Online]. Available: https://www.abuseipdb.com

[7] Samira. Douzi, F. A. AlShahwan, Mouad. Lemoudden, and Bouabid. El Ouahidi, “Hybrid Email Spam Detection Model Using Artificial Intelligence,” Int J Mach Learn Comput, vol. 10, no. 2, pp. 316–322, Feb. 2020, doi: 10.18178/ijmlc.2020.10.2.937.

[8] A. Hikmaturokhman, H. Nafi’ah, S. Larasati, A. Wahyudin, G. Ariprawira, and S. Pramono, “Deep Learning Algorithm Models for Spam Identification on Cellular Short Message Service,” Journal of Communications, vol. 17, no. 9, pp. 769–776, Sep. 2022, doi: 10.12720/jcm.17.9.769-776.

[9] J. Palimote, V. I. E. Anireh, and N. D. Nwiabu, “A Model for Filtering Spam SMS Using Deep Machine Learning Technique,” IJARCCE, vol. 10, no. 4, Apr. 2021, doi: 10.17148/ijarcce.2021.10403.

[10] X. Liu, H. Lu, and A. Nayak, “A Spam Transformer Model for SMS Spam Detection,” IEEE Access, vol. 9, pp. 80253–80263, 2021, doi: 10.1109/ACCESS.2021.3081479.

[11] S. Menthe, K. Rawal, M. Hirave, and A. J. Patil, “SMS SPAM DETECTION USING MACHINE LEARNING,” IJARCCE, vol. 13, no. 3, Feb. 2024, doi: 10.17148/ijarcce.2024.13307.

[12] D. E. P, D. A. MCA Scholar, and A. Professor, “NEXT-GEN CYBERSECURITY: AI-POWERED SMS SPAM DETECTION,” 2024. [Online]. Available: www.ijnrd.org

[13] A. M. G, M. S. H, and A. Professor, “International Journal of Research Publication and Reviews SMS Classification and Spam Detection by Using RNN,” 2023. [Online]. Available: www.ijrpr.com

[14] M. A. Mukunthan, “SMS Spam Classifier Using Machine Learning,” 2023. [Online]. Available: www.ijrpr.com