

Improving spam email detection using deep recurrent neural network

Souad Larabi-Marie-Sainte¹, Sanaa Ghouzali², Tanzila Saba³, Linah Aburahmah¹, Rana Almohaini¹

¹Department of Computer Science, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia

²Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

³Artificial Intelligence and Data Analytics (AIDA) Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Oct 23, 2021

Revised Dec 26, 2021

Accepted Jan 13, 2022

Keywords:

Activation function

Deep learning

Email spam detection

Machine learning

Recurrent neural network

ABSTRACT

Nowadays the entire world depends on emails as a communication tool. Spammers try to exploit various vulnerabilities to attack users with spam emails. While it is difficult to prevent spam email attacks, many research studies have been developed in the last decade in an attempt to detect spam emails. These studies were conducted using machine learning techniques and various types of neural networks. However, with all their attempts the highest accuracy acquired was 94.2% by random forest classifier. Deep learning techniques have demonstrated higher accuracy performance compared to the traditional machine learning algorithms. In this paper, deep recurrent neural network was used to determine whether an email is a spam email. After investigating different configurations for this method, the best setting that generated the highest accuracy was based on using Tanh as the activation function with the dropout rate equals to 0.1 and the number of epochs achieving 100. The proposed approach attained a high accuracy of 99.7% which surpassed the best accuracy (98.7%) obtained by the hybrid gated recurrent unit recurrent neural network approach.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Sanaa Ghouzali

Department of Information Technology, College of Computer and Information Sciences

King Saud University

Riyadh, Saudi Arabia

Email: sghouzali@ksu.edu.sa

1. INTRODUCTION

The email is one of the communication methods that has been frequently used by people in many fields such as education, business, and for personal matters. By 2025, the number of daily exchanged emails is expected to increase over 375 billion emails [1]. The reason for this widespread use is due to the effectiveness to satisfy the users' need, in addition to the fact that it is cost-free. Spam emails or unsolicited emails are known to be emails that advertise drugs, cheap mortgage rates, and items for sale. The average percentage of spam in global email traffic was 45,67% in Q1 2021 [2]. Sending millions of spams (through email and other messaging systems such that Youtube [3], [4]) is considered a lucrative business because the profit is still large even if a very small percentage of responses is received. These emails cause troubles for both users and internet services. Beyond just being annoying and disruptive, spam significantly reduces work productivity as users spend time checking and deleting these emails. Spam emails are also used to widely distribute malware as attachments with the aim to damage the user's data. Moreover, spam emails are used for social engineering attacks to steal user's confidential data. As for the internet service, spam emails impose significant cost on the network infrastructure needed to relay this traffic. Henceforth, an intensive protection

mechanism is required against spam emails. Most organizations install and monitor spam filters to block spam before it ever reaches the user. However, spammers continue to develop new sophisticated techniques to circumvent detection by spam filters, rendering the protection of email communications from spammers a very challenging task that needs a lot of work and improvements.

Various studies have been carried out to detect spam emails by experimenting the potential possibility of creating and applying different machine learning (ML) algorithms and models. Many comparative studies aimed to identify the best model that can produce the highest accuracy rate in detecting spam emails [5]-[7]. The highest achieved accuracy is 94.2% obtained by using the random forest classifier [7]. To enhance the performance of the machine learning (ML) algorithms, many studies combined them with bio-inspired algorithms, or artificial neural networks [8]-[10]. Particle swarm optimization (PSO) is among the most popular algorithms that has been used in spam email detection. However, ML techniques cannot handle a large dataset of millions records [11]. In addition, better results are only achieved after performing data preprocessing and dimensionality reduction. These two phases require more effort and time to be processed.

The main disadvantage of the ML methods is that they are unable to learn lower-level features contrary to the deep learning methods. Deep learning (DL) is one field of ML that involves using neural networks (NN) [12]. It has a high ability in learning from abstract features which eliminates the need for data processing and dimensionality reduction as it is the case with ML algorithms. The data pass through different hidden layers such that the information learned in the previous layer will serve future layers. DL techniques have demonstrated higher accuracy performance than the traditional ML algorithms especially when dealing with large datasets [13]. DL has been used in many applications such as speech recognition, visual recognition, and drug discovery [14]. Two DL techniques are widely used, namely recursive neural network (RNN) and convolution neural network (CNN). These techniques were recently used in spam detection for social media [13], [15], [16], but have not been widely used in the detection of the spam emails. In this paper, we take advantage from the capabilities of the RNN technique to enhance the detection of spam emails. Moreover, a comparison will be addressed with recent papers to evaluate the effectiveness of the proposed method using the SpamBase dataset.

This paper is organized as follows. An overview of the related works using DL approaches to spam detection is provided in section 2. Section 3 introduces the proposed technique. Section 4 addresses the experimental study, presents the results and the discussion. Finally, the conclusion is drawn in section 5.

2. RELATED WORKS

Recent studies have shown that deep learning outperforms the standard machine learning procedures to detect spam messages. In the paper, Mi *et al.* [17], realized the power of DL for email spam detection using stacked auto-encoder (SAE). Information gain (IG) and bag-of-words (BoW) are used to extract feature vectors from email samples. The experimental results on different benchmark databases such as PU1, PU2, PU3, PUA, and enron-spam, showed that the proposed approach achieved 97.02% average accuracy which outperformed traditional machine learning algorithms such naive bayes (NB), support vector machine (SVM), decision tree (DT), boosting, random forest, and traditional artificial neural network (ANN). The authors mentioned that the limitation of SAE is the running time. They encouraged to use other types of DL and to investigate the parameter setting to well enhance the performance and reduce the execution time.

In the paper, Barushka and Hajek [18], proposed a spam filter by combining an ngram TF-IDF feature selection, deep multi-layer perceptron NN and balancing distribution-based algorithm. The aim of using the balancing distribution-based algorithm is to overcome the imbalanced datasets. The experimentation was conducted on four spam databases, SpamAssassin, enron, social networking, and SMS spam. The proposed approach was successfully compared to spam filters existing techniques such factorial design using NB and SVM, random forest, minimum description length, voting and convolutional neural network (CNN). The proposed approach showed an accuracy of 98.76% and 99.89% using enron-spam and SpamAssassin dataset, respectively. The authors mentioned that the proposed approach cannot be used as an online spam filtering technique due to the high running time caused by the additional hidden layers.

In the paper, Chetty *et al.* [19], proposed a deep learning based spam detection model. This deep model has two architectures to deal with the numeric and text data respectively. The first architecture consists of an input layer that has 57 nodes, 2 hidden layers with 16 nodes each, followed by a dropout layer, and the output layer that has 1 node. The second architecture comprises the word embedding layer followed by pooling, dense and output layers. Both architectures used the rectified linear unit (ReLU) as the activation function for the dense layer, and Sigmoid function is chosen for the output layer. Adaptive moment estimation (ADAM) optimizer was employed along with the cross-entropy loss function. The model (with the first architecture) achieved 92.8% accuracy and 84.9% F1 score on SpamBase dataset. The authors did not

investigate the running time. However, they mentioned that the present model could be improved by exploring the parameter setting to find the best values that can eventually enhance its performance. They also advised to use other types of DL architectures.

In the paper, Alauthman [20], introduced a Bot spam email detection system by using gated recurrent unit recurrent neural network (GRU-RNN) with SVM. First, the CART algorithm was employed for feature reduction. GRU is then used to solve the gradient problem encountered in traditional RNN, allowing a faster training phase. The author used ADAM optimizer and the cross-entropy cost function. At the final step of the neural network, the prediction of the model is computed by employing the decision function of SVM. The approach in this study showed a detection rate of 98.7% when applying the minimum number of features using the SpamBase dataset. However, the DL related parameters were randomly set with no experimental analysis and the execution time was not shown. The author stated that the proposed model could be further improved by combining it with other ML techniques.

In the paper, Sumathi and Pugalendhi [21], and introduced a hybrid approach for spam detection using random forest and deep neural network (DNN). The random forest algorithm is used to select the important features with the gini measure. These features are then trained using DNN classifier. The authors used backpropagation with one hidden layer and 10 hidden nodes. They employed softmax as the loss function. However, they did not investigate the DL parameters to find the best values. Experimental results obtained on the SpamBase dataset showed that the classification rate of DNN outperformed K-nearest neighbor (K-NN) and SVM with an accuracy of 88.59% when only considering the top-ranked five features. The authors did not investigate the running time. They encouraged the use of bioinspired-based feature selection algorithms to enhance the accuracy instead of exploring the DL architectures and parameters.

In the paper, Hossain *et al.* [22], proposed some ML and DL techniques for spam detection model. Outliers are first removed from the dataset using Isolation Forest. The ML techniques were random forest, K-NN, and multinomial NB. While DL technique was based on RNN with one input/output layer. The number of the hidden layers was not set by the authors. The accuracy of 99.28% is achieved using RNN on SpamBase dataset. The authors showed that reducing the feature set can significantly reduce the running time for ML techniques. However, this hypothesis was not demonstrated when using RNN. They encouraged to use ensemble learning for spam detection.

In the paper, AbdulNabi and Yaseen [23], used word embedding and bidirectional encoder representations from transformers (BERT) to detect spam from text emails. They employed the attention layers to handle the texts. The parameters were set without valid investigation. The epochs number was set to 3, the batch size equaled to 32, the learning rate was set to 4e-5, and the optimizer to ADAM. The loss function is not defined. Two datasets (HAM and Spam) were merged and used to test and compare the proposed model against some ML techniques and Bidirectional long-short term memory (LSTM). The new model achieved an accuracy of 98.67%. The authors set the sequence to 300 tokens or words but stated that the results could be improved if the sequence is increased. They also encouraged exploring further spam detection in different languages, particularly in Arabic language.

In Baccouche *et al.* [24], proposed a new DL model to detect spam in social media and emails. They used a modified version of multi-label LSTM model and bigram to handle texts and extract the spam. Many layers were used such that the Embedding, LSTM, dense, fully connected and output layers. The softmax activation function was employed along with the cross-entropy loss function. The related parameters were defined but without a deep investigation of the optimal values. Two datasets (Fraud and Spam) were combined to validate the proposed model. The results demonstrated the effectiveness of this model in recognizing malicious text unrelatedly of the source. The accuracy achieved 92.7%. However, the authors did not show its performance in terms of running time.

To sum up, only few articles handling email spam detection based on DL were found. The authors employed Stacked auto-encoder, deep multi-layer perceptron, gated recurrent unit recurrent neural network, recurrent neural network, and LSTM. Contrary to the ML-based email spam detection studies (discussed in the introduction), DL is not well involved in this research field. Moreover, spam detection is mainly investigated in the social media [25] and SMS [26] using DL and ML. This study fills the gap found in this research area. Moreover, it presents a deep investigation of the parameter setting which was not done in the literature review.

3. RESEARCH METHODOLOGY

Deep learning methods have been deployed for detection of spam messages especially in social media. However, only few studies used deep learning for detecting spam emails. In this paper, the recurrent neural network is further investigated to improve the accuracy of spam emails detection.

3.1. Deep learning approach (DL)

Deep learning is a subfield of machine learning that was developed in the 1980s to enhance the ANN to be used in processing large datasets, owing to the availability of massive data and powerful computers. In the paper, Schmidhuber [12], Schmidhuber proposed a comprehensive survey on deep learning neural networks (DNN). These DNNs have many hidden layers that mimic the functionalities and the power of the human's brain. The number of hidden layers differentiates a simple NN from a DNN as shown in Figure 1 [27].

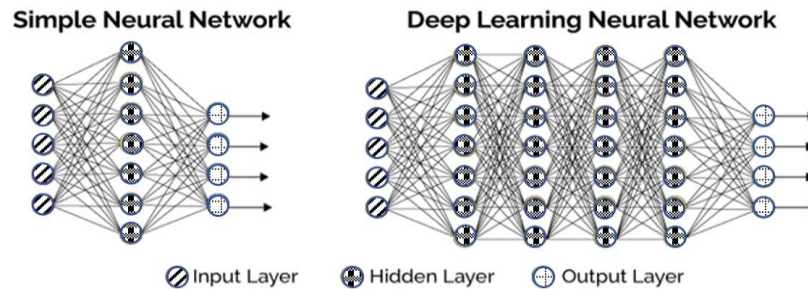


Figure 1. The difference between simple and deep learning neural networks [27]

3.2. Recurrent neural network (RNN)

In this study, RNN is used to process large dataset to classify the emails as spam or not spam. RNN is a supervised learning technique that mimics the short-term memory. The short-term memory is located at the frontal lobe part of the brain. The concept behind RNN is that it remembers the knowledge it learned from the previous observations. Then, it uses this knowledge as it moves forward. In the case of RNN, the hidden layers do not just produce outputs, but it also feedbacks itself as displayed in Figure 2. The RNN utilizes the power of short-term memory in processing the data [28].

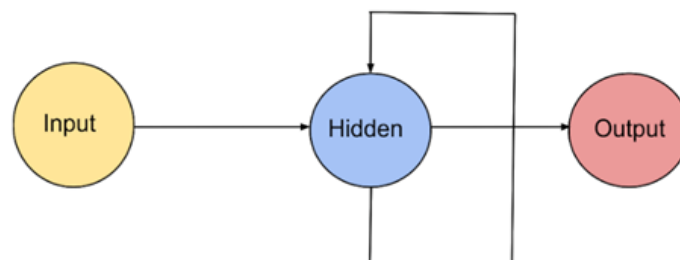


Figure 2. RNN simple structure

The neurons are connected to themselves through time. This represents the concept of having a sort of memory (short-term memory (STM)). The neurons can remember what was in them previously. The neuron learns from the previous observations and passes this knowledge to the next neurons. For example, when RNN is used for translating a sentence, the network needs to remember the translations of each word as it proceeds forward to understand the concept and therefore develop an accurate translation. There are different types of RNN: (a) "One-Many" which can be used when describing an image using different words, for example. The image is the input while the texts are the output. (b) "Many-One" which can be used in the semantic analysis such as analyzing if the text is positive or negative. The input, in this case, will be a group of texts while the output is one value as positive or negative. (c) "Many-Many" which is used in google translation for example, where different words in one language can be translated into another language [9].

RNN learns from the output generated from previous neurons. The time measured for the output to become the input is called timestep [29]. The inputs are the number of attributes. In RNN, the weights of the inputs are computed along with the previous output before applying the activation function. This output will be the input for the next layer. The number of iterations of all the training instances with one forward pass

and one backward pass is presented by the value of the epochs [30]. The hidden layer contains a set of neurons generated by using the (1).

$$N_h = N_s / (\alpha * (N_i + N_o)) \tag{1}$$

where N_i is the number of input neurons, N_o is the number of output neurons, N_s is the number of samples in training dataset, and α is an arbitrary scaling factor between 2 and 10 according to [31].

The hidden layer uses an activation function which transforms the input signal into an output to be used in the following layer. The most common types of activation functions are Sigmoid, ReLu, and Tanh. The Sigmoid activation function is defined in (2).

$$f(x) = 1 / (1 + \exp(-x)) \tag{2}$$

Its value ranges between 0 and 1 and represented as a S-shaped curve. The concept of the Sigmoid is easy to understand and apply. However, the generated outputs are not zero-centered and are plotted in a scattered manner making the optimization harder. Therefore, it causes a slow convergence rate which makes it less popular than the other functions [32].

Tanh solves the issue of centralizing the output to zero because the values range between -1 and 1. Hence, the optimization can happen easily [31]. The Tanh formula is defined in (3).

$$f(x) = 2 / (1 + \exp(-2x))^{-1} \tag{3}$$

The Sigmoid and Tanh functions suffer from the vanishing gradient problem. It is a problem associated with the selected activation function, where the parameters of the early layers in the NN becomes extremely small causing the accuracy of the prediction to drop [31]. However, ReLu overcomes the vanishing gradient problem and proved that it converges six times better than Tanh function which makes it the most common activation function used in DL [33]. The formula of the ReLu is defined in (4).

$$f(x) = \max(0, x) \tag{4}$$

Furthermore, the dropout rate is one of the parameters that can be used to enhance the performance of the neural networks. This is due to its ability to avoid the overfitting problem in NN and it ranges between 0 and 1 according to [34].

4. RESULTS AND DISCUSSION

In this study, the RNN was used to detect spam emails in the SpamBase dataset from the UCI Machine Learning Repository. The dataset has 57 attributes of 4601 email messages. Deep learning studio, which is an open-source tool for building deep learning networks, was used to train and test the data. Multiple experiments are done based on changing the activation function, the dropout rate, and the number of epochs as seen in Figure 3.

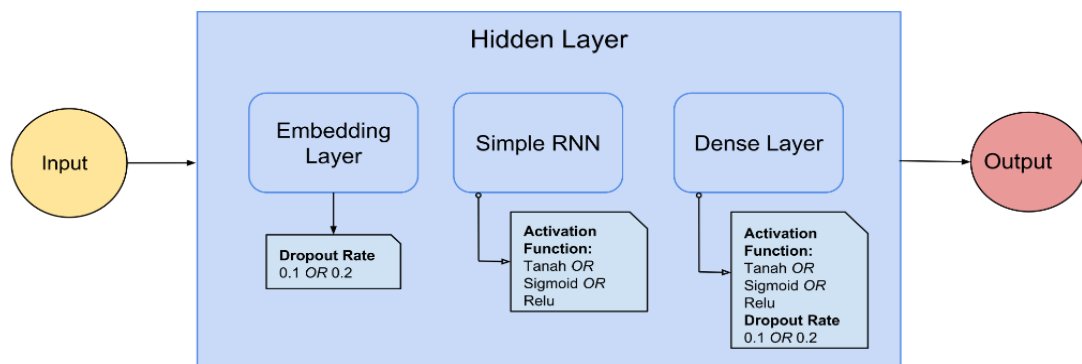


Figure 3. RNN Structure used in this study

The parameters providing the best results are selected for this experiment. The number of neurons in the input layer is equal to the number of the attributes. Three rounds are performed, each with four runs. In each round, the activation function is fixed while the epoch number and the dropout rate are changed. For the first round, the Tanh activation function is set. Then, for the first two runs, the dropout is equal to 0.1 while changing the epochs number for each run to 50 and 100, respectively. For the other remaining runs in the first round, the dropout rate is changed to 0.2, and the epochs number for each run is set to 50 and 100, respectively. The same process is repeated in the next two rounds while changing the activation function for each round. The dataset is divided into three sets as 80%, 10%, and 10% for the training, validation, and testing, respectively. The accuracy rate for the training and the validation is documented for all the runs. The testing accuracy is only mentioned for the highly performed run. The best accuracy result generated from the proposed model is compared with the accuracy of the recent papers that used the same dataset.

4.1. Experimental study

After implementing the RNN on the SpamBase dataset using different settings, the accuracy of the training and the validation are listed in Table 1. After using different activation functions to RNN, Tanh attained the highest results in the overall runs. The highest values achieved by Tanh was 97% and 99% for the training accuracy and the validation accuracy, respectively. To validate our model, testing dataset is used and attained an accuracy of 99.7%.

Table 1. Accuracy of RNN using different settings

Round #	Run #	Activation Function	Dropout Rate	Epochs	Training Accuracy	Validation Accuracy
1	1	Tanh	0.1	50	94%	98%
	2	Tanh	0.1	100	97%	99%
	3	Tanh	0.2	50	91%	94%
	4	Tanh	0.2	100	88%	90%
2	5	Sigmoid	0.1	50	91%	95%
	6	Sigmoid	0.1	100	91%	91%
	7	Sigmoid	0.2	50	88%	89%
	8	Sigmoid	0.2	100	90%	87%
3	9	ReLu	0.1	50	88%	94%
	10	ReLu	0.1	100	97%	96%
	11	ReLu	0.2	50	84%	85%
	12	ReLu	0.2	100	84%	98%

4.2. Comparative analysis

Many works have been carried out to improve the accuracy of spam emails detection. Most of these research studies combined models of ML, ANN, or Bio-Inspired algorithms. Several researchers provided the comparison between the different classifiers used in the literature. In Table 2, the result produced by the proposed RNN-DL approach is compared with the recent spam emails detection studies that used the SpamBase dataset.

The comparison study comprised three categories. The first category involves the comparison with ML based-related works. In this part, two well known ML techniques (rotation forest and bayesian logistic regression) [7] were compared with the proposed model. The second category encompasses the comparison with the hybrid studies based on ML and bio-inspired algorithms and/or neural networks. In this part, three related works were investigated. The first one was based on PSO and the decision tree J48 [8], the second tackled MLP neural network and biogeography-based optimization [9], while the last work proposed SVM-based PSO and MLP [10]. The third category includes the comparison with DL related works. In this part, four related works were used for comparison including CNN [19], GRU-RNN with SVM [20], random forest integrated with deep neural network [21], and RNN with isolation forest [22].

By referring to Table 2, the highest accuracy, using ML techniques, was 94.2% achieved by random forest (RF) for predicting the emails as spam or not spam. RF is a ML classifier that creates multiple decision trees based on a randomly selected subset. This method is popular in classification due to its performance to obtain a high accuracy [35]. Even though the ML techniques performed well on the SpamBase dataset, their accuracy could not beat the deep learning neural network. The majority of the results obtained from using RNN are more accurate than machine learning techniques as well as the multilayer neural network. An accuracy of 98.7% is the best obtained result using DL algorithm, which is achieved when combining gated recurrent unit recurrent neural network with SVM and employing the minimum number of features. In this study, the highest accuracy achieved by the proposed RNN is 99.7%. This drives the conclusion that RNN is effective in Spam detection especially when using the Tanh activation function with 100 epochs and dropout rate of 0.1.

Table 2. Comparison results against the state-of-the-art methods references

Category	Reference	Algorithm(s)	Accuracy
Machine Learning	[7]	Rotation Forest	94.2%
	[7]	Bayesian Logistic Regression	93.1%
Bio-inspired	[8]	PSO and the Decision Tree J48	98.3%
	[9]	MLP Neural Network and Biogeography Based Optimization	88%
	[10]	SVM-PSO & MLP for feature selection	93.07%
Deep Learning	[19]	Modified DL	92.8%
	[20]	GRU-RNN with SVM	98.7%
	[21]	Random Forest integrated with Deep Neural Network	88.59%
	[22]	RNN with Isolation Forest	99.28%
	Proposed Model	Customized RNN	99.7%

5. CONCLUSION

The power of deep learning techniques has been utilized in this study for the detection of spam emails. RNN is used with different configurations regarding the activation function, the number of epochs, and the dropout rate. The highest result is 99.7% which is obtained when setting the parameters with Tanh for activation function, 0.1 for the dropout rate, and 100 for the number of epochs. Moreover, the proposed scheme is compared with other studies that used SpamBase dataset. The proposed RNN has shown to outperform the best accuracy of 98.7% achieved by the approach combining Gated Recurrent Unit Recurrent Neural Network with SVM and employing the minimum number of features. The future direction of this study is to apply the long-short term memory (LSTM) in spam email classification. LSTM is a particular type of RNN that can generate better results.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of Prince Sultan University for paying the article processing charges (APC) of this publication. This work was also supported by artificial intelligence and data analytics lab (AIDA), Prince Sultan University, Riyadh, Saudi Arabia.




REFERENCES

- [1] J. Johnson, "Number of sent and received e-mails per day worldwide from 2017 to 2025." Oct. 2021, Accessed: Jan. 20, 2022. [Online]. Available: <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/>
- [2] T. Kulikova, T. Shcherbakova, and T. Sidorina, "Spam and phishing in Q1 2021 | Securelist." 2021, Accessed: Jan. 20, 2022. [Online]. Available: <https://securelist.com/spam-and-phishing-in-q1-2021/102018/>
- [3] N. M. Samsudin, C. F. B. Mohd Foozy, N. Alias, P. Shamala, N. F. Othman, and W. I. S. Wan Din, "Youtube spam detection framework using naïve bayes and logistic regression," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 3, pp. 1508–1517, Jun. 2019, doi: 10.11591/ijeecs.v14.i3.pp1508-1517.
- [4] N. Alias, C. F. M. Foozy, and S. N. Ramli, "Video spam comment features selection using machine learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 2, pp. 1046–1053, Aug. 2019, doi: 10.11591/ijeecs.v15.i2.pp1046-1053.
- [5] A. Al-Ajeli, R. Alubady, and E. S. Al-Shamery, "Improving spam email detection using hybrid feature selection and sequential minimal optimisation," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp. 535–542, Jul. 2020, doi: 10.11591/ijeecs.v19.i1.pp535-542.
- [6] A. Sharaff, N. K. Nagwani, and A. Dhadse, "Comparative Study of Classification Algorithms for Spam Email Detection," in *Emerging Research in Computing, Information, Communication and Applications*, Springer India, pp. 237–244, 2016.
- [7] S. M. Abdulhamid, M. Shuaib, O. Osho, I. Ismaila, and J. K. Alhassan, "Comparative Analysis of Classification Algorithms for Email Spam Detection," *International Journal of Computer Network and Information Security*, vol. 10, no. 1, pp. 60–67, Jan. 2018, doi: 10.5815/ijcnis.2018.01.07.
- [8] H. Kaur and A. Sharma, "Novel Email Spam Classification using Integrated Particle Swarm Optimization and J48," *International Journal of Computer Applications*, vol. 149, no. 7, pp. 23–27, Sep. 2016, doi: 10.5120/ijca2016911466.
- [9] A. Rodan, H. Faris, and J. Alqatawna, "Optimizing Feedforward Neural Networks Using Biogeography Based Optimization for E-Mail Spam Identification," *International Journal of Communications, Network and System Sciences*, vol. 09, no. 01, pp. 19–28, 2016, doi: 10.4236/ijcns.2016.91002.
- [10] M. Zavvar, M. Rezaei, and S. Garavand, "Email Spam Detection Using Combination of Particle Swarm Optimization and Artificial Neural Network and Support Vector Machine," *International Journal of Modern Education and Computer Science*, vol. 8, no. 7, pp. 68–74, Jul. 2016, doi: 10.5815/ijmecs.2016.07.08.
- [11] L. Bottou, F. E. Curtis, and J. Nocedal, "Optimization methods for large-scale machine learning," *SIAM Review*, vol. 60, no. 2, pp. 223–311, Jan. 2018, doi: 10.1137/16M1080173.
- [12] J. Schmidhuber, "Deep Learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, Jan. 2015, doi: 10.1016/j.neunet.2014.09.003.
- [13] G. Jain and B. Agarwal, "An Overview of RNN and CNN Techniques for Spam Detection in Social Media," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 10, p. 2277, 2016.
- [14] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
- [15] G. Jain, M. Sharma, and B. Agarwal, "Optimizing semantic LSTM for spam detection," *International Journal of Information Technology (Singapore)*, vol. 11, no. 2, pp. 239–250, Apr. 2019, doi: 10.1007/s41870-018-0157-5.




- [16] G. Jain, M. Sharma, and B. Agarwal, "Spam detection in social media using convolutional and long short term memory neural network," *Annals of Mathematics and Artificial Intelligence*, vol. 85, no. 1, pp. 21–44, Jan. 2019, doi: 10.1007/s10472-018-9612-z.
- [17] G. Mi, Y. Gao, and Y. Tan, "Apply stacked auto-encoder to spam detection," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9141, Springer International Publishing, pp. 3–15, 2015.
- [18] A. Barushka and P. Hajek, "Spam filtering using integrated distribution-based balancing approach and regularized deep neural networks," *Applied Intelligence*, vol. 48, no. 10, pp. 3538–3556, Mar. 2018, doi: 10.1007/s10489-018-1161-y.
- [19] G. Chetty, H. Bui, and M. White, "Deep learning based spam detection system," in *Proceedings - International Conference on Machine Learning and Data Engineering, iCMLDE 2019*, Dec. 2019, pp. 91–96, doi: 10.1109/iCMLDE49015.2019.00027.
- [20] M. Alauthman, "Botnet spam e-mail detection using deep recurrent neural network," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 5, pp. 1979–1986, May 2020, doi: 10.30534/ijeter/2020/83852020.
- [21] S. Sumathi and G. K. Pugalendhi, "Cognition based spam mail text analysis using combined approach of deep neural network classifier and random forest," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 5721–5731, May 2021, doi: 10.1007/s12652-020-02087-8.
- [22] F. Hossain, M. N. Uddin, and R. K. Halder, "Analysis of optimized machine learning and deep learning techniques for spam detection," Apr. 2021, doi: 10.1109/IEMTRONICSS2119.2021.9422508.
- [23] I. AbdulNabi and Q. Yaseen, "Spam email detection using deep learning techniques," *Procedia Computer Science*, vol. 184, pp. 853–858, 2021, doi: 10.1016/j.procs.2021.03.107.
- [24] A. Baccouche, S. Ahmed, D. Sierra-Sosa, and A. Elmaghraby, "Malicious text identification: Deep learning from public comments and emails," *Information (Switzerland)*, vol. 11, no. 6, p. 312, Jun. 2020, doi: 10.3390/info11060312.
- [25] P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS Spam," *Future Generation Computer Systems*, vol. 102, pp. 524–533, Jan. 2020, doi: 10.1016/j.future.2019.09.001.
- [26] G. Jain, M. Sharma, and B. Agarwal, "Spam Detection on Social Media Using Semantic Convolutional Neural Network," *International Journal of Knowledge Discovery in Bioinformatics*, vol. 8, no. 1, pp. 12–26, Jan. 2018, doi: 10.4018/ijkdb.2018010102.
- [27] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, Apr. 2017, doi: 10.1016/j.neucom.2016.12.038.
- [28] G. V. Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5929–5955, May 2020, doi: 10.1007/s10462-020-09838-1.
- [29] L. Castrejón, K. Kundu, R. Urtasun, and S. Fidler, "Annotating object instances with a polygon-RNN," in *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, vol. 2017-January, Jul. 2017, pp. 4485–4493, doi: 10.1109/CVPR.2017.477.
- [30] O. Mogren, "C-RNN-GAN: Continuous recurrent neural networks with adversarial training," Nov. 2016. Accessed: Jan. 20, 2022 [Online]. Available: <http://arxiv.org/abs/1611.09904>.
- [31] Z. C. Lipton, J. Berkowitz, and C. Elkan, "A Critical Review of Recurrent Neural Networks for Sequence Learning," May 2015. Accessed: Jan. 20, 2022 [Online]. Available: <http://arxiv.org/abs/1506.00019>.
- [32] R. Jozefowicz, W. Zaremba, and I. Sutskever, "An empirical exploration of recurrent network architectures," *32nd International Conference on Machine Learning, ICML 2015*, vol. 3, pp. 2332–2340, 2015.
- [33] B. Zoph and Q. V. Le, "Neural architecture search with reinforcement learning," *5th International Conference on Learning Representations, ICLR 2017 - Conference Track Proceedings*, Nov. 2017, [Online]. Available: <https://arxiv.org/abs/1611.01578v2>.
- [34] A. Pauls, "Determining Optimum Drop-out Rate for Neural Networks," *The Midwest Instruction and Computing Symposium*, p. 0–11, 2018.
- [35] M. Belgiu and L. Drăgu, "Random forest in remote sensing: A review of applications and future directions," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 114, pp. 24–31, Apr. 2016, doi: 10.1016/j.isprsjprs.2016.01.011.

BIOGRAPHIES OF AUTHORS







Souad Larabi-Marie-Sainte    earned her Ph.D. in AI from Computer Science Department, Toulouse1 University, France, in 2011. She was an Assistant Professor with the College of Computer and Information Sciences, King Saud University. She is currently an Associate Professor with the Department of Computer Science and Associate Director of postgraduate programs at Prince Sultan University, Riyadh, KSA. She is also Vice-Chair of the ACM Professional Chapter at Prince Sultan University. She taught several courses at the graduate and postgraduate levels. She published several articles in ISI/Scopus indexed and attended various specialized international conferences. Currently, she is an editorial board member and reviewer of reputed journals and on the panel of TPC of international conferences. Her research interests include Statistics, AI, Machine/Deep Learning, Pattern recognition. slarabi@psu.edu.sa.







Sanaa Ghouzali    is an Associate Professor in the College of Computer and Information Sciences at King Saud University (Riyadh, Saudi Arabia). She received her Ph.D. degree in computer science and telecommunications from University of Mohamed V-Agdal (Rabat, Morocco), in 2009. Between 2005 and 2008, she received a Fulbright grant for joint-supervision program in the Visual and Communication Laboratory at Cornell University (Ithaca, NY, USA). From 2009 to 2011, she held an Assistant Professor position in ENSA (the National school of Applied Sciences) at the University of Abdelmalek Essaadi (Tetuan, Morocco) before joining King Saud University in 2012. Her research interests include Pattern Recognition, Biometrics, Biometric Template Protection, Information Security. sghouzali@ksu.edu.sa.







Tanzila Saba     is a Research Professor in CCIS Prince Sultan University Riyadh Saudi Arabia. Her area of specialization is Artificial Intelligence, Forecasting, Big data mining security. She is an eminent researcher in the field and has won several awards. tsaba@psu.edu.sa.



Linah Aburahmah     earned a Master's degree in Software Engineering from Prince Sultan university in 2019. She is part of the Customer and Marketing consulting team at Deloitte's office in Riyadh. She is expert in using customer-centric design approaches to design digital solutions and services. She is experienced with Enterprise design Thinking and have conducted multiple design thinking workshops with. She is certified as a Project Manager from the Project Management Institute. She is NN/g certified on Managing User Experience Strategy, CX Transformation and Journey Management, Design Tradeoffs and UX Decision Frameworks, and others. She is certified from IDEO on Human-Centered Service Design, Design thinking, and designing strategy. l.aburahmah@gmail.com.



Rana Almohaini     earned a Master's degree in Software Engineering from Prince Sultan university in 2021. Currently, she works as a Business Analyst at Channels by STC. almohaini.r@gmail.com.