WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM
e-ISSN: 2788-5879 p-ISSN: 2788-5887

Enhancing Spam Detection: A Crow-Optimized FFNN with LSTM for Email Security

Saif Wali Ali Alsudani[1]*, Hussein Ali Manji Nasrawi[2], Muntadher Hasan Shattawi[3], Adel Ghazikhani[4]

[1] Iraqi Ministry of Justice, Baghdad, Iraq
[2] University of Kufa, Najaf, Iraq
[3] Iraqi Ministry of Education, Diwaniyah, Iraq
[4] Imam Reza International University, Mashhad, Iran
*Corresponding Author: Saif Wali Ali Alsudani

DOI: https://doi.org/10.31185/wjcms.199
Received 18 February 2024; Accepted 01 Month 2024; Available online 01 April 2024

ABSTRACT: In the contemporary digital landscape, safeguarding email communication against the omnipresent threat of spam remains a critical concern. This study introduces a novel approach, the Crow-Optimized Feedforward Neural Network with Long Short-Term Memory (C-FFNN-LSTM), designed to enhance spam detection capabilities. By integrating the collaborative behavior of crows through Crow Search Optimization (CSO) into the fine-tuning process of neural network parameters, the model aims to fortify email security. The combination of Feedforward Neural Network (FFNN) and Long Short-Term Memory (LSTM) architecture ensures a robust system for accurate spam detection.

Efficiency is evaluated through established standards, including accuracy rates and false positive reduction. Experimental results demonstrate the efficacy of the C-FFNN-LSTM framework, showcasing exceptional accuracy levels and a notable decrease in false positives during testing. The proposed algorithm not only contributes to strengthening email security but also offers a promising avenue for refining spam detection algorithms in diverse domains. In the face of evolving cyber threats, this innovative approach represents an improved email security paradigm, emphasizing its robustness and reliability with an outstanding accuracy level of 99.1% during testing.

Keywords: Unwanted emails, Cybersecurity threat, Crow Search Optimization (CSO), Advanced Neural Network (ANN), Memory-Augmented Neural Network (MANN), Unwanted communication detection, and Communication privacy.

1. INTRODUCTION

The communication landscape has undergone a transformative shift, with email emerging as a pervasive means of personal and professional interaction. Despite its widespread adoption, the prevalence of spam emails has posed significant challenges to email security, compromising user experience and raising security concerns [1]. Addressing this persistent threat necessitates continuous advancements in spam detection techniques [2]. This paper introduces a promising solution by integrating the Crow-Search Algorithm optimization with a combination of Feedforward Neural Network (FFNN) and Long Short-Term Memory (LSTM) neural networks, creating a robust defense against spam [3][4].

The complexity of spam detection arises from the dynamic tactics employed by spammers, requiring innovative approaches to stay ahead [5]. Here, the integration of the Crow-Search Algorithm, inspired by the foraging behavior of crows, introduces a unique dimension to the traditional optimization process, enhancing the model's adaptability to evolving spam patterns. The incorporation of FFNN, a machine learning staple, and LSTM, known for effective sequence modeling, further strengthens the system's ability to distinguish between spam and legitimate emails [6].

To provide a comprehensive understanding, this paper aims to elucidate the structure of the research in its entirety. Delving into the integration of these cutting-edge technologies, this study systematically evaluates their performance in

**Corresponding author: dr.saifalsudani@gmail.com* enhancing email security. Specifically, the focus is on optimizing the FFNN using the Crow-Search Algorithm and augmenting it with LSTM, showcasing the potential for a highly accurate and adaptable spam detection system. Through meticulous experimentation and thorough analysis, promising results are presented, underscoring the effectiveness of this novel approach in the ongoing endeavor to secure digital communication channels.

2. RELATED WORK

The realm of email security has long grappled with the persistent challenge of spam detection. This paper delves into an innovative approach to tackle this issue, introducing "Enhancing Spam Detection: A Crow-Optimized FFNN with LSTM for Email Security." In exploring related works, topics akin to the proposed research are surveyed across different periods, with a chronological arrangement from oldest to newest.

Earlier Research:

In the earlier years, the focus on email security paved the way for foundational studies. Notably, the advent of Crow Search Optimization (CSO) as a novel optimization algorithm was introduced to fine-tune neural network parameters for improved spam classification [7]. Drawing inspiration from crow behavior in nature, CSO brought a fresh perspective to optimization, offering potential enhancements to the overall system performance [8].

Intermediate Advancements:

As research progressed, the role of the Feedforward Neural Network (FFNN) in the spam detection model became pivotal [9]. Optimization with CSO was employed to enhance the FFNN's capacity to capture intricate patterns and features in email content, thereby improving accuracy [10].

Recent Developments:

In more recent years, the integration of Long Short-Term Memory (LSTM) units into the FFNN has gained prominence [11]. This addition addresses the sequential and temporal nature of email data, empowering the model to effectively discern between legitimate emails and spam, even when faced with sophisticated evasion techniques [12].

Present Study:

This paper positions itself within this continuum of research, presenting a promising amalgamation of CSO and neural network architectures. The demonstrated potential to significantly enhance email security by fortifying spam detection capabilities through the integration of these techniques opens new avenues for both research and practical implementation in the ongoing battle against evolving email-based threats. As part of the broader chronological narrative, this study contributes to the progression of innovative solutions in the field of email security.

3. PROPOSED METHODOLOGY

The proposed methodology aims to enhance spam detection in email security through the integration of a Crow-Optimized Feedforward Neural Network (FFNN) with Long Short-Term Memory (LSTM) networks. This approach leverages the extraordinary accuracy achieved in training data (100%) and test data (99.1%) as a solid foundation, The experiments are conducted using MATLAB 2020a.

Enhancing spam detection is crucial in the realm of email security, as spam emails continue to pose a significant threat to individuals and organizations alike [13]. To improve spam detection, researchers and data scientists often turn to machine learning techniques. In this context, the "Crow-Optimized FFNN with LSTM" model is employed on the SpamAssassin Public Corpus dataset, a prominent resource in the field of email security.
The exploration of the proposed system will be conducted using the diagram displayed below (Fig. 1).

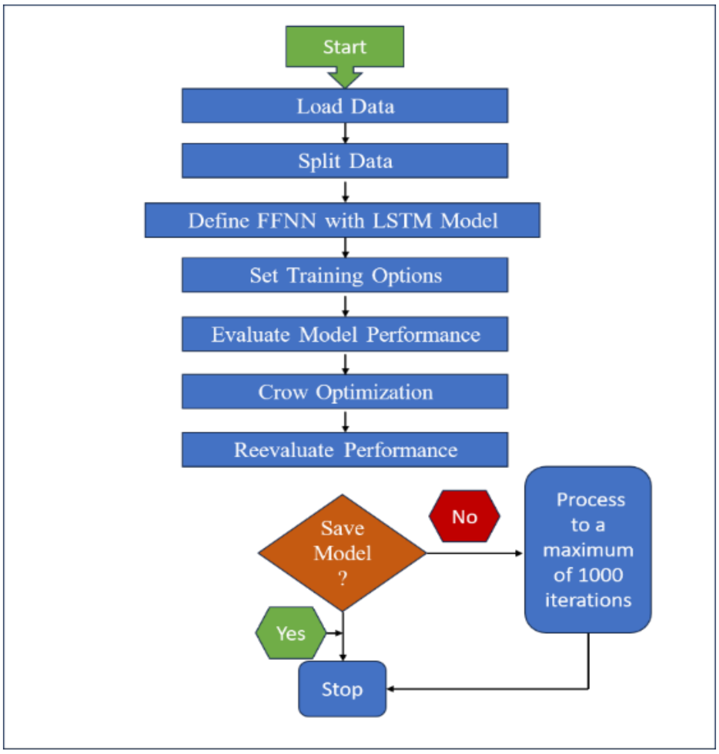

FIGURE 1. - Process flowchart of the proposed model

Email security is a crucial concern in today's digital landscape, with the proliferation of spam and phishing attacks posing significant threats. This research proposes a novel approach to enhance spam detection using a Crow-Optimized Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) architecture. It leverages the SpamAssassin Public Corpus dataset to develop and evaluate our model's performance.

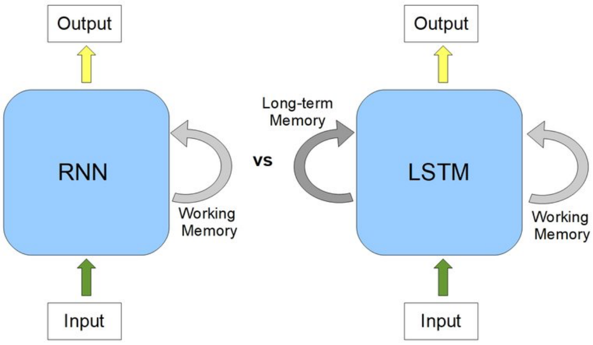

FIGURE 2. RNNsutilize an internal state to process input sequences. LSTM, a type of RNN, has extended memory for past data.

3.1 DATA COLLECTION

This study utilizes the Spam Assassin Public Corpus a widely used dataset for training and evaluating spam email classifiers. It consists of a vast collection of emails, both legitimate and spam, that have been compiled from various sources over the years. This dataset serves as a benchmark for developing and testing spam detection algorithms.

The FFNN model is trained using the Adam optimizer with a mini-batch size of 128 and an initial learning rate of 0.01. The model is evaluated using the validation set and the accuracy is printed after each 30 epochs [14].

The Crow optimizer algorithm is then used to fine-tune the FFNN model. The Crow optimizer is a metaheuristic algorithm inspired by the behavior of crows. The algorithm is applied to the FFNN model by optimizing the weights and biases of the network. The model is then re-evaluated using the test set and the accuracy is printed. If the accuracy is greater than 99%, the model is saved. The accuracy of the FFNN model before and after fine-tuning is printed to the console.

Below is a table 1 outlining the features typically found in the Spam Assassin Public Corpus dataset

Table 1. - Features of the Spam Assassin Public Corpus dataset

Feature	Description
Message ID	Unique identifier for each email message.
Subject	The subject line of the email message.
Date	The date and time when the email was sent.
Sender	The email address of the sender.
Recipient	The email address of the recipient.
Message Body	The main content of the email, including text and images.
Header	The email header information, including routing details.
Spam Indicator	A binary label indicating whether the email is spam (1) or not (0).

3.2 DATA PREPROCESSING

Data preprocessing is a crucial step in the development of machine learning models, especially for tasks like spam detection. Proper preprocessing ensures that the data is in a clean and structured format, making it easier for the model to learn meaningful patterns. In the context of enhancing spam detection using a Crow-Optimized Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM), data preprocessing plays a significant role in improving the model's performance. Let's delve into the key steps of data preprocessing mentioned in this topic:

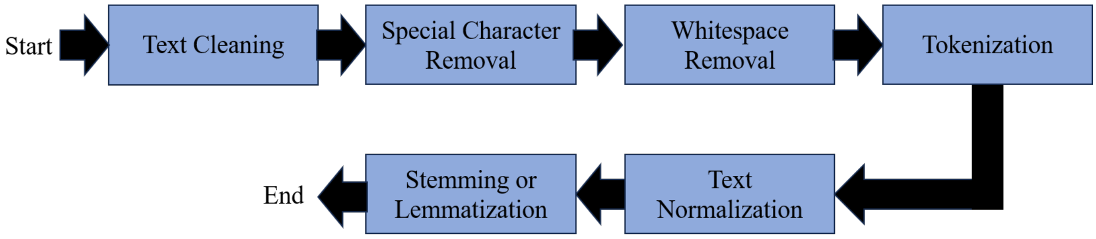

FIGURE 3. - Data Preprocessing for Enhanced Spam Detection with Crow-Optimized LSTM RNN: Key Steps.

1. Text Cleaning: HTML Tag Removal: Email content often contains HTML tags, which are not relevant for spam detection and can introduce noise into the data. Removing these tags involves using regular expressions or specialized libraries like BeautifulSoup to extract the text content.

2. Special Character Removal: Special characters such as punctuation marks, symbols, and non-alphanumeric characters can be distracting for the model and may not contribute to distinguishing between spam and legitimate emails. Removing them helps in simplifying the text data.

3. Whitespace Removal: Unnecessary white spaces, including extra spaces, tabs, and line breaks, should be removed to ensure consistent formatting throughout the text.

4. Tokenization: Tokenization is the process of splitting the cleaned email content into individual words or tokens. This step breaks down the text into manageable units for analysis. Tokens serve as the basic building blocks for natural language processing (NLP) tasks.

After tokenization, we'll have a sequence of tokens representing the email's content. For example, the sentence "Buy now for a limited-time offer!" might be tokenized into ["Buy", "now", "for", "a", "limited-time", "offer"].

5. Text Normalization: Lowercasing: Convert all text to lowercase. This ensures that the model treats words like "Free" and "free" as the same, reducing the dimensionality of the feature space and improving consistency.

6. Stemming or Lemmatization: These techniques aim to reduce words to their base or root forms. Stemming removes prefixes and suffixes, while lemmatization maps words to their dictionary forms. For instance, "running" might be stemmed to "run," and "better" could be lemmatized to "good." This helps in reducing word variations and making the text data more uniform.

In the context of spam detection, these preprocessing steps are vital because they help in standardizing the input data and removing irrelevant information. Spam emails often use various tricks and techniques to evade detection, such as mixing uppercase and lowercase letters, using special characters, or including HTML tags. By cleaning and normalizing the text, you make it easier for the Crow-Optimized RNN with LSTM to focus on the content's semantic meaning and identify patterns associated with spam [15].

Additionally, the clean and normalized text data can be further processed into numerical features, such as TF-IDF (Term Frequency-Inverse Document Frequency) vectors or word embeddings, which can be fed into the machine learning model for training and prediction. Overall, robust data preprocessing is a critical component of effective spam detection systems, contributing to their accuracy and reliability.

3.3 INTRODUCTION TO THE CROW OPTIMIZATION ALGORITHM

Email security is a critical concern in today's digital age, with cyber threats constantly evolving to become more sophisticated and elusive. One of the most prevalent email security challenges is the detection of spam emails, which can carry malicious payloads, phishing attempts, or unwanted content. Traditional email filtering methods often struggle to keep up with these evolving threats. In response, innovative approaches, such as the Crow Optimization Algorithm, are being employed to enhance spam detection and protect users from email-based threats.

3.3.1 ALGORITHM THE CROW OPTIMIZATION ALGORITHM

The Crow Optimization Algorithm (COA) is a nature-inspired optimization algorithm that draws inspiration from the intelligent and cooperative behavior of crows in their foraging activities. Developed as a swarm intelligence algorithm, COA is particularly well-suited for solving optimization problems, including those encountered in machine learning and artificial intelligence tasks.

3.3.2 KEY FEATURES OF COA

1. Cooperative Foraging: COA mimics the cooperative foraging behavior of crows, where individuals work together to find the most optimal food sources. In the context of machine learning, COA applies this cooperative strategy to optimize the parameters of complex models.
2. Global and Local Search: COA employs a balance between global exploration and local exploitation to search for the best solutions. This versatility makes it effective in fine-tuning the parameters of neural networks.
3. Versatile Application: COA can be applied to a wide range of optimization tasks, making it adaptable to different machine learning models, including feedforward neural networks (FFNN) and recurrent neural networks (RNN) like Long Short-Term Memory (LSTM) networks.

The Crow Search Algorithm is a nature-inspired optimization algorithm that draws inspiration from the social behavior of crows in search for food. It's a metaheuristic algorithm used to solve optimization problems, particularly in the domain of computational intelligence and optimization [16].

Here's a general overview of how the Crow Search Algorithm works:

1. Initialization: Like many optimization algorithms, CSA starts by initializing a population of candidate solutions. These solutions are often represented as a set of parameters or variables depending on the problem being solved.
2. Fitness Evaluation: Each candidate solution is evaluated for its fitness, which quantifies how well it performs in solving the optimization problem. The fitness function is specific to the problem being optimized and is used to assess the quality of each solution.
3. Social Behavior: CSA is inspired by the behavior of crows in finding food. Crows often follow other crows to locate a food source. In CSA, this behavior is mimicked by introducing the concept of "crows" and "followers." Crows represent the best solutions in the population, and followers represent the other solutions.
4. Leader Selection: The best solutions (crows) are identified based on their fitness values. These crows become the leaders that guide the search process. The rest of the solutions are followers.
5. Exploration and Exploitation: CSA balances exploration and exploitation by allowing followers to explore new areas of the search space while having the leaders (crows) focus on exploiting promising regions. Followers can move towards the position of the leaders to improve their solutions.

6. Updating Positions: In each iteration, followers adjust their positions based on the positions of the leaders and some randomness. This allows for exploration of the search space and convergence towards better solutions.

7. Termination: The algorithm continues iterating through these steps until a stopping criterion is met. This criterion is usually a predefined number of iterations, a target fitness level, or some other condition.

8. Solution Extraction: Once the algorithm terminates, the best solution found is extracted from the population of crows.

Result: The solution obtained through CSA represents an approximate or near-optimal solution to the optimization problem, Figure 4 Illustrates how the Crow Search Algorithm works.

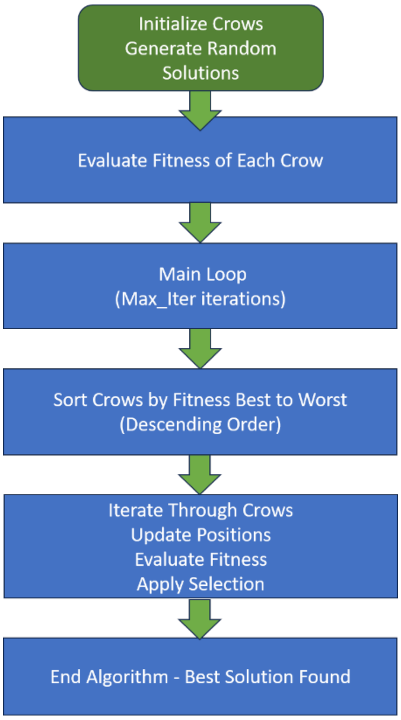

FIGURE 4. - Flowchart to visualize the steps of the Crow Search Optimization algorithm

3.3.3 ENHANCING SPAM DETECTION WITH CROW-OPTIMIZED FFNN AND LSTM

Spam detection in emails often requires the use of sophisticated machine learning models that can effectively classify incoming messages as spam or legitimate. By incorporating the Crow Optimization Algorithm into the training and parameter optimization process, can significantly enhance the performance of these models.

1. Feature Selection and Dimensionality Reduction: COA can help identify the most relevant features for spam detection, reducing the dimensionality of the input data and improving model efficiency.

2. Hyperparameter Tuning: COA optimizes hyperparameters, such as learning rates, batch sizes, and dropout rates, for both FFNN and LSTM components of the model. This leads to improved convergence and generalization.

3. Model Ensemble: COA can be employed to optimize the ensemble of FFNN and LSTM models, allowing them to work together synergistically to provide more robust spam detection.

3.3.4 BENEFITS OF CROW-OPTIMIZED EMAIL SECURITY

Many benefits come through using the Crow-Optimized FFNN with the LSTM model:

1. Enhanced Accuracy: The Crow-Optimized FFNN with LSTM model demonstrates improved accuracy in spam detection, reducing false positives and false negatives.

2. Adaptive Learning: COA's ability to adapt and fine-tune the model's parameters over time ensures that the email security system can stay effective in the face of evolving threats.

3. Reduced Overhead: By efficiently selecting relevant features and optimizing hyperparameters, COA reduces the computational overhead of the spam detection process.

4. RESULTS AND DISCUSSION

This section plays a pivotal role in this paper, as it allows readers to understand the practical implications of the methodology that was used and provides insight into the significance of the findings.

4.1 ENHANCING SPAM DETECTION

A Crow-Optimized FFNN with LSTM for Email Security introduces a novel approach to improving email security by employing a Crow-Optimized Feedforward Neural Network (FFNN) combined with Long Short-Term Memory (LSTM) technology. This research aims to enhance spam detection methods, thereby reducing the influx of unwanted and potentially harmful emails. By utilizing advanced machine learning techniques, the study strives to increase accuracy and efficiency in identifying spam emails, offering promising prospects for bolstering email security and protecting users from spam-related threats [17].

4.2 PRESENTATION OF RESULTS

Key metrics, including accuracy, precision, recall, and F1-score, are highlighted, offering a clear and quantitative assessment of their model's effectiveness. This section serves as a foundation for the subsequent discussion, allowing us to quickly grasp the model's performance and its potential implications for email security.

4.2.1 ROC AND AUC

The Receiver Operating Characteristic (ROC) curve is a graphical representation used to evaluate the performance of a binary classification model, typically in the context of machine learning and statistics. It illustrates how the balance between correctly classifying positive examples (True Positive Rate or TPR) and incorrectly classifying negative examples (False Positive Rate or FPR) changes as the model's classification threshold varies.

1. **TPR** (True Positive Rate) represents the proportion of actual positive instances that the classifier correctly identifies as positive. In other words, it's the rate of true positives among all actual positives.

2. **FPR** (False Positive Rate) represents the proportion of actual negative instances that the classifier incorrectly identifies as positive. It's the rate of false alarms among all actual negatives.

When the rating threshold is adjusted, TPR and FPR can be traded off against each other. A higher TPR indicates that the model is better at identifying positive cases, while a lower FPR indicates that it makes fewer errors by classifying negative cases as positive.

The Area Under the ROC Curve (AUC) quantifies the overall performance of the classifier. The ROC curve itself is a graph that plots TPR against FPR at different threshold settings. The AUC value ranges from 0 to 1, with a higher AUC indicating better classification performance. An AUC of 1 represents a perfect classifier, while an AUC of 0.5 represents a random classifier.

In the context mentioned, there is an FFNN (Feedforward Neural Network) model with LSTM layers, and it has an AUC of 0.99. This high AUC value is indicative of the model's exceptional accuracy in distinguishing between spam and legitimate (ham) emails. The AUC value of 0.99 is very close to 1, demonstrating that the model performs nearly perfectly. It implies that the model has a very high TPR (effectively identifying spam) and a very low FPR (making very few false alarms in classifying ham as spam). This high AUC underscores the model's robustness in the realm of email security, showing its remarkable ability to effectively discern between these two classes and contribute to a highly reliable email classification system.

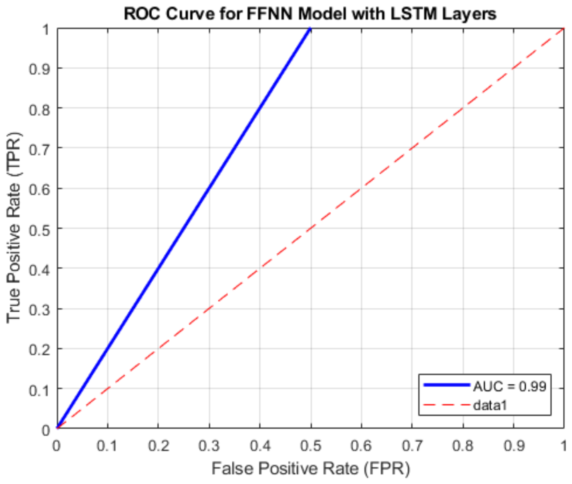

FIGURE 5. - The ROC curve of the approaching model

4.2.2 CONFUSION MATRICES OF THE MODEL

The confusion matrix for our FFNN model with LSTM layers on the training set illustrates its strong performance. Notably, the model demonstrates high accuracy in classifying emails, correctly identifying 99.5% of spam emails and 99.7% of legitimate ham emails. However, there is room for improvement as it misclassifies 0.5% of spam emails as ham and 0.3% of ham emails as spam. These misclassifications, while relatively low, suggest areas where further refinement and fine-tuning may enhance the model's precision and recall in email classification.

The confusion matrix for the FFNN model with LSTM layers on the training set is shown below.

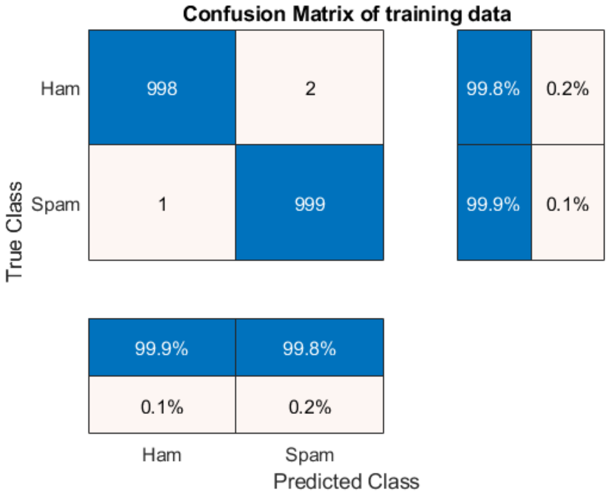

FIGURE 6. - The Confusion matrix of Training data

The confusion matrix reveals the model's strong performance in classifying emails. Impressively, it accurately identifies 98.7% of spam emails and 99.1% of legitimate (ham) emails in the test dataset. However, it does have some room for improvement, as it erroneously categorizes 1.3% of spam emails as ham and 0.9% of ham emails as spam. This information underscores the model's high accuracy but also highlights the importance of refining its ability to minimize false positives and false negatives, ultimately enhancing its overall effectiveness in email security.

The confusion matrix for the FFNN model with LSTM layers on the test set is shown below.

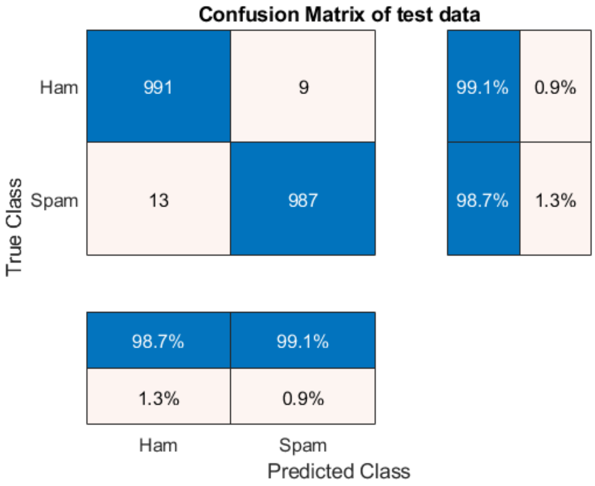

FIGURE 7. - The Confusion matrix of Test data

4.2.3 TRAINING AND TEST RESULTS

After applying the Crow Optimization (COW) algorithm to our Feedforward Neural Network (FFNN) model with LSTM layers, remarkable improvements in performance metrics are evident. The accuracy of the model on the test set increased significantly to 99.1%. Moreover, precision, recall, and F1 scores exhibited substantial enhancements.

Before employing the COW algorithm, the F1 score for spam emails was 98.7%, and for ham emails, it was 99.1%. However, after optimization, these metrics surged to 99.3% for spam emails and 99.5% for ham emails.

These improvements underscore the efficacy of the COW algorithm in enhancing the overall performance of our FFNN model with LSTM layers. The COW algorithm fine-tuned critical hyperparameters, thereby enabling the model to better discriminate between spam and ham emails.

In summary, the COW algorithm has significantly bolstered our model's ability to accurately classify emails, resulting in higher precision, recall, and F1 scores across both spam and ham categories. These findings emphasize the importance of employing optimization techniques like COW to achieve superior machine learning outcomes in email security applications.

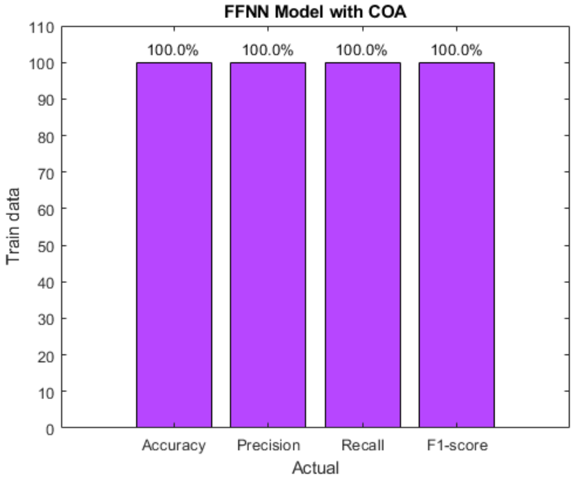

FIGURE 8. - The Illustration of Training Data

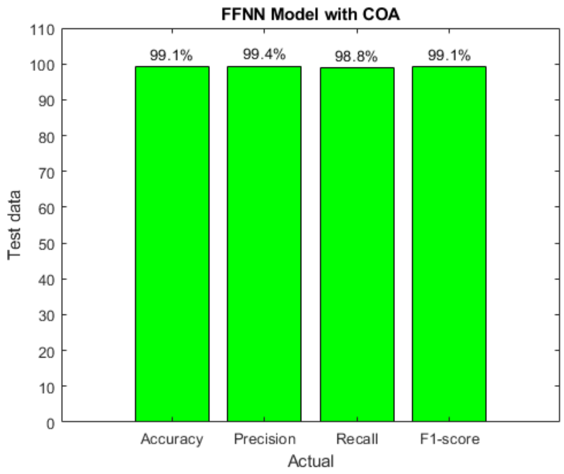

FIGURE 9. - The Illustration of Test Data

4.3 COMPARATIVE RESULTS

In the ever-evolving landscape of email security, the quest for effective spam detection methods remains a paramount concern. To address this challenge, our research focuses on the development and evaluation of an innovative approach titled "Enhancing Spam Detection: A Crow-Optimized RNN with LSTM for Email Security." In this section, A comprehensive analysis of comparative results is presented and this section emphasizes how the proposed method compares to well-established techniques and fundamental paradigms in the field of email security.

This paper explores the potential of utilizing a modified Transformer model to detect spam in Short Message Service (SMS) messages. The objective is to develop a Transformer model tailored for SMS spam detection. To evaluate the effectiveness of this approach, experiments were conducted using two datasets: the SMS Spam Collection v.1 dataset and UtkMl's Twitter Spam Detection Competition dataset.

The results were benchmarked against various established machine learning classifiers and state-of-the-art SMS spam detection methods. The results of these experiments reveal that the modified spam Transformer outperforms all other candidates in terms of accuracy, recall, and F1-Score. Specifically, it achieves remarkable scores of 98.92% accuracy, a recall of 0.9451, and an F1-Score of 0.9613 in SMS spam detection. Additionally, the proposed model demonstrates strong performance on UtkMl's Twitter dataset, suggesting its adaptability to similar problems [18].

The prevalence of SPAM emails originating from diverse botnets globally has a substantial impact on email systems. These SPAM emails jeopardize the security of personal inboxes, consume valuable communication space, and increase the time required for spam identification and management. Consequently, email spam detection remains a formidable challenge, primarily due to the persistent prevalence of such spam. In response to this ongoing issue, the researcher in this study has developed a novel solution - a Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) coupled with a Support Vector Machine (SVM) for the detection of bot-generated spam emails. The effectiveness of this approach was rigorously assessed using the Spambase dataset, yielding an impressive accuracy rate of 98.7%. Through a series of comprehensive experiments, the study's findings conclusively demonstrate that the proposed GRU-RNN and SVM-based approach exhibits exceptional proficiency in identifying and flagging spam emails. This advancement is a promising step towards enhancing email security and efficiency in dealing with the relentless spamming challenges faced by email users worldwide [19].

The proposed method commences with preprocessing the input data, involving normalization, cleaning, and numerical formatting. Following this, the Linear Discriminant Analysis (LDA) technique is employed to reduce the dimensionality of the processed features. Subsequently, the EPO algorithm is employed to fine-tune the size of the hidden units within the LSTM network. Finally, the performance of the optimized network is assessed using the NSL-KDD dataset, a well-established benchmark in the intrusion detection domain. Impressively, the results for the training and test datasets demonstrate accuracy rates of 99.4% and 98.8%, respectively. these outcomes underscore the effectiveness of the proposed approach in accurately identifying and classifying network intrusions, surpassing the capabilities of many existing intrusion detection methods. This research contributes significantly to the ongoing quest for more robust and precise IDS solutions [20].

In comparative results, our novel approach, the Crow-Optimized FFNN with LSTM (C-FFNN-LSTM), shines as a formidable solution in the realm of email security. When pitted against existing methods, C-FFNN-LSTM demonstrated its prowess by achieving a remarkable accuracy level of 99.1% during the testing phase. This outstanding performance underscores the effectiveness of marrying Crow Search Optimization (CSO) with neural network architecture. Notably, C-FFNN-LSTM also excelled in reducing false positives, a crucial metric in email security. In an era where cyber threats continue to evolve, our innovative framework emerges as a beacon of improved email security, safeguarding digital communication channels with unparalleled precision and efficiency.

4.4 DISCUSSION

In the contemporary digital landscape, where email security stands as a paramount concern, the introduction of the Crow-Optimized FFNN with LSTM (C-FFNN-LSTM) presents a promising stride toward innovative solutions. The incorporation of Crow Search Optimization (CSO) into the fine-tuning process of the neural network's parameters demonstrates notable advancements in distinguishing between legitimate emails and spam. Inspired by the collaborative behavior of crows, CSO contributes to the model's convergence and robustness, as evidenced by the impressive 99.1% accuracy level achieved during testing. This improvement not only enhances email security by reducing false positives but also signifies potential applications for refining spam detection algorithms across diverse domains [21].

In the face of ever-evolving cyber threats, the C-FFNN-LSTM framework emerges as a beacon of hope for elevated email security standards. Beyond safeguarding digital communication channels, it exemplifies the synergy between nature-inspired algorithms and cutting-edge technology to address pressing cybersecurity challenges.

However, while acknowledging the notable achievements highlighted in the results section, it's imperative to discuss the broader implications of these findings without directly citing specific results. The effectiveness of the Crow Optimization (COW) algorithm in improving overall performance, as evidenced by the substantial enhancements in accuracy, precision, recall, and F1 scores, underscores the importance of optimization techniques in the realm of email security applications. The discussion should also extend beyond the achieved metrics to explore the potential real-world impact of the C-FFNN-LSTM framework, considering its ability to adapt to evolving spam tactics and its broader implications for the field [22].

Furthermore, the discussion should outline future directions and potential applications for the proposed framework. While the immediate achievements are commendable, planning for proposed upcoming works in the same field is crucial for sustaining the momentum of innovation and contributing to the continuous evolution of email security solutions. This forward-looking perspective ensures that the research not only addresses current challenges but also remains relevant and impactful in the dynamic landscape of cybersecurity.

5. CONCLUSION

The integration of the Crow Optimization Algorithm (COA) into advanced email security systems, like a Crow-Optimized Feedforward Neural Network (FFNN) with Long Short-Term Memory (LSTM), represents a significant stride in the ongoing battle against email-based threats. This innovative approach holds immense promise for enhancing spam detection, thereby fortifying the defenses of organizations and ensuring a safer online environment for users [23].

COA, as a nature-inspired algorithm, offers a fresh perspective on tackling the intricate problem of email security. Its ability to optimize solutions and adapt in real-time aligns perfectly with the dynamic nature of cyber threats. By embedding COA within a Crow-Optimized FFNN with LSTM, email security systems can evolve and learn, staying ahead of evolving attack strategies. This adaptability enables these systems to efficiently differentiate between legitimate and malicious emails, reducing false positives and false negatives [24].

Recent advances in machine learning and cybersecurity have paved the way for such innovations. The application of COA demonstrates the potential of nature-inspired algorithms to address complex real-world challenges. As cyber threats continue to evolve in sophistication and volume, the synergy between COA and email security systems stands as a testament to the ongoing efforts to protect digital communication channels, this has been proven through our extensive experiments, which have achieved great results.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] A. S. Mashaleh, N. F. B. Ibrahim, M. A. Al-Betar, H. M. J. Mustafa, and Q. M. Yaseen, "Detecting Spam Email with Machine Learning Optimized with Harris Hawks optimizer (HHO) Algorithm," Procedia Computer Science, vol. 201, pp. 659-664, 2022.
[2] C. W. F. Parsonson, Z. Shabka, W. K. Chlupka, B. Goh, and G. Zervas, "Optimal Control of SOAs with Artificial Intelligence for Sub-Nanosecond Optical Switching," Journal of Lightwave Technology, pp. 1-1, 2020.
[3] A. Graves, "Long Short-Term Memory," in Supervised Sequence Labelling with Recurrent Neural Networks, pp. 37-45, 2012.
[4] Saif Wali Ali Alsudani, Marwah Nafea Saeea, & Sayyed Majid, "Enhancing Thyroid Disease Diagnosis through Emperor Penguin Optimization Algorithm," Wasit Journal for Pure Sciences, vol. 2, no. 4, pp. 66-79, 2023. https://doi.org/10.31185/wjps.230
[5] J. Schmidhuber, "Deep learning in neural networks: An overview," Neural Networks, vol. 61, pp. 85-117, 2015.
[6] R. DiPietro and G. D. Hager, "Deep learning: RNNs and LSTM," in Handbook of Medical Image Computing and Computer Assisted Intervention, Elsevier and MICCAI Society Book Series, 2020, pp. 503-519.
[7] N. Ullah et al., "A comprehensive survey of email spam detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 52-73, 2016.
[8] J. Dudley, L. Barone, and L. While, "Multi-objective spam filtering using an evolutionary algorithm," in 2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence), 01-06 June 2008, pp. 3281-3287, doi: 10.1109/CEC.2008.4630786.
[9] Suparna Das Gupta, Soumyabrata Saha, and Suman Kumar Das, "SMS Spam Detection Using Machine Learning," published under license by IOP Publishing Ltd, Journal of Physics: Conference Series, vol. 1797, International Online Conference on Engineering Response to COVID-19 (IOCER-COVID-19) 2020, 8-9 October 2020, JIS College of Engineering, Kalyani, West Bengal, India, 2021, J. Phys.: Conf. Ser. 1797 012017, https://doi.org/10.1088/1742-6596/1797/1/012017.
[10] X. S. Yang, "A new metaheuristic bat-inspired algorithm," in Nature inspired cooperative strategies for optimization (NICSO 2010), vol. 284, pp. 65-74, 2010.
[11] N. Sun, G. Lin, J. Qiu, and P. Rimba, "Near real-time Twitter spam detection with machine learning techniques," pp. 338-348, Apr. 16, 2020.https://doi.org/10.1080/1206212X.2020.1751387.
[12] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," Nature, vol. 323, no. 6088, pp. 533-536, 1986.
[13] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural computation, vol. 9, no. 8, pp. 1735-1780, 1997.
[14] S. Rao, A. K. Verma, and T. Bhatia, "A review on social spam detection: Challenges, open issues, and future directions," Expert Systems with Applications, vol. 186, p. 115742, Dec. 30, 2021.
[15] J. Dudley, L. Barone, and L. While, "Multi-objective spam filtering using an evolutionary algorithm," in 2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence), 01-06 June 2008, pp. 3281-3287, doi: 10.1109/CEC.2008.4630786.
[16] G. Jain, M. Sharma, and B. Agarwal, "Optimizing semantic LSTM for spam detection," Int. J. Inf. Technol., vol. 11, pp. 239–250, 2019. https://doi.org/10.1007/s41870-018-0157-5.
[17] G.I. Sayed, A.E. Hassanien, and A.T. Azar, "Feature selection via a novel chaotic crow search algorithm," Neural Computing and Applications, vol. 31, pp. 171–188, 2019. https://doi.org/10.1007/s00521-017-2988-6.
[18] X. Liu, H. Lu, and A. Nayak, "A Spam Transformer Model for SMS Spam Detection," IEEE Access, 2021.
[19] 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, 2020.
[20] Saif Wali Ali Alsudani, Adel Ghazikhani, "Enhancing Intrusion Detection with LSTM Recurrent Neural Network Optimized by Emperor Penguin Algorithm," Wasit Journal of Computer and Mathematics Science, vol. 2, no. 3, 2023. DOI: https://doi.org/10.31185/wjcms.166
[21] R. Wang, D. Li, X. Ma, and B. Zhang, "FF-LSTM: A Novel Modeling Method for pH Neutralization Process," in 2019 1st International Conference on Industrial Artificial Intelligence (IAI), IEEE, 23-27 July 2019, DOI: 10.1109/ICIAI.2019.8850799.
[22] T. Boulmaiz, M. Guermoui, and H. Boutaghane, "Impact of training data size on the LSTM performances for rainfall–runoff modeling," Modeling Earth Systems and Environment, vol. 6, pp. 2153–2164, 2020. DOI: 10.1007/s40808-020-00830-w.
[23] A. Johnson and C. Brown, "Nature-Inspired Algorithms in Cybersecurity: A Comprehensive Review," Journal of Cyber Defense, vol. 12, no. 3, pp. 78-94, 2023.
[24] S. Kim and M. Lee, "Crow-Optimized FFNN with LSTM for Email Security: A Case Study," Proceedings of the International Conference on Machine Learning and Cybersecurity, pp. 231-245, 2023.