International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

An Enhanced Mechanism for Deep Learning based Spam E-Mail Detection

Kola Navya, Mohammed Abdul Adil, MD Sohail Khan, Mohammed Nehal, Mohammed Mujahid Uddin Quadri

Department of Computer Science and Engineering, Vijay Rural Engineering College, Rochis Valley, Manikbhandar, Telangana, India

navya.mettu92@gmail.com, cse41project14@gmail.com

ABSTRACT

In the world of the internet, Spam email is becoming the biggest issue. Financial organisations are influenced by spam emails, which also exacerbate individual email users' experiences. At present, email communication is becoming more frequent, making it more challenging to maintain its security and integrity and detect spam emails. The development of effective spam detection models has been an important advance in existing research, but adaptability and classification performance remain challenging as spamming techniques evolve. This presents an Enhanced Mechanism for Deep Learning based Spam E-Mail Detection. From the Enron Corpus, raw email data was collected. The e-mail classification stage includes mapping between the training and test sets using Convolutional Neural Networks (CNNs). This analysis describes the Sand Cat Swarm Optimisation (SCSO) algorithm, which employs a CNN to enhance accuracy and minimise loss. The described model distinguishes between undesired (spam) and genuine (non-spam) emails. Accuracy, Precision and Recall are the parameters used in this paper to measure performance. Results confirmed that the described model gives very accurate results.

Keywords: *Spam email, Convolutional Neural Networks (CNNs), Sand Cat Swarm Optimization (SCSO), Deep Learning, Spam.*

I. Introduction

In our lives, the internet is an integral part of everyday life, and it is more prevalent among people who use email. Common and effective communication sources in the present day include the email system [1]. The email system is more popular mainly because of its fast communication and cost-effectiveness. In 2021, worldwide billion email accounts were created and 3

million emails sent per second. Therefore, email services have become important in both personal and professional transactions. Sending emails in bulk becomes challenging because they are often flagged as spam. The main factor driving their proliferation is the efficiency of spam emails as an advertising medium [2]. By sharing our email addresses on websites that are not authorized that results in undesired (spam) emails and unwanted messages being sent to recipients, even it shows negative effects like cluttering inboxes, slowing down the internet, theft of important data, manipulating search results, and wasting a lot of time with these spam mails [3].

Modern enterprises are highly automated and face intense competition in the twenty-first century. There will be Effective email communication between an organisation and its different branches. It is essential to ensure its longevity [4]. In this situation, dealing with spam is extremely difficult, and the battle against it remains unchanged; the perfect solution has not yet been found despite the numerous antispam methods proposed by Internet Service Providers (ISPs) and various organisations. This is mainly due to the growing sophistication of spammers and the effective characteristics of electronic communication [5]. The first step in identifying spam emails is categorising incoming emails as undesired (spam) or genuine (not spam).

It aimed to steal confidential information by phishing, linking to malware-hosting websites in Spam emails. Even though it is classified as non-self, and it is not used for advertisement [6]. To protect our mailboxes from spam emails, various spam filtering techniques are used to address these problems [7]. In spam detection, many research studies have been conducted to identify spammers and spam content accurately, but it remains a challenging task [8].

To solve problems such as malware detection and network traffic analysis, Deep learning models are used across a number of computer science domains [9]. Regularly, people will communicate or have social interactions through emails only. Customer data is exposed through security breaches, and spammers can send fake emails by creating them. Therefore, spammers can easily send unauthorized (spam) emails [10]. It tricks people by clicking on spam links in fake emails through Phishing attacks. Companies are developing many tools and methods to detect unwanted emails in networks [11]. To identify and prevent unsolicited emails, organisations use filtering methods, established rules, and configure firewall settings [12]. Communication for both individuals and organisations was streamlined via email. The spammers will take advantage of it by sending unsolicited email.

Because of their efficacy in recognition and classification tasks, Convolutional Neural Networks (CNNs) have received a lot attention recently. The automatic recognition makes CNNs function more advantageous by collecting complex low-level features from images than conventional techniques and producing better results [13]. The suggested algorithms aim to increase spam detection's overall effectiveness by improving each step of the spam detection process. By using bio-inspired methodologies, deep learning algorithms are developed. This paper proposes a method for detecting spam emails. The hunting behaviour of sand cats mimics metaheuristic optimisation, as implemented in the novel Sand Cat Swarm Optimisation (SCSO) algorithm. The goal of increasing accuracy and decreasing loss is optimised by each epoch's weights.

The remaining paper is organised as follows: Section II describes the Literature survey, and Section III explores the model for Spam E-Mail Detection. Results and discussion are presented in Section IV, and the paper concludes in Section V.

II. Literature Survey

In [14], the issue of spam identification with conventional content-matching criteria is addressed by integrating the modified binomial logistic algorithm. The study, starting with three fundamental categories: adult content, special words, and particular symbols and numbers, also creates seven content-matching categories. The remaining four categories are created by combining fundamental categories in different ways. This proposed approach demonstrates its effectiveness by evaluating accuracy, precision, recall, F-measure, and AUC_ROC. It was sufficiently handled with a high sample size without compromising effectiveness.

In [15], using a hybrid Water Cycle and Simulated Annealing to enhance feature selection accuracy by evaluating the described Detection and optimisation of Spam. The study's methodology contains quality comparison, evaluation, improvement, induction, and groundwork. With an accuracy of 96.3%, the hybridization model performed better than other feature selection techniques like Particle Swarm, Harmony Search and Genetic Algorithm(GA). The SVM performs better than other classifiers, it shows F1-Score of 96.3% to the three classifier algorithms

In [16], a new Spam Detection System (SDS) method is proposed by using a set of six extended Grasshopper Optimisation Algorithm (EGOA) variants. Advanced spam email detection is achieved by integrating variants with a Multilayer Perceptron (MLP). This context is created by combining MLPs with EGOAs; EGOAMLPs are Neural Network (NN) models. The EGOAs train the suggested MLP model to demonstrate the finding. It performs better than other optimisation techniques in terms of detection rate accuracy and false alarm rate.

In [17], to cluster spam and ham emails, unsupervised learning is used to investigate. By employing a clustering strategy, an unsupervised framework is created using several algorithms, primarily the subject header and the body of the email, and this is the objective of this study. The DBSCAN (Density-Based Spatial Clustering of Applications with Noise) is the nearest performer for OPTICS (Ordering Points to Identify Cluster Structure), which is the best clustering, with an average of 0.26%. The average balanced accuracy of DBSCAN and OPTICS was approximately 75.76%.

In [18], machine learning methods are enhanced with bio-inspired techniques, and a spam email detection technique is introduced. A thorough investigation was conducted to apply machine learning models utilizing SVM, NB, Random Forest (RF), MLP and Decision Tree (DT), in addition to feature extraction and pre-processing with seven different email datasets. The machine learning and bio-inspired model is most appropriate, as results are compared with those of other models.

In [19], to examine how spam email filtering models' performance, an advanced evaluation technique is suggested. This proposed method includes text pre-processing, embedding training, a spam email filtering model, evaluation, and analysis of the classification patterns of learning-based spam email filtering models. The output is demonstrated with different datasets and spam email filtering models distribute different test datasets from the training dataset. The spam email filtering model's accuracy is decreased.

In [20], a new effective method for multiclass email classification, called SeFACED, is proposed using a Gated Recurrent Unit (GRU) based on Long Short-Term Memory (LSTM). To achieve optimal performance and evaluation by evaluating deep learning models of SeFACED focuses on optimizing LSTM-based GRU parameters with conventional machine learning. The SeFACED outperforms current techniques and maintains a robust, accurate classification process.

In [21], a new model message filter is proposed using the Euclidean distance. It shows beyond the containment methodologies that are currently more used. Based on the distribution of character frequencies in your content and in the creation of signatures, a novel communication filter is described. Architecture that prevents spam and phishing is suggested to help contain attempted mail fraud.

In [22], by scanning 236 million domains and 139 nations' most popular domains for analysing the global adoption rate of SPF and Domain-based Message Authentication, Reporting, and Conformance (DMARC) in two extensive campaigns. It suggests a novel approach for detecting listed as well as registered domains with incorrectly configured SPF rules by simulating the Sender Policy Framework (SPF) check function. The attackers will successfully send fake emails to user inboxes when a significant portion of domains fail to properly configure SPF and DMARC rules, as evaluated in this finding.

In [23], using Python Naïve Bayes (NB) and support vector machine (SVM), an email filter is developed to identify email attacks. The NB and SVM email filters using various kernel functions show better filtering performance for the Total Cost Ratio (TCR), Accuracy, and precision. The effects of the feature on stop word removal are evaluated, and other filtering algorithm parameters are evaluated to optimise the filters.

In [24], the Bcrypt algorithm and a randomly generated salt serve as security layers for a modified version of the SHA-512 algorithm. It was thoroughly assessed against the updated SHA-512 standard, meeting numerous requirements, including hash construction, collision resistance, attack resistance, data integrity, and computational efficiency, and demonstrating that data integrity and collision resistance were effectively ensured by the algorithm. For email addresses, the SHA-512 algorithm is a more efficient and secure hashing technique that works effectively.

In [25], a deep Recurrent Neural Network (RNN) is utilized to identify spam email. Tanh was found to be the optimal activation function, with a dropout rate of 0.1 and an epoch count of 100, achieving the highest accuracy after experimenting with several configurations. The suggested method achieves a high accuracy of 99.7%, performs better than the hybrid gated recurrent unit RNN method, with a highest accuracy of 98.7%.

III. Deep Learning based Spam E-Mail Detection

The block diagram of An Enhanced Mechanism for Deep Learning based Spam E-Mail Detection is shown in Figure 1. The Enron Corpus, a dataset of real-world email examples gathered at Enron Corporation in 2002 during the investigation following the company's bankruptcy. The dataset consists of more than 600,000 emails by 158 employees. In the pre-processing stage, the data is preprocessed by removing the special characters and unnecessary details from the raw data. In each data sample, @ and # symbols are counted in data pre-processing, and from original corpus's@ and # counts are removed.

For Spam detection, text analysis is an essential component, and emails' content must be normalized. It is represented as feature vectors for any spam detection model to work. ns the first step, unprocessed text data is tokenized. The model can analyze by obtaining the data in number of phases. The email content is splitted by using the tokenization technique as fundamental processing units known as tokens or features. The individual words are only in tokens, and paper contains text data. By using stemming, the word's morphological variations are then reduced to their base (stem). The English language has two stemmers: PorterStemmer and LancasterStemmer. This paper was selected and evaluated by PorterStemmer (PS). The word's stem is searched by complex method called lemmatization, and root word in this case is called a lemma.

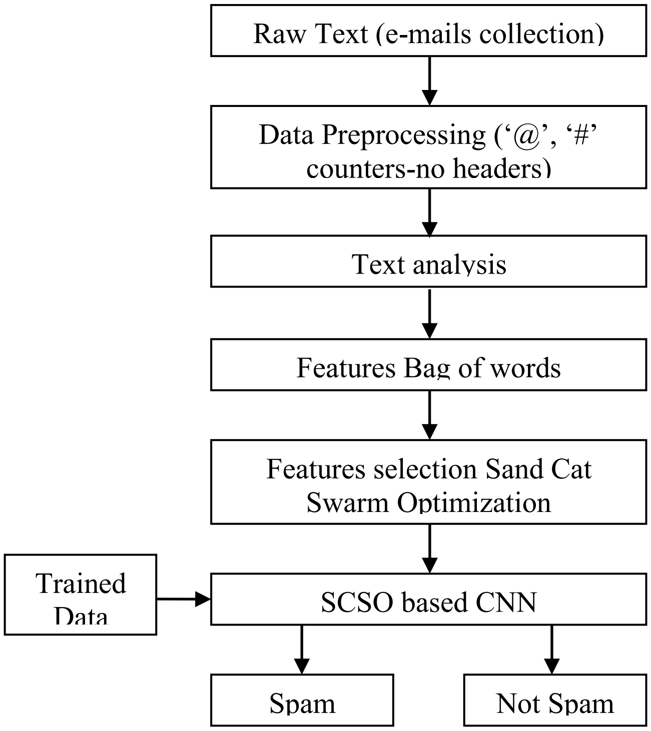
Raw Text (e-mails collection)
Data Preprocessing (‘@’, ‘#’ counters-no headers)
Text analysis
Features Bag of words
Features selection Sand Cat Swarm Optimization
Trained Data
SCSO based CNN
Spam
Not Spam

Figure 1: Block diagram of Deep Learning based Spam E-Mail Detection

By using natural language generation techniques sentences are created. For the generation of sentences, it requires an extensive understanding of syntax, ontology, semantics, other linguistic elements and morphology. Here producing words from a bag of words is considered as main objective. The input is also given from bag of words. The unordered words are in bag of words. Even this is a fundamental unit of a sentence, and it is derived from a grammatically correct sentence. Depending on syntax knowledge, rule-based technique and linguistic rules is used to generate sentences. By taking advantage of the interdependencies that exist between words in language, the approach attempted to create meaningful and coherent sentences.

For the Sand Cat Swarm Optimisation (SCSO) method, sand cats' natural behaviours serve as the model, and in their natural habitat, the sand cats mostly attack animals and carry out attacks. The sand cat's exceptional ability to detect low-frequency noises, which allows them to locate prey both above and below ground with efficiency in this manner. The SCSO method starts by generating a candidate matrix that shows the population of Sand Cat and is moulded by the problem's size (Npop × Nd), and "pop" varies from '1 to n' and "d" represents the dimensions. To determine each Sand Cat's fitness, a particular fitness function is considered. These parameters are iteratively optimised in SCSO, as its primary goal is to find their best values. In this process, fitness assessment is influenced by function value that is produced by associating with each Sand Cat.

Neural Networks (NN) will use fully connected layers. In this, each neuron in one layer is connected to every other neuron in the next layer. This allows for the efficient processing of correlations between any points in the trained vectors, taking their proximity into account. Convolutional Neural Networks (CNNs) are less effective when crucial data is not addressed to the local context. As they are designed to manage local structures. CNNs have the advantage of fewer convolutional layers, which allow for more effective training than fully connected layers.

In the next stage, the collected data is classified into spam and non-spam emails. Performance of the described model is measured by using parameters like Accuracy, Precision and Recall.

IV. Result Analysis

This section presents a performance analysis of the described Enhanced Mechanism for Deep Learning based Spam e-mail detection. The dataset is a collection of real e-mail examples. From the Enron Corpus, raw email data was collected. By using deep learning models, the given attributes were used to correctly identify between spam and genuine emails. The given dataset is classified into trained and test sets, and the majority of the data is used for testing, and 75% is used for training. The performance of the described model is measured using the parameters Accuracy, Precision, and Recall.

Accuracy: Accuracy is the ratio of correct predictions out of all predictions made by an algorithm.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Precision: Precision is ratio of true positives over sum of false positives and true positives. It is called as a positive predictive value.

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Recall: The method correctly identifies number of positive instances.

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

Where,

TP: spam text which is categorized as such, by number of true positives,

TN: genuine text which is categorized as such, by number of true negatives,

FP: genuine text which is categorized as bad, by number of false positives,

FN: spam text which is categorized as good, by number of false negatives,

The performance of described Enhanced Mechanism for Deep Learning based Spam e-mail detection (SCSO based CNN) is compared with email spam detection models based on Support Vector Machine (SVM) and K-Nearest Neighbors (KNN). The comparative performance analysis is presented in Table 1.

Table 1: Comparative performance analysis

Parameters	**Spam E-Mail Detection**		
	SCSO-based CNN	**SVM**	**KNN**
Accuracy	98	91	85
Precision	97.6	90	85
Recall	97	90	84

Accuracy parameter comparative analysis is represented in Figure 2 for the described Enhanced Mechanism for Deep Learning based Spam e-mail detection (SCSO-based CNN), email spam detection models based on SVM and KNN. It is observed that, Accuracy percentage is high for described model.

Figure 3 shows a comparative analysis of the Precision parameter for Spam email detection using the described SCSO-based CNN, SVM, and KNN. The precision of the described model is higher than that of other classifier models.

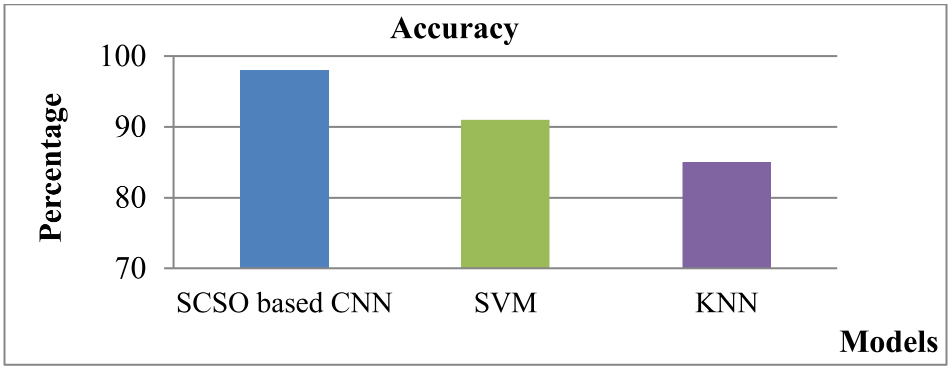

Figure 2: Comparative analysis in terms of Accuracy

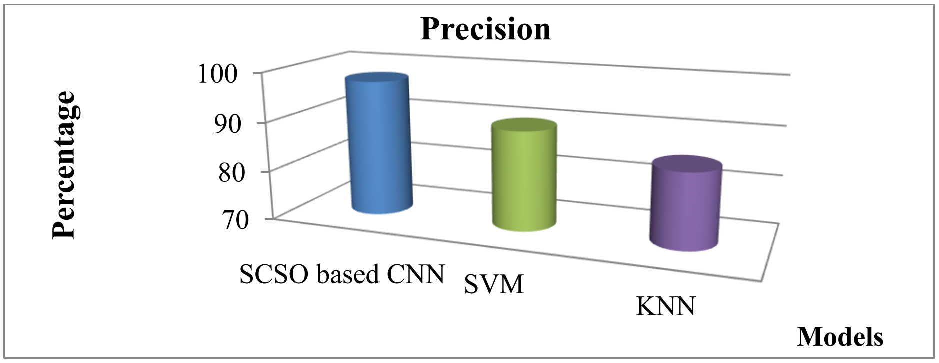

Figure 3: Comparative analysis in terms of Precision

Comparative graphical analysis of the Recall parameter for the described Enhanced Mechanism for Deep Learning based Spam e-mail detection (SCSO-based CNN), email spam detection models based on SVM and KNN are shown in Figure 4. The recall parameter percentage is higher for the described model than for other models.

From the overall analysis, it is found that the described Enhanced Mechanism for Deep Learning-based Spam e-mail detection is efficient across all parameters. The obtained percentage values for the described model are Accuracy as 98%, Precision as 97.6% and Recall as 97%.

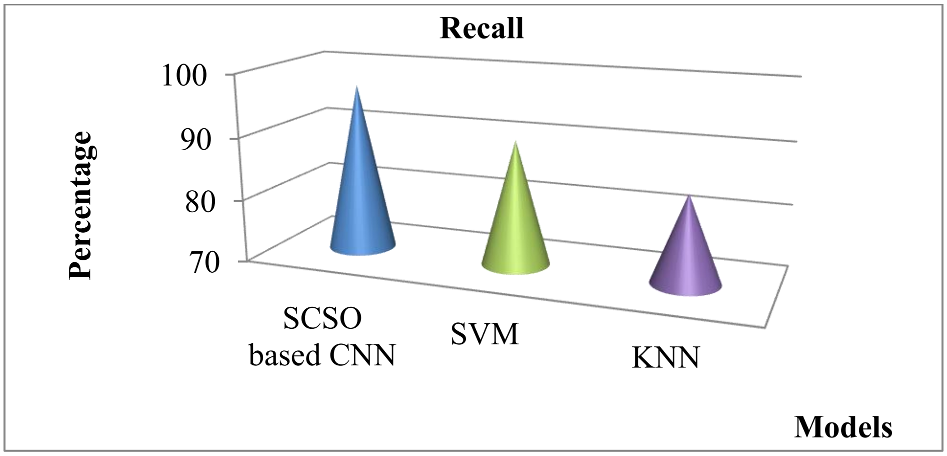

Figure 4: Comparative analysis in terms of Recall

V. Conclusion

In this paper, An Enhanced Mechanism for deep learning-based spam email detection is described. Sending emails or unwanted messages on unauthorised websites frequently results in spam emails due to the sharing of our email addresses. Detecting spam emails requires maintaining the security and integrity of email communication. The dataset is a collection of real e-mail examples. From the Enron Corpus, raw email data was collected. This paper describes a method for identifying undesired emails using deep learning models fine-tuned with the Sand Cat Swarm Optimisation (SCSO) method. The performance of the described model is measured using the Accuracy, Precision, and Recall metrics. From the overall analysis, it is found that the described Enhanced Mechanism for Deep Learning-based Spam e-mail detection is efficient across all parameters. The obtained percentage values for the described model are: Accuracy 98%, Precision 97.6%, and Recall 97%.

References

[1] R. Wongwatkit, M. Raktham and T. Phawananthaphuti, "Intelligent Blacklist Security System for Protecting Spammer in Corporate Email Solution: A Case of Corporate Email Service Provider in Thailand," 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, Republic of, 2022, pp. 387-391, doi: 10.23919/ICACT53585.2022.9728878.

[2] M. Habib, H. Faris, M. A. Hassonah, J. Alqatawna, A. F. Sheta and A. M. Al-Zoubi, "Automatic Email Spam Detection using Genetic Programming with SMOTE," 2018 Fifth HCT Information Technology Trends (ITT), Dubai, United Arab Emirates, 2018, pp. 185-190, doi: 10.1109/CTIT.2018.8649534.

[3] S. Stryczek et al., "CyberDART: A Corporate Federation System for Mitigating Email Threats," in IEEE Access, vol. 12, pp. 189344-189358, 2024, doi: 10.1109/ACCESS.2024.3516657.

[4] H. Shen and Z. Li, "Leveraging Social Networks for Effective Spam Filtering," in IEEE Transactions on Computers, vol. 63, no. 11, pp. 2743-2759, Nov. 2014, doi: 10.1109/TC.2013.152

[5] C. -Y. Tseng, P. -C. Sung and M. -S. Chen, "Cosdes: A Collaborative Spam Detection System with a Novel E-Mail Abstraction Scheme," in IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 5, pp. 669-682, May 2011, doi: 10.1109/TKDE.2010.147.

[6] G. Mujtaba, L. Shuib, R. G. Raj, N. Majeed and M. A. Al-Garadi, "Email Classification Research Trends: Review and Open Issues," in IEEE Access, vol. 5, pp. 9044-9064, 2017, doi: 10.1109/ACCESS.2017.2702187.

[7] J. Mythili, B. Deebeshkumar, T. Eshwaramoorthy and J. N. Ajay, "Enhancing Email Spam Detection with Temporal Naive Bayes Classifier," 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2024, pp. 1-6, doi: 10.1109/IC3IoT60841.2024.10550229.

[8] R. Agarwal et al., "A Novel Approach for Spam Detection Using Natural Language Processing with AMALS Models," in IEEE Access, vol. 12, pp. 124298-124313, 2024, doi: 10.1109/ACCESS.2024.3391023.

[9] D. Liu and J. -H. Lee, "CNN Based Malicious Website Detection by Invalidating Multiple Web Spams," in IEEE Access, vol. 8, pp. 97258-97266, 2020, doi: 10.1109/ACCESS.2020.2995157.

[10] G. Kambourakis, G. D. Gil and I. Sanchez, "What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security," in IEEE Access, vol. 8, pp. 130066-130081, 2020, doi: 10.1109/ACCESS.2020.3009122.

[11] R. Valecha, P. Mandaokar and H. R. Rao, "Phishing Email Detection Using Persuasion Cues," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 747-756, 1 March-April 2022, doi: 10.1109/TDSC.2021.3118931

[12] K. Dan, N. Kitagawa, S. Sakuraba and N. Yamai, "Spam Domain Detection Method Using Active DNS Data and E-Mail Reception Log," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 896-899, doi: 10.1109/COMPSAC.2019.00133.

[13] T. Georgieva-Trifonova, "Research on Filtering Feature Selection Methods for E-Mail Spam Detection by Applying K-NN Classifier," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-4, doi: 10.1109/HORA55278.2022.9799999.

[14] R. Indu and S. C. Dimri, "Detecting Spam E-mails with Content and Weight-Based Binomial Logistic Model," in Journal of Web Engineering, vol. 22, no. 7, pp. 939-959, October 2023, doi: 10.13052/jwe1540-9589.2271.

[15] G. Al-Rawashdeh, R. Mamat and N. Hafhizah Binti Abd Rahim, "Hybrid Water Cycle Optimization Algorithm with Simulated Annealing for Spam E-mail Detection," in IEEE Access, vol. 7, pp. 143721-143734, 2019, doi: 10.1109/ACCESS.2019.2944089

[16] S. A. A. Ghaleb, M. Mohamad, S. A. Fadzli and W. A. H. M. Ghanem, "Training Neural Networks by Enhance Grasshopper Optimization Algorithm for Spam Detection System," in IEEE Access, vol. 9, pp. 116768-116813, 2021, doi: 10.1109/ACCESS.2021.3105914.

[17] A. Karim, S. Azam, B. Shanmugam and K. Kannoorpatti, "An Unsupervised Approach for Content-Based Clustering of Emails into Spam and Ham Through Multiangular Feature Formulation," in IEEE Access, vol. 9, pp. 135186-135209, 2021, doi: 10.1109/ACCESS.2021.3116128.

[18] S. Gibson, B. Issac, L. Zhang and S. M. Jacob, "Detecting Spam Email With Machine Learning Optimized With Bio-Inspired Metaheuristic Algorithms," in IEEE Access, vol. 8, pp. 187914-187932, 2020, doi: 10.1109/ACCESS.2020.3030751.

[19] J. -S. Kim, H. -J. Lee, H. -J. Lee and S. -H. Choi, "Advanced Analysis of Learning-Based Spam Email Filtering Methods Based on Feature Distribution Differences of Dataset," in IEEE Access, vol. 12, pp. 167313-167323, 2024, doi: 10.1109/ACCESS.2024.3495830.

[20] M. Hina, M. Ali, A. R. Javed, F. Ghabban, L. A. Khan and Z. Jalil, "SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning," in IEEE Access, vol. 9, pp. 98398-98411, 2021, doi: 10.1109/ACCESS.2021.3095730

[21] I. L. d. Oliveira, J. L. Corrêa and A. M. Cansian, "Using the Euclidean Distance as a Mechanism Distance between Signatures to the Detect Spam and Phishing Scams," in IEEE Latin America Transactions, vol. 8, no. 4, pp. 340-348, Aug. 2010, doi: 10.1109/TLA.2010.5595123

[22] S. Maroofi, M. Korczyński, A. Hölzel and A. Duda, "Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3184-3196, Sept. 2021, doi: 10.1109/TNSM.2021.3065422.

[23] Yujia Fang, Gabriela Mogos, “Detecting attacks on e-mail,” Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 33, no. 3, 2024, doi.org/10.11591/ijeecs.v33.i3.pp1576-1588

[24] Sean Eljim S. Castelo, Ruben Jolo L. Apostol IV, Dan Michael A. Cortez, Raymund M. Dioses, Mark Christopher R. Blanco, Vivien A. Agustin, “Modification of SHA-512 using Bcrypt and salt for secure email hashing,” Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol 33, no. 1, 2024, doi.org/10.11591/ijeecs.v33.i1.pp398-404

[25] Souad Larabi-Marie-Sainte, Sanaa Ghouzali, Tanzila Saba, Linah Aburahmah, Rana Almohaini, “Improving spam email detection using deep recurrent neural network,” Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol 25, no. 3, 2022, doi.org/10.11591/ijeecs.v25.i3.pp1625-1633