Journal of Current Research in Engineering and Science
Bi-Annual Online Journal ( ISSN: 2581 - 611X )
VOLUME:8, ISSUE:1, FEBRUARY 2025, PAPER NUMBER:09

# An Efficient Analysis of Email Spam Detection Using Deep Learning Algorithms

Dr. R. Sabitha
*Professor,*
*Department of Computer Science and Engineering,*
*Rajalakshmi Engineering college,* Tamil Nadu, India
sabitha.r@rajalakshmi.edu.in

Deepak S
*UG Students, Department Computer Science and Engineering,*
*Rajalakshmi Engineering college,*
Tamil Nadu, India
200701056@rajalakshmi.edu.in

Narendran R
*UG Students, Department Computer Science and Engineering,*
*Rajalakshmi Engineering college,*
Tamil Nadu, India
200701524@rajalakshmi.edu.in

*Abstract*— **Email spam remains a persistent challenge in modern communication, necessitating advanced techniques for efficient detection and mitigation. This work presents a comprehensive analysis of email spam detection utilizing a hybrid approach that combines traditional machine learning algorithms, such as Naive Bayes and Random Forest, with a state- of-the-art deep learning algorithm, Long Short-Term Memory (LSTM) & Recurrent Neural Network. The work begins by exploring the effectiveness of Naive Bayes, a probabilistic algorithm known for its simplicity and efficiency in text classification. the Deep Learning Algorithm utilized in this study harnesses the power of neural networks to automatically learn and extract intricate patterns from email data. We investigate its performance in distinguishing between spam and legitimate emails based on various features, including sender information, email content, and structural characteristics. This work incorporates Random Forest, a powerful ensemble learning method, to enhance the accuracy and robustness of spam detection. LSTM networks excel at capturing dependencies and long-range contextual information, making them suitable for detecting nuanced patterns indicative of spam emails. By leveraging the collective decision-making of multiple decision trees, Random Forest addresses potential limitations of individual classifiers and provides a more reliable email filtering mechanism. To further improve the detection capabilities, this work integrates LSTM Recurrent Neural Network, a deep learning architecture specifically designed for sequence data. The LSTM model excels in capturing temporal dependencies within email content, allowing for more nuanced analysis and identification of spam patterns that may evolve over time.**

*Keywords*— ***Random Forest, Accuracy, Efficiency, Evolving spam techniques, Naïve Bayes, long short- term memory, Recurrent neural network.***

## INTRODUCTION

In today's interconnected digital landscape, email communication stands as one of the most worlds widely used mediums for personal, professional, and organizational correspondence. However, this convenience comes with a significant drawback; the rapid increase of email spam. Email spam not only inundates users with irrelevant and unsolicited message but also poses potential security threats, including phishing attacks and malware dissemination. The evolution of spamming techniques, becoming increasingly sophisticated and evasive, has rendered traditional spam filters less effective, necessitating innovative approaches to combat these threats. This work, delves into the domain of "An efficient analysis of email spam detection using seep learning algorithm," Aiming to combine the strengths of both classical machines learning and deep learning algorithms. Specifically, this work focuses on the integration of Naïve Bayes, a classic probabilistic classifier, and Long Short-Term Memory Networks (LSTM), a sophisticated type of Recurrent neural network (RNN), to enhance the efficiency and accuracy of email spam detection systems.

This motivation of work is driven by the goal of utilizing the complimentary abilities of LSTMs and Naïve Bayes. Our goal is to develop a hybrid model that combines the precision and efficiency of email spam detection with deep learning's nuanced understanding of contextual information. This will reduce false positives and improve detection accuracy by combining the probabilistic nature of Naïve Bayes with LSTMs' deep learning capabilities.

The work is organized as follows with the literature survey in section II which is followed by the methodologies used on spam detection in section III and the conclusion in section VI.

## I. EXISTING MODEL

Exploring the broader landscape of relevant research and technologies is pivotal before delving into our proposed system. This literature survey provides a comprehensive overview of existing research on email spam detection, emphasizing the integration of Naive Bayes with DLAs and LSTMs. The studies reviewed collectively underscore the 1 need for a holistic approach, leveraging the strengths of traditional and advanced techniques for effective and adaptive email spam detection. The proposed journal paper will contribute to this evolving landscape by presenting an integrated model that addresses the limitations of individual methods.

Here we will be discussing the different techniques and approaches that were used in many research papers.

Isra 'a AbdulaNabi, Qussai Yaseen **[1]** The issue of identifying spam emails and the use of deep learning methods to this problem—more especially, the BERT (Bidirectional Encoder Representations from Transformers) model. The BERT model's performance is compared to that of traditional classifiers like Naive Bayes and k-NN (k-nearest neighbors), as well as a baseline deep neural network (DNN) model. They assess each model's accuracy and F1 score after using two open-source datasets for training and testing. The findings demonstrate that the BERT model is the most successful in categorizing spam emails, with the maximum accuracy of 98.67% and F1 score of 98.66%.

Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Mamoun Alazab **[2]** This paper provides a thorough analysis of intelligent spam email detection. It examines several methods and frameworks for identifying and categorizing spam emails, with an emphasis on machine learning (ML) and artificial intelligence (AI) techniques. The use of methods including adaptive spam filters, genetic algorithms, fuzzy logic, and particle swarm optimization is covered in the text.

Xiaoxu Liu, Haoye Lu, Amiya Nayak **[3]** A modified Transformer model for SMS spam detection is proposed in this paper. Two datasets are used to assess the model, and it is contrasted with different deep learning techniques and machine learning classifiers. The outcomes demonstrate that the suggested model has good accuracy, recall, and F1-Score on

both datasets. The model obtains the greatest performance on the UtkMl's Twitter dataset and outperforms other classifiers on the SMS Spam Collection
v.1 dataset. Nevertheless, the model is impacted by unfamiliar terms, which occasionally impairs its functionality. Future work to solve the problem of unknown words, expand the model to bigger datasets, and investigate enhanced models based on the Transformer are suggested in the study. Overall, the suggested updated Transformer model appears to be a promising method for identifying SMS spam.

Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Mamoun Alazab **[4]** An unsupervised method for grouping emails into spam and ham categories is covered in the paper. A sophisticated and automatic anti-spam framework is required due to the exponential increase in spam email attacks. Based on topic headers and content, the paper suggests using unsupervised learning algorithms to cluster spam and ham emails. A unique binary dataset of 22,000 emails with ten attributes designed to reflect email properties is created by the study. After examining five clustering methods, it is discovered that OPTICS yields the best clustering outcomes. For OPTICS and DBSCAN, the average balanced accuracy is around 75.76%. Additionally, a thorough summary of relevant studies in the area of spam email detection is included in the publication. Overall, the study shows how successful email grouping can be achieved by unsupervised learning, and clustering and spam detection.

B. Natarajan, R. Elakkiya, R. Bhuvaneswari, Kashif Saleem, Dharminder Chaudhary, Syed Husain Samsudeen **[5]** The work is to create a hybrid model for warning message generation and wild animal activity detection dubbed Hybrid VGG-19+Bi-LSTM. To achieve high recognition accuracy, the model makes use of fine-tuned hyperparameters and deep neural networks. It accurately recognizes animals in photos and videos by applying object detection and classification algorithms. After testing on a number of benchmark datasets, the suggested model outperformed earlier methods in terms of performance. To assist foresters in keeping an eye on and responding to animal activity, it provides speedier SMS alert services and forecast performance that is more accurate. The project's main goal is to reduce animal suffering and save human lives by delivering accurate information based on animals.

Simran Gibson, Biju Issac, Li Zhang and Seibu Mary Jacob **[6]** This work was to identify spam emails by applying bioinspired metaheuristic algorithms and machine learning techniques. The performance of several algorithms used in the studies was compared by the researchers. To optimize the classifiers, they used bioinspired techniques such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). The best overall performance was achieved by Multinomial Naïve Bayes with Genetic Algorithm, according to the results. Utilizing programs like Scikit- Learn and WEKA to implement and assess the models was another aspect of the research.

Rati Bhan, Parvez Faruki, and Rajendra Pamula **[7]** A system for identifying hidden harmful activity in Android applications is proposed in this study. The methodology finds hidden functionality that adversaries might exploit by using inter-component control-flow analysis and data flow analysis. It is capable of identifying private functions like SMS, phone calls, and audio and video recording that are utilized improperly and without the user's express permission. The framework has a high detection rate and low false positive rate when tested against known malware, benign applications, and disguised malicious apps. It works better than current cutting-edge methods and is capable of successfully identifying harmful activity that is hidden within Android applications..

Long Chen, Chunhe Xia, Shengwei Lei, and Tianbo Wang **[8]** This work identification, tracking, and dissemination of mobile malware threats are the main topics of this work report. It investigates several virus dissemination scenarios, including social networks, Bluetooth, SMS/MMS, and SMS. The creation of a mobile Internet big data knowledge graph and the use of machine learning methods to malware detection are covered in the paper. Additionally, it emphasizes how crucial it is to safeguard the ecology of mobile Internet use and suggests security precautions.

Souad Larabi, Marie-Sainte, Sanaa Ghouzali, Tanzila Saba, Linah Aburahmah, Rana Almohaini **[9]** The work concludes that deep literacy ways, specifically the use of deep intermittent neural networks (RNN), are effective in perfecting spam dispatch discovery. The paper proposes a fashion using RNN with different configurations of activation function, powerhouse rate, and number of ages. The loftiest delicacy achieved in the trials was99.7 using Tanh as the activation function, a powerhouse rate of0.1, and 100 ages. The proposed RNN model outperforms former studies and shows promising results in spam dispatch discovery.

Chillakuru Neeharika, and Kalaiarasi **[10]** This work aims to ameliorate the delicacy of dispatch spam vaticination using machine literacy algorithms. Specifically, it compares the performance of the Novel intermittent Neural Network (RNN) and the Artificial Neural Network (ANN) in prognosticating dispatch spammers. The study was conducted at the Saveetha School of Engineering and comported of two groups, each with a sample size of 10. The Novel RNN achieved a delicacy of 97.96, while the ANN had a delicacy of93.79. The results showed that the Novel RNN outperformed the ANN in prognosticating dispatch spam.

Zhi-Yan and Peng Zeng **[11]** This work proposes an effective each- or- nothing public key encryption scheme with authenticated equivalency test (AoN- PKEAET). The scheme improves upon being schemes by adding a ciphertext authentication operation before the plaintext equivalency test, icing accurate results. It's grounded on the separate logarithm problem and utilizes cryptographic hash functions. The scheme achieves effectiveness with smaller exponentiation operations compared to former schemes. The security of the scheme is proven under a readdressed security model.

Sanaa Ghaleb, Mumtazimah Mohamad, Waheed Ali H. M. Ghanem, Abdullah Nasser, **[12]** This work focuses on developing a spam discovery system (SDS) using amulti-objective optimization approach. The proposed system utilizes the grasshopper optimization algorithm (GOA) for point selection and the revised EGOA algorithm for training neural networks. The study aims to ameliorate the performance and delicacy of SDS by opting applicable features from dispatch dispatches. The system's effectiveness is estimated using three spam datasets, and it outperforms being styles in terms of delicacy.

Pavan Kumar Chaganti and Mohd Hafizi Ahmad **[13]** This work focuses on the development of a fiber optical aural detector (FOAS) for detecting partial discharge (PD) events in power mills. The FOAS is grounded on a single- mode fibre-multimode fiber-single- mode fiber (SMS) structure with a thin polymer diaphragm. The diaphragm enhances the perceptivity of the detector to aural pressure swells generated by PD events. The FOAS was characterized using both Band and tunable light sources, and it achieved a high perceptivity and signal- to-noise rate (SNR) in both air and oil painting media.

Mani, Gunasekaran and Geetha **[14]** This work focuses on email spam detection using a Gated Recurrent Neural Network (GRU). The goal is to filter spam emails based on their content. The work uses open-source Keras neural network software and tokenizes the data by converting characters into integers. The GRU model is trained using a dataset of spam messages and achieves a high accuracy rate of 98.7%. The work also discusses the limitations of other spam detection methods like KNN and proposes the advantages of using GRU.

Ghada Al-Rawashdeh, Rabiei Mamat and Noor Hafhizah Binti Abd Rahim **[15]** This work focuses on improving the accuracy of spam email detection by using a hybrid Water Cycle Optimization Algorithm (WCA) with Simulated Annealing (SA) for feature selection. The work shows that the hybridization of WCA with SA outperforms other feature selection algorithms. The accuracy achieved with the hybridization is 96.3%, and the SVM classifier performs the best among the three classifiers tested. The number of features is reduced by more than 50% using the hybridization.

Mohammad Alauthman **[16]** This work employs a deep recurrent neural network to detect spam emails from botnets. For efficient spam identification, the study suggests using a Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) in conjunction with Support Vector Machines (SVM). The work talks about the benefits of employing botnets to send spam as well as the difficulties in detecting spam emails. It also contrasts the suggested strategy with alternative machine learning algorithms and offers a summary of previous research on the subject. The GRU-SVM technique achieves a high accuracy rate of 98.7%, according to the experimental data.

Karishma, Akila and Govindasamy **[17]** This work addresses the issue of spam and suggests utilizing recurrent neural networks (RNNs) with a BiGRU model as a means of solving it. The experimental analysis of hyperparameters for the suggested models is presented in the report along with a discussion of the shortcomings of current methods. When compared to other machine learning and deep learning methods, the BiGRU model performs well, displaying a high accuracy of 99.07%. The dataset and evaluation metrics that were utilized to gauge the model's performance are also covered in length in the work.

Nazeeh Ghatasheh, Ismail Altaharwa and Khaled Aldebei **[18]** The main goal of this work is to create a modified genetic algorithm (GA) that leverages the XGBoost method for feature selection and hyperparameter optimization in spam detection. The researchers discuss the difficulties of detecting spam on social networking sites, especially Twitter, which has an uneven distribution of data and a wide feature space. The suggested method makes advantage of GA to concurrently minimize the feature space's dimensionality and optimize the XGBoost classifier's parameters.

Kulwinder Kaur and Mukesh Kumar **[19]** The work main objective is to identify spam in emails by applying several categorization techniques. The researchers suggest a new approach for categorizing unsolicited emails as well as a methodology for preparing data. For the purpose of categorization, they create extensive lists of spam words, which they then compare to emails that have been manually classified. As classification methods, the paper also presents the ideas of KNN, Back Propagation Neural Network, and Recurrent Neural Network. Using the Enron dataset, the effectiveness of different methods is examined, and the RNN algorithm is determined to be the most accurate.

Sanaa Ghaleb, Mumtazimah Mohamad, Syed Abdullah Fadzli and Waheed Ali Ghanem **[20]** This work introduces a novel framework for the Spam Detection System (SDS) that uses Multilayer Perceptron (MLP) and an extended Grasshopper Optimization Algorithm (EGOA) for advanced spam email detection. When compared against alternative optimization techniques, the suggested framework outperforms them in terms of accuracy, detection rate, and false alarm rate across three distinct spam datasets. The Grasshopper Optimization Algorithm (GOA) and its variants, which are used to optimize the MLP's parameters, are also introduced in the work.

**Table 1:** Advantages and Disadvantages of some popular techniques used in the supply chain

| Technique | Advantage | Disadvantage |
|---|---|---|
| Naive Bayes: | • handle both numerical and categorical data, | •It can sensitive to the quality of the input data, |
| Random Forest: | • Handle large datasets with high dimensionality. | • Not perform well on imbalanced in the datasets. |
| Recurrent Neural Networks (RNNs): | •It captures the sequential dependencies in the input data. | • expensive to train, the data especially for long sequences and large datasets. |
| Long Short-Term Memory (LSTM) Networks: | •the vanishing gradient problem can be handled. | • complex to train and tune, may still require a large amount of labeled data. |

## IV. PROPOSED FRAMEWORK

Our work proposed various in order to identify and categorize spam and spammers, our experimenters suggested vibrant spam discovery techniques. Semantically- grounded techniques and geste pattern-grounded approaches make up the two main categories of being spam discovery strategies. These methods have drawbacks and restrictions. Spam emails have increased significantly in tandem with the arrival of the Internet and global communication.

### *A.* System Architecture

The work consists of two Phases (i.e., the Testing Phase and Training Phase). Initially, the dataset is preprocessed and split into two parts based on the 80/20 splitting ratio. The two machine learning models as well as the other two deep learning models are trained with the 80% data which is obtained after the data split. Further, the trained models are tested with 20% of the test data obtained after the data split. The metrics are produced after the testing process. Then the metrics of the algorithms are analyzed and results are achieved. The achieved results are fetched from the back-end through the use of API and showcased to the user via a user-interactive website.

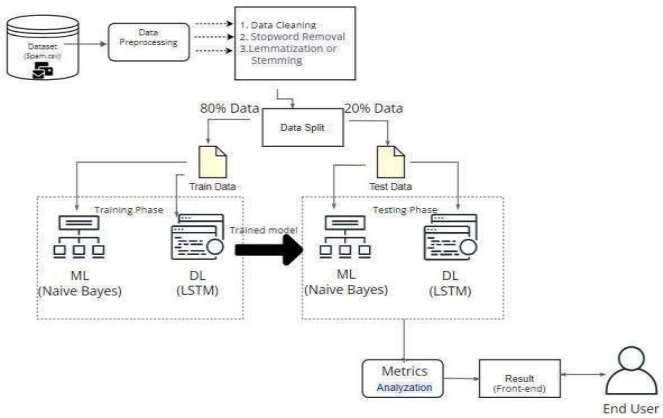


**Fig 1. Architecture Diagram**

### *B. Function Involved*

The procedure involves many functions. These functions are employed in a number of different activities, including training, assessment, prediction, model construction, and data preparation. The following are some typical, often utilized functions:

#### *[1]* Dataset Collection:

Acquire a diverse dataset of labeled emails, including both spam and non-spam instances. Ensure the dataset represents real-world scenarios and includes variations in email content, sender information, and structural characteristics.

Dataset Information

| LABEL | COUNT |
|---|---|
| Spam | 4825 |
| Ham | 747 |
| Total | 5572 |

**Fig 3. Dataset collection**

### *[2]* Data Preprocessing:

Cleanse the dataset by removing irrelevant information, such as HTML tags, special characters, and irrelevant metadata. Tokenize and vectorize the email content, transforming it into a format suitable for machine learning algorithms. Extract relevant features, including sender information, email content, and structural characteristics.

### *[3]* Training the data

Function to use mini-batch gradient descent or Adam optimization to train the deep learning model on the training data. In order to keep an eye on the model's performance and avoid overfitting, it can be functionally validated on a different validation set. The early stopping function is designed to stop the model from training once the validation loss ceases to decrease.

### *[4]* Naive Bayes Algorithm:

Apply and train a Naive Bayes classifier using the preprocessed dataset. estimate the performance of the Naive Bayes algorithm using criteria similar as delicacy, perfection, recall, and F1 score..

### *[5]* Random Forest Algorithm:

Implement and train a Random Forest classifier using the preprocessed dataset. Fine-tune hyper-parameters to optimize the Random Forest model. Evaluate the performance of the Random Forest algorithm using the same metrics.

### *[6]* LSTM & Recurrent Neural Network:

Implement and train an LSTM & Recurrent Neural Network using the preprocessed sequence data of email content. Consider hyper-parameter tuning and model architecture adjustments for optimal performance. Evaluate the LSTM model's performance using appropriate metrics.


**Fig 4. Training for LSTM**

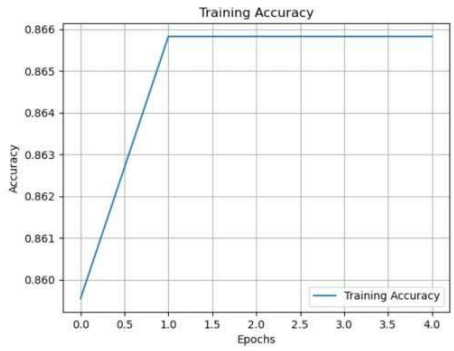


**Fig 5. Training for RNN**

### *[7]* Integration of Algorithms:

Combine the outcomes of Naive Bayes, Random Forest, and LSTM to create an integrated model. Explore ensemble techniques or weighted voting mechanisms to leverage the strengths of each algorithm.

### *[8]* Performance Evaluation:

Assess the individual and combined performance of the algorithms using a comprehensive set of metrics. Consider the trade-offs between precision, recall, and overall accuracy.

### *[9]* Cross-Validation:

Apply cross-validation ways to insure the robustness of the models and alleviate overfitting.

### *[10]* Comparison and Analysis:

Compare the performance of individual algorithms against the integrated model. dissect the strengths and sins of each algorithm in secerning between spam and licit emails.

### *[11]* Result Interpretation

Provide a detailed interpretation of the results, highlighting the effectiveness of the integrated approach. Discuss any observed patterns or challenges in spam detection across different algorithms. Final Accuracy status given below:

| Metrics | Naive Bayes | Random Forest | LSTM | RNN |
|---|---|---|---|---|
| Accuracy | 98.74 | 94.11 | 86.84 | 98.03 |
| Precison | 98.56 | 99.40 | | |
| Loss | | | 0.4003 | 0.1744 |
| | | | | |

**Fig 5.**
**Metrics**

## VI. CONCLUSION

In summary, our work scrutinized a variety of algorithms for spam detection, spanning both machine learning (Naive Bayes and Random Forest) and deep learning (LSTM and RNN) methodologies, leading to the deployment of four distinct models. Noteworthy among these, Naive Bayes boasted the highest accuracy rate of 98.74%, contrasting with LSTM's lower accuracy of 86.84%. RNN, however, edged past LSTM with an accuracy of 98.03%, while Random Forest achieved a respectable accuracy of 94.11%. We discerned a pattern wherein LSTM's accuracy tended to improve as the dataset size expanded, whereas RNN's performance remained stable or slightly declined with increased dataset sizes. Of particular significance is the observation that in the realm of spam detection, where datasets encompass

several thousand instances, Naive Bayes outshone LSTM, while RNN displayed promise with smaller datasets. These findings accentuate the nuanced interplay between model performance and dataset characteristics, with Naive Bayes emerging as a sturdy choice for moderate dataset sizes, while RNN demonstrates potential efficacy for smaller-scale datasets. Such insights deepen our comprehension of model selection considerations in the domain of spam detection applications.

## REFERENCES

**[1]** Kumar, P., Kumar, S.V. (2023). DDoS Attack Prediction System Using Machine Learning Algorithms. In: Tuba, M., Akashe, S., Joshi, A. (eds) ICT Systems and Sustainability. ICT4SD 2023. Lecture Notes in Networks and Systems, vol 765. Springer, Singapore.

**[2]** Ananthajothi, K., Rajasekar, P. & Amanullah, M. Enhanced U-Net-based segmentation and heuristically improved deep neural network for pulmonary emphysema diagnosis.

**[3]** Ananthajothi K, Karthick T, Amanullah M, Automated rain fall prediction enabled by optimized convolutional neural network-based feature formation with adaptive long short- term memory framework. Concurrency Computat Pract Exper. 2022;

**[4]** Isra'a AbdulNabi and Qussai Yaseen, "Spam email detection using deep learning techniques," 2021 the 2nd International workshop on data-driven security (DDSW), Warsaw, Poland, March 2021.

**[5]** Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti and Mamoun Alazab, "A comprehensive survey for intelligent spam email detection," 2019 International Conference on Computer Communication and Informatics (ICCCI).2019.

**[6]** Xiaoxu Liu, Haoye Lu and Amiya Nayak, "A Spam transformer model for SMS spam detection," School of electrical engineering and computer science, university of Ottawa, Canada, May 2021.

**[7]** Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti and Mamoun Alazab, "An unsupervised approach for content-based clustering of emails into spam and ham through multangular feature formulation," College of engineering, IT and environment, Charles Darwin University, Australia 2021.

**[8]** B. Natarajan, R. Elakkiya, R. Bhuvaneswari, Kashif Saleem, Dharminder Chaudhary and Syed Husain Samsudeen, "Creating alert message based on wild animal activity detection using hybrid deep neural networks," King Saud university, Riyadh, Saudi Arabia 2023.

**[9]** Simran Gibson, Biju Issac, Li Zhang and Seibu Mary Jacob, "Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms," Teesside University, October 2020.

**[10]** Rati Bhan, Parvez Faruki and Rajendra Pamula, "Detection of sensitive malicious android functionalities using inter- component control-flow analysis," Indian school of mines, Dhanbad, 2019.

**[11]** Long Chen, Chunhe Xia, Shengwei Lei and Tianbo Wang, "Detection, Traceability and Propagation of mobile malware threats," January 2021.

**[12]** Souad Larabi-Marie-Sainte, Sanaa Ghouzali, Tanzila Saba, Linah Aburahmah, Rana Almohaini, "Improving spam email detection using deep learning recurrent neural network", Prince Sultan University, Saudi Arabia, 2022.

**[13]** Chillakuru. Neeharika, Kalaiarasi, "Comparison of novel recurrent neural network over artificial neural network in predicting email spammers with improved accuracy," India, 2023.

**[14]** Zhi Yan Zhao and Peng Zeng, "Efficient all or nothing public key encryption with authenticated equality test," East China normal University, Shanghai, 2021.

**[15]** Sanaa Ghaleb, Mumtazimah Mohamad, Waheed Ali Ghanem, Abdullah Nasser, Mohamed Ghetas, "Feature selection by multi objective optimization application to spam detection system by neural networks and grasshopper optimization algorithm," Finland, 2022.

**[16]** Pavan Kumar Chaganti, Mohd Hafizi Ahmad, Mohamed Afendi Maohamed Piah, Muhammad Yusof Mohd Noor, "Fiber optic acoustic sensor based on SMS structure with thin polymer diaphragm for partial discharge detection," Malaysia, 2020.

**[17]** Mani, Gunasekaran and Geetha, "Email spam detection using gated recurrent neural network," Dr.M.G.R educational and research institute, India April 2023.

**[18]** Ghada Al-Rawashdeh, Rabiei Mamat, and Noor Hafhizah binti ABD Rahim, "Hybrid water cycle optimization algorithm with simulated annealing for spam email detection," Malaysia, September 2019.

**[19]** Mohammad Alauthman, "Botnet spam email detection using deep learning recurrent neural network," Zarqa University, Zarqa, Jordan, May 2020.

**[20]** Kulwinder Kaur and Mukesh Kumar, "Spam detection using KNN, back propagation and recurrent neural network" Panjab University, Chandigarh, 2015.