Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 20s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

A Hybrid Fully Homomorphic Encryption Based Privacy Preserving DeepCNN Framework for Email Spam Classification

Dr. T.Poonkodi[1], Dr. M.Subathra[2]

[1]Assistant Professor, Department of Computer Science, Hindusthan College of Science and Commerce, Ingur, Erode, India.
Email ID: ponrohit.0707@gmail.com

[2]Assistant Professor, Department of Computer Applications, Vellalar College For Women, Erode, India.
Email ID: subathra@vcw.ac.in

Cite this paper as: Dr. T.Poonkodi, Dr. M.Subathra, (2025) A Hybrid Fully Homomorphic Encryption Based Privacy Preserving DeepCNN Framework for Email Spam Classification. *Journal of Neonatal Surgery*, 14 (20s), 121-129.

ABSTRACT
The E-mail filtering systems have been designed mainly to identify spam and either block it or put it in the spam folder. An effective adaboost sequential classification based ensemble method used where the differential grading weighting schemes are used to classify the results more accurately as nonspam emails are delivered to inbox and spam emails are stored in filtering system folder. The execution of the spam action would be impaired by the lack of effective strategies to deal with threats to the security of the spam filter. The need to apply deep learning to spam filtering to leverage its many layers of processing and multiple levels of abstraction to learn data representations. In this Paper, the effect of implementing the filtering spam emails in email spam filtering system entirely overcome by addressed fully homomorphic encryption based privacy preserving and deep convolution neural network. In deep convolution neural network, an adapted transnet is proposed to increase the spam classification accuracy and reduce communication complexities on the transit layer. The proposed fully homomorphic encryption based protocol concealed with privacy preserving mechanism. Initially, firewall check the spam emails to find IP address, media access control address and domain name. An unauthenticated spam mails are stored in deny list and delivered to trash. In fully homomorphic encryption based privacy preserving and deep convolution neural network, an authenticated spam emails are encrypted using fully homomorphic encryption algorithm then encrypted emails are fed into deep learning classifier. The deep learning classification method classify the encrypted emails as spam and nonspam. The encrypted spam and nonspam emails are send to mail server decrypted and deliver emails to spam folder and inbox. The experiments results prove that the proposed method is better than existing email text spam classification method.

Keywords: *E-mail, Spam Filtering, Fully Homomorphic Encryption, Deep Convolution Neural Network, FHE based Privacy Preserving Protocol*

1. INTRODUCTION

One of the biggest challenges facing researchers is analyzing and reducing spam mail. Spammers send spam to promote business by advertising of selling products online shopping websites. Also send spam messages to hack details of user's personal confidential information by using fake websites appending bank links. Large volumes of spam emails are sent, and these messages contain malware, viruses, trojans, and phishing scams. Problems are arise when number of unwanted mails are come from unknown sites and how to classify the user that email are received which is spam email or ham [1].

Deep Learning is the process of learning abstract representations of data in order to extract features from a number of mediums such as pictures, speech and text data [2]. For each token or word, a single dimension matrix is created and a multidimensional matrix is formed for the complete text sentence. Convolution, activation function, pooling stage and application of softmax function are the four process that make up CNN's architecture [3].

Effective FHE applications nowadays require the direct involvement of a cryptographic professional with adequate knowledge of encryption schemes. At the beginning while Homomorphic Encryption used partial scheme and with the passage of time, researchers advanced a fully Homomorphic Encryption scheme which allowed whole computation on any form of data. Homomorphic encryption strategies may be partly divided into completely Homomorphic Encryption and partially Homomorphic Encryption [4]. As individual homomorphic operations are orders of importance high expensive than equivalent plaintext operations, amortizing the value of individual FHE operations utilizing the vectorization capabilities of the encryption schemes [5].

2. RELATED WORKS

Benavides et al. [6] proposed that each chosen work and classification be combined.They describe the DL calculations used in each arrangement, revealing that the Deep Neural Network (DNN) and Convolutional Neural Network (CNN) are the most commonly used. Various Diverse DL methodologies have been published and analyzed, but there is a research gap in the application of DL computations to cyber-attack detection.

Ajinkya Gulunjkar et al. [7] suggested machine learning and its implementation in the field of spam filtering. In this study, the hybridization of the optimization algorithm and the Neural Network (NN), Particle Swarm Optimization (PSO) and Random Weight Network (RWN) were applied. In order to effectively manage the danger of spam, flaws in machine learning algorithms were identified, and comparative analyses of computer training methodologies in the literature were conducted. Statistics from the literature reviewed and the quantity reviewed suggests substantial improvement in this area overall.

Carlos Laorden et al. [8] offered a modification of the utility of anomaly detection in email spam filtering that reduces the need for classifying email spam messages and only works with the representation of single class of emails. An improvement of the technique that applied a data minimization methodology to the characterized dataset corpus to reduce processing time while maintaining recognition rates, a demonstration of the first anomaly-based spam sieving approach, and an examination of whether choosing spam or non-spam emails is a demonstration of normalcy are all included in the study.

Alhassan Khedr et al. [9] developed an efficient implementation based on Ring Learning With Errors (RLWE) of a variant of the HE system recently proposed by Gentry, Sahai and Waters (GSW). Although this system was generally believed to be less efficient than its contemporaries, the does opposite behavior for a large class of applications. In this study, the algebraic features of the system are achieve significant speedup compared to the snext generation HE implementation, namely the IBM homomorphic encryption library (HElib). Along with the HE implementation, the various optimizations employ the resulting system to construct a homomorphic evaluator for binary decision trees, a secure multiple keyword search, and a homomorphic Bayesian spam filter.

Ahmad Al Badawi et al. [10] proposed PrivFT: Private and Fast Text classification solution for FHE encrypted data. PrivFT provides two services: 1) use a plaintext model that has already been learned to draw conclusions on encrypted data, and 2) train an effective model on encrypted data to produce an encrypted model. PrivFT can be used for a variety of text classification tasks including sentiment analysis, spam detection, and topic classification without compromising the confidentiality of input data privacy. on various datasets PrivFT takes 0.17 seconds per inference (on GPU).

Haseeba Yaseen et al. [11] proposed collaborative spam detection platform referenced in this document offers several advantages in terms of protecting the privacy of all the stakeholders and the amount of data being used. on MapReduce Platforms, the encoding technique used outperforms several distance-preserving hashing techniques in terms of scalability. The bucketing approaches simplified the process by allowing for easy item classification and grouping as well as anomaly detection using histograms, which effectivetly discriminated spam from ham.

3. PROPOSED METHODOLOGY

The proposed FHEPP-DLCM method is described in detail. The firewall checks spammed emails IP address, Domain Name and MAC address. If the emails are unauthenticated, automatically emails delivered to trash. Authenticated emails are encrypted using Fully Homomorphic Encryption Algorithm. The Encrypted emails are classified as spam and nonspam by using DLCM classification method. Both spam and nonspam classified emails are stored in mailserver. Then the mailserver decrypted spam and nonspam emails delivered to spam folder and inbox.

3.1 Firewall

Complex networks are protected by email firewalls. The firewall in an email spam filtering system examines the IP address, domain name and MAC address of spammed emails. Then, the authenticated spam emails are moved to encryption process. For email server traffic, the firewall administrator establishes a set of rules.

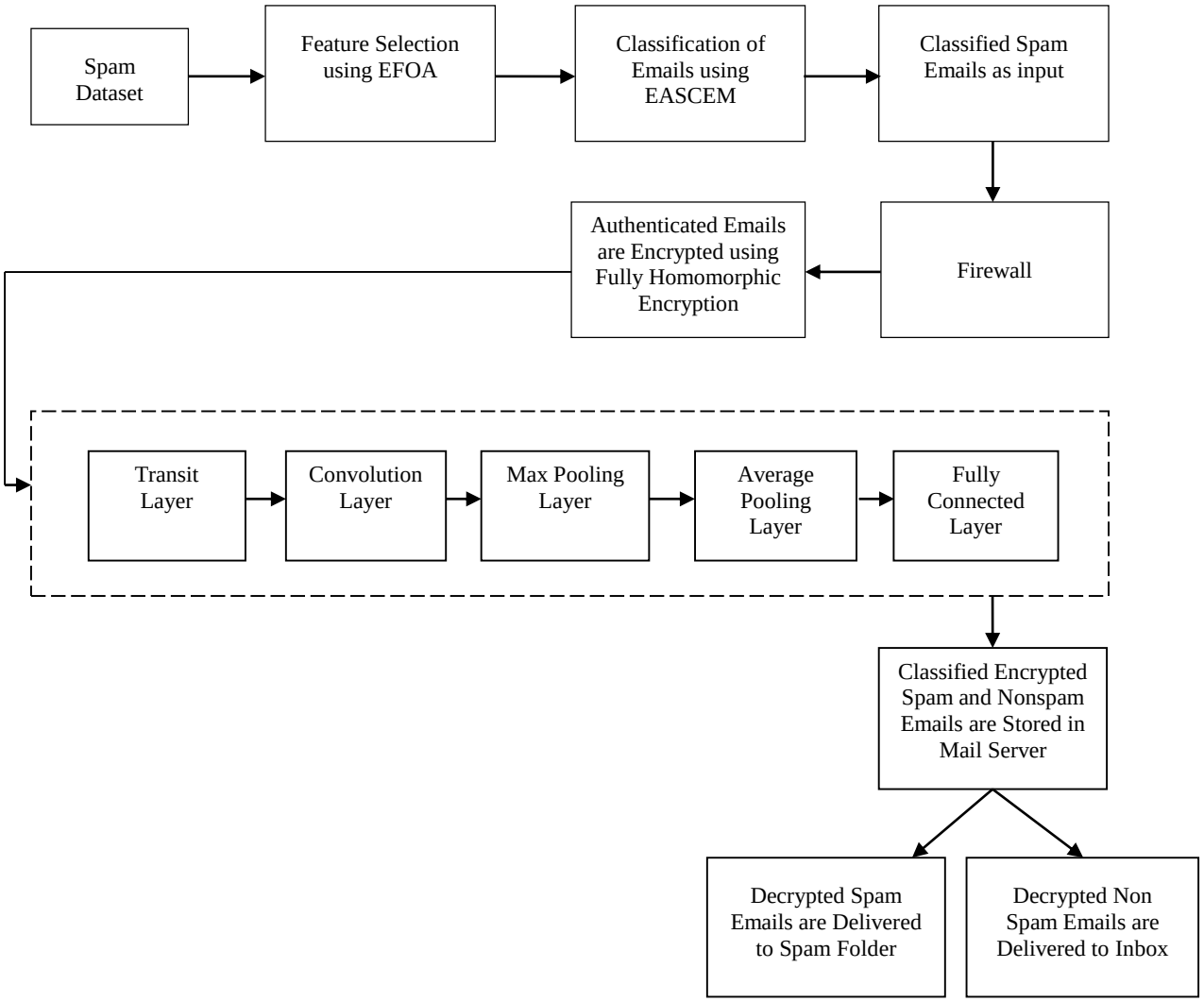
3.2 Encryption Method for Email text message

In FHEPP-DLCM, the email text messages are encrypted using homomorphic encryption based on paillier scheme.

3.2.1. Fully Homomorphic Encryption based Privacy Preserving Protocol

FHE would provide ciphertext operations that correspond to functions on the encrypted messages within. The blueprint of this construction remains the only way to design FHE schematics. FHE can be used to evaluate the set of functions known as arithmetic circuits over plaintext ring. In any case, this is often not a simple plaintext space to work with; elements in R_t are polynomials of degree up to several thousand. For prime t=1 mod 2N, $X^N+1=\prod_{t=1}^{N}(X-a_i) \bmod t$ for some $a_i \in \{1,$

….., t-1}. This means that $R_i = \frac{\prod_{t=1}^{N} z_i[x]}{t-1}(X - a_i) \cong\cong \prod_{t=1}^{N} z_t.$



DeepCNN

Figure 1: Block Diagram of FHEP-DeepCNN Method

The circuits examined using the HAdd and HMult algorithms should be leveled for efficiency. This means that the circuits gates can be grouped into layers, with inputs in the first layer and outputs in the last, and the outputs of one layer can be used as inputs to gates in the next layer. The depth of arithmetic circuits is the most significant attribute for FHE. The depth of the circuit is the greatest number of multiplication gates that can be found along any path from the input to output layers.

A levelled FHE scheme with input level L can evaluate circuits of maximum depth L, which influences the choice of the parameter q due to noise in ciphertext. The principle limiting the problem to homomorphic assessments is specifically the HMult operation on the ciphertext.

KeyGen(ʎ,L): Given security parameter and level L as inputs, choose k, q so that security Level ʎ is achieved. Choose a random element $\alpha \in R_q$, small noise $\alpha \in R_q$ and secretkey $s \in R_2$, the public key is defined to be $pk = (b = e - as, a).$ We note that for an evaluation key (evk) is also generated to aid in the control of ciphertext size following homomorphic multiplications. First, choose an integer w to control the decomposition rate and number of components l + 1 in evk, where $l = [\log_w q].$ For 0<i<1, sample $a_i \in R_q$ and $e_i \in R_q$ and compute $evk[i] = (\lfloor w^i s^2 - (a_i s + e_i) \rfloor q, a_i).$

Encrypt (pk,m): Given public key pk and message $m \in R_i$ as input, the encryption of m is defined as $c = \left(br' + e' + \left[\frac{q}{t}\right]m, ar'\right)$, for some random noise $e', r' \in R_q$.

Decrypt (sk,c): Given secret key sk and ciphertext $c = (c_0, c_1) \in R_q^2$ as inputs, the decryption of c is $m = [(\frac{t}{q})(c_0 + c_1 s \bmod q)] \bmod t$.

HAdd(c_1, c_2): Given two ciphertexts $c_1 = (c_0, 1, c_1), c_2 = (c_0, 2, c_1, 2)$ as inputs, the operation is simply component-wise addition, i.e. the output ciphertext is:

$$c' = (c_0, 1 + c_0, 2, c_1, 1 + c_1, 2) \quad (3.1)$$

HMul(c_1, c_2): Given two ciphertexts $c_1 = (c_0, 1, c_1), c_2 = (c_0, 2, c_1, 2)$ as input follows:

$$c^* = (c_0 = c_0, 1, c_1), c_1 = (c_0, 1, c_1, 2)(c_1, 1, c_0, 2), c_2 = (c_1, 1, c_1, 2) \quad (3.2)$$

3.2.2. Paillier Scheme

The Paillier encryption scheme is divided into three phases: key generation, encryption, and decryption. A ciphertext generated by the encryption process is required for decrypting a paillier scheme. For encryption, the public key is (n,g) and the private key for decryption is (λ,μ). The following are the paillier cryptosystem's homomorphic properties.

Addition of plaintexts: the result of multiplying two ciphertexts would decipher the sum of their respective plaintexts, as described in the following formula:

$$D_{priv}(E_{pub}(m1)E_{pub}(m2) \mod(n^2) = m1 + m2 \bmod(n) \quad (3.3)$$

The ciphertext that results from increasing to the plaintext would decrypted to the sum of their respective plaintexts, as described in the following formula:

$$D_{priv}(E_{pub}(m1)g^{m2} \mod(n^2) = m1 + m2 \bmod(n) \quad (3.4)$$

3.3 Homomorphic Convolutional Neural Network

An arithmetic circuit with a preset number of layers is called a neural network. The initial node is the network's input, and each layer is composed of several nodes. Layer nodes are outside of the initial node. The outputs from a subset of nodes in the preceding layer.

The functions used in the activation layers are quite varied, including sigmoid (f(z)= $\frac{1}{1+e^{-z}}$), $softplus\ (f(z) = \log(1 + e^z))$. Use the following layers to adapt NN operations over encrypted data:

Convolution (weighted-sum) layer : At each node, we take a subset of the outputs from the previous layer, also known as a filter, and do a weighted-sum to get its output.

Average-Pooling layer : At each node, we take a subset of the outputs from the previous layer and average them to get the output.

FHEPP-DLCM Algorithm

Step 1:	*Initialize Email Spam Datasets.*
Step 2:	*Email features are Selected using EFOM method.*
Step 3:	*Selected emails are classified as spam and nonspam using EASCEM method.*
Step 4:	*Declare classified spam emails.*
Step 5:	*Identify authenticate and unauthenticated emails using Firewall.*
Step 6:	*Encrypted authenticate emails using Fully Homomorphic Encryption.*
Step 7:	*Divide the dataset.*

Step 8: Add Adapted TransNet layer to increase processing speed and reducing noise.

Step 9: Get convolution layer using eq.

$$(f * g)[n] = \sum_{min}^{M} f[n-m]g[m]$$

Step 10: Get the email message feature and location information.

Step 11: Email text represented as array for 1D convolution.

Step 12: Apply a filter or kernel size.

Step 13: Get the corresponding tensor.

Step 14: Get kernel from whole sequence values of convolution in max pooling layer.

Step 15: Convolution ID, padded with average pooling.

Step 16: Sigmoid of the convolution using eq.

$$f(z)=\frac{1}{1+e^{-z}}$$

Step 17: Final email message classification as spam and nonspam.

Adapted TransNet layer: Each node is connected to a single node z node of the previous layer; its output is the square of the output of z.

Fully Connected layer: similar to the convolution layer, each node generates a weighted sum, but over the entire previous layer and not over a subset of it.

3.3.1. Adaptive TransNet

The training of the neural network through the original dataset as a function N_0 and the same training of the model through the transit layer as a function N_1. Each participant provides the server a 0/1 table at first to determine which spots in the dataset (including labels) it owns. The ID attribute is hashed using a well-known hash method. The server can determine the type of data partition and transmit a 0/1 table to each participant, instructing it on how to manage the dataset's distinct parts. The set of the labels y Ɛ G are scrambled with a common negotiated permutation S : G ! S(G).

Assume that p participants Pi (i = 1; 2;….; p) train for TransNet. Pi has partitioned dataset Xi during the training phase. Ri and Ki are secret parameters that are produced at randomly. An example z will be anticipated during the prediction phase. If the dataset is vertically or arbitrarily partitioned, Pi owns portion of z, denoted as zi. The trained neural network is represented as a function N, while the training server is represented by S.

3.3.2 Homomorphic Neurons

FHEPP-DLCM design involves several aspects of efficient implementations. Each neuron performs a weighted sum and a nonlinear activation function f(y). The multiplication procedure is slower and introduces a lot of noise in the HE scheme. When there is too much noise in a ciphertext, a bootstrapping procedure should be used. Weighted-sum calculations involve a series of additions and multiplications between ciphertexts and known constant weights. Since one of the operands is plaintext and the output ciphertext's measure is the same as the input ciphertext's, processing of y can be enhanced.

Results and Discussion

For the experimental purpose, the emails are collected from spambase in UCI repository and enron spam publicaly available dataset. The spambase dataset consists of 4,601 emails and enron spam dataset contains 30,041 emails. Here, the efficiency of SCA, ALO-Boosting and FHEPP-DLCM are tested in terms of accuracy, precision, sensitivity, f-measure and error rate. Spam filtering results of SCA, ALO-Boosting and FHEPP-DLCM are shown in the following Tables. Table 1 and Table 2 shows each column of the matrix represents the instances in a predicted class, while each row represents the instances in an actual class.

Table 1 Confusion Matrix for Spambase Dataset using FHEPP-DLCM

Actual Class / Predicted Class	**Non Spam**	**Spam**

Non Spam	2770	18
Spam	22	1791

Table 2 Confusion Matrix for Enron Spam Dataset using FHEPP-DLCM

Actual Class / Predicted Class	**Non Spam**	**Spam**
Non Spam	16284	261
Spam	312	13184

4.1 Accuracy

Accuracy is computed as the percentage of the dataset correctly caregorized by the algorithm. The percentage of total number of properly recognized e-mails defined by the following formula:

$$Accuracy = \frac{No\ of\ correctly\ classified\ non\ spam\ emails + No\ of\ correctly\ classified\ spam\ emails}{Total\ No\ of\ spam\ emais + Total\ No\ non\ spam\ emails} \quad (4.1)$$

Table 3 shows the accuracy of SCA, ALO-Boosting and FHEPP-DLCM for filtering spam email messages on spam dataset and enron spam dataset.

Table 3 Evaluation of Accuracy for Spam and Enron Spam Dataset

Methods	**Spam Dataset(%)**	**Enron Spam Dataset(%)**
SCA	97.92	92.39
ALO-Boosting	97.95	93.22
FHEPP-DLCM	99.13	98.09

The email spam accuracy of FHEPP-DLCM based email spam filtering method is greater than ALO-Boosting and SCA based email spam filtering method on spam dataset and enron spam dataset. From this analysis, it is proved that proposed FHEPP-DLCM method has high accuracy than ALO-Boosting method on spam dataset and enron spam dataset for email spam filtering.

4.2 Precision

Precision indicates the number of jurisdictions which are positively ranked and relevant. High precision demonstrates high pertinence for positive detection.

$$Precision = \frac{Correctly\ classified\ non\ spam\ emails}{Correctly\ classified\ non\ spam\ emails + Falsely\ classified\ non\ spam\ emails\ as\ spam} \quad (4.2)$$

Table 4 shows the precision of SCA, ALO-Boosting and FHEPP-DLCM for filtering spam and non-spam email messages on spam dataset and enron spam dataset.

Table 4 Evaluation of Precision

Methods	**Spam Dataset**	**Enron Spam Dataset**
SCA	98.00	92.47
ALO-Boosting	98.04	98.11
FHEPP-DLCM	99.21	98.96

The precision of FHEPP-DLCM based email spam filtering method has 98.00%, 98.04% and 99.21% greater than ALO-Boosting and SCA based email spam filtering method on spam dataset. Similarly, FHEPP-DLCM method has 92.47%,

98.11% and 98.96% greater than ALO-Boosting and SCA method on enron spam dataset. From this analysis, it is proved that proposed FHEPP-DLCM method has high precision than ALO-Boosting method on spam dataset and enron spam dataset for email spam filtering.

4.3 Sensitivity

Sensitivity is defined as the probability of correctly classifying spam e-mails as spam, and the legitimate sensitivity is defined as the probability of properly classifying correctly legitimate e-mails. The sensitivity formulas are listed below:

$$Sensitivity = \frac{Correctly\ classified\ non\ spam\ emails}{Correctly\ classified\ non\ spam\ emails + Falsely\ classified\ spam\ emails\ as\ non\ spam} \quad (4.3)$$

Table 5 shows the sensitivity of SCA, ALO-Boosting and FHEPP-DLCM for filtering spam and non-spam email messages on spam dataset and enron spam dataset.

Table 5 Evaluation of Sensitivity

Methods	Spam Dataset	Enron Spam Dataset
SCA	98.47	92.94
ALO-Boosting	98.53	93.89
FHEPP-DLCM	99.35	98.42

The sensitivity of FHEPP-DLCM based email spam filtering method has 98.47%, 98.53% and 99.35% greater than ALO-Boosting and SCA based email spam filtering method on spam dataset. Similarly, FHEPP-DLCM method has 92.94%, 93.89% and 97.81% greater than ALO-Boosting and SCA method on enron spam dataset. From this analysis, it is proved that proposed FHEPP-DLCM method has high precision than ALO-Boosting method on spam dataset and enron spam dataset for email spam filtering.

4.4 F-Measure

The f-measure defines harmonic mean of precision and recall. The f-measure formulas are listed below:

$$F - Measure = \frac{(2 * Sensitivity * Precision)}{(Sensitivity + Precision)} \quad (4.4)$$

Table 6 shows the f-measure of SCA, ALO-Boosting and FHEPP-DLCM for filtering spam and non-spam email messages on spam dataset and enron spam dataset.

Table 6 Evaluation of F-Measure

Methods	Spam Dataset	Enron Spam Dataset
SCA	98.23	92.70
ALO-Boosting	98.28	93.61
FHEPP-DLCM	99.27	98.26

The f-measure of FHEPP-DLCM based email spam filtering method has 98.23, 98.28 and 99.27 greater than ALO-Boosting and SCA based email spam filtering method on spam dataset. Similarly, FHEPP-DLCM method has 92.70, 93.61 and 98.26 greater than ALO-Boosting and SCA method on enron spam dataset. From this analysis, it is proved that proposed FHEPP-DLCM method has high precision than ALO-Boosting method on spam dataset and enron spam dataset for email spam filtering.

4.5 Error Rate

The error rate defined as the percentage of the dataset incorrectly classified by the method. It is the probability of misclassification of a classifier. The error rate formulas are listed below:

$$Error\ Rate = 1 - Accuracy \quad (4.5)$$

Table 7 shows the error rate of SCA, ALO-Boosting and FHEPP-DLCM for filtering spam and non-spam email messages on spam dataset and enron spam dataset.

Table 7 Evaluation of Error Rate

Methods	**Spam Dataset**	**Enron Spam Dataset**
SCA	2.08	7.61
ALO-Boosting	2.05	6.78
FHEPP-DLCM	0.87	1.91

The error rate of FHEPP-DLCM based email spam filtering method has 2.08, 2.05 and 0.87 better than ALO-Boosting and SCA based email spam filtering method on spam dataset. Similarly, FHEPP-DLCM method has 7.61, 6.78 and 1.91 better than ALO-Boosting and SCA method on enron spam dataset. From this analysis, it is proved that proposed FHEPP-DLCM method low error rate than ALO-Boosting method on spam dataset and enron spam dataset for email spam filtering.

4. CONCLUSION

This paper proposed an Adapted TransNet to increase the email spam classification accuracy and reduce the communication complexities. In FHEPP-DLCM method, the homomorphic encryption scheme enables both the security of emails and good classification accuracy. The performance has been evaluated using metrics such as false positive rate, false negative rate, accuracy, precision and recall. The results show a high level of efficiency for encrypted emails. The experimental results prove that the proposed FHEPP-DLCM has better accuracy rate of spam and non spam, precision and recall than the existing spam classification method.

REFERENCES

[1] Vijayasekaran, G., & Rosi, S. (2018), "Spam and Email Detection in Big Data Platform using Navies Bayesian Classifier", International Journal of Computer Sci. and Mobile Computing, Vol. 7, No. 4, pp. 53-58, ISSN: 2320-088X.

[2] Gauri Jain., Manisha., & Basant Agarwal, (2016), "An Overview of RNN and CNN Techniques for Spam Detection in Social Media", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No.10, pp.126-138, ISSN: 2277 128X.

[3] Ajay Shrestha., & Ausif Mahmood, (2019), "Review of Deep Learning Algorithms and Architectures", IEEE Access, Vol. 7, pp. 53040-53065, ISSN: 2169-3536.

[4] Muhammd Imran Tariq., Nisar Ahmed Memon., & Muhammad Imran, (2020), "A Review of DeepLearning Security and Privacy Defensive System", Mobile Information System, PP 1-18 ISSN: 1574-017X.

[5] Zvika Brakerski., Craig Gentry., & Vinod Vaikuntanathan, (2014), "Fully Homomorphic Encryption without Bootstrapping", ACM Transactions on Computation Theory, Vol. 6, No.3, pp. 1-36.

[6] Benavides E., Sanchez S., & Fuertes, W. (2020), "Classification of Phishing Attack Solutions by employing DeepLearning techniques : A Systematic literature Review", Springer, pp. 51-64.

[7] Ajinkya Gulunjkar., & Rakesh Rathi (2020), "A Machine Learning Approach Based Spam Filtering With the Use of Neural Network", ITEE Journal, Vol.9, No.4, ISSN: 2306-708X.

[8] Carlos Laorden., Xabier Ugarte Pedrero., & Igor Santos, (2014), "Study on the Effectiveness of anomaly detection for spam filtering", Information Sciences, Elsevier, Vol.277, pp. 421-444, ISSN: 0020-0255.

[9] Khedr, A., Gulak, G., & Vaikuntanathan, V. (2014), "SHIELD: Scalable Homomorphic Implementations of Encrypted Data Classifiers", IEEE Transactions on Computers, Vol.65, No.9, ISSN: 2848-2858.

[10] Ahmad Al Badawi., Louie Hoang., & Chan Fook Mun (2020), "PrivFT: Private and Fast Text Classification with Homomorphic Encryption", IEEE Access, Vol.8, pp. 22654-22656.

[11] Renukadevi, R. et al. "An Improved Collaborative User Product Recommendation System Using Computational Intelligence with Association Rules." Communications on Applied Nonlinear Analysis (2024): n. pag. https://doi.org/10.52783/cana.v31.1243

[12] "TransNet: Minimally Supervised Deep Transfer Learning for Dynamic Adaptation of Wearable Systems", ACM Transactions on Design Automation, Vol.26, No.1, pp 1-31, ISSN: 1084-4309.

[13] Ammara Zamir, Hikmat Ullah Khan & Waqar Mehmood, "A feature-centric spam email detection model using diverse supervised machine learning algorithms",pp 633-657,

[14] Erkin, Z., Veugen, T., & Toft, (2012), "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, pp. 1053–1066.

[15] Badsha, S., X. Yi., & Khalil, I. (2016) , "A practical privacy-preserving recommender system," Data Science and Engineering, vol. 1, no. 3, pp.161–177.

[16] Aono, Y., Hayashi, T., & Wang, L. (2017), "Privacy-preserving deep learning via additively homomorphic encryption", IEEE Trans. Inf. Forensics Secur., Vol. 13, 1333-1345.

[17] Al-Rubaie, M., Chang. J.M. (2019), "Privacy-preserving machine learning: Threats and solutions", IEEE Secur. Priv., Vol. 17, 49-58.

[18] Mohamad .M & Selamat .A, "An evaluation on the efficiency of hybrid feature selection in spam email classification", IEEE Communications and Control Technology (I4CT), pp. 227-231, 2015.

[19] Karthika Renuka .D, Visalakshiand .P, Rajamohana .SP, "An Ensembled Classifier for Email Spam Classification in Hadoop Environment", Appl. Math. Inf. Sci., Vol. 4, No. 11, pp. 1123-1128, 2017.

[20] Izzat Alsmadi & Ikdam Alhami, "Clustering and Classification of email contents", Journal of King Saud and Information Sciences, pp. 46-57, 2015.