Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.022720
Article

Tech Science Press

Social Networks Fake Account and Fake News Identification with Reliable Deep Learning

N. Kanagavalli[1,*] and S. Baghavathi Priya[2]

[1]Department of CSE, Rajalakshmi Institute of Technology, Chennai, 600124, Tamil Nadu, India
[2]Department of CSE, Rajalakshmi Engineering College, Chennai, 602105, Tamil Nadu, India
*Corresponding Author: N. Kanagavalli. Email: kanagavallirec@gmail.com
Received: 17 August 2021; Accepted: 20 October 2021

Abstract: Recent developments of the World Wide Web (WWW) and social networking (Twitter, Instagram, etc.) paves way for data sharing which has never been observed in the human history before. A major security issue in this network is the creation of fake accounts. In addition, the automatic classification of the text article as true or fake is also a crucial process. The ineffectiveness of humans in distinguishing the true and false information exposes the fake news as a risk to credibility, democracy, logical truth, and journalism in government sectors. Besides, the automatic fake news or rumors from the social networking sites is a major research area in the field of social media analytics. With this motivation, this paper develops a new reliable deep learning (DL) based fake account and fake news detection (RDL-FAFND) model for the social networking sites. The goal of the RDL-FAFND model is to resolve the major problems involved in the social media platforms namely fake accounts, fake news/rumor identification. The presented RDL-FAFND model detects the fake account by the use of a parameter tuned deep stacked Auto encoder (DSAE) using the krill herd (KH) optimization algorithm for detecting the fake social networking accounts. Besides, the presented RDL-FAFND model involves an ensemble of the machine learning (ML) models with different linguistic features (EML-LF) for categorizing the text as true or fake. An extensive set of experiments have been carried out for highlighting the superior performance of the RDL-FAFND model. A detailed comparative results analysis has stated that the presented RDL-FAFND model is considerably better than the existing methods.

Keywords: Social networking; fake account; fake news; rumor detection; deep learning; linguistic features

1 Introduction

The advancement of the World Wide Web (WWW) and quick adoption of the social networks like Twitter and Instagram has established the basis for data distribution which has never been witnessed before in the human history [1]. Moreover, news channels have gained benefits from the extensive utilization of the social networks by offering upgraded news to their real time users. The news media has

been developed from the tabloids, magazines, and newspapers in digital forms like social media feeds, blogs, online news platforms, and different digital media formats [2]. It would be simple for the users to obtain the updated news in their hands. Facebook referral accounts have been found to utilize 70% of the traffic for their news websites. These social networks in the present condition are highly effective and beneficial for the clients for deliberating and sharing their ideas and for discussing the problems related to education, health, and democracy. But, this network is also being utilized by negative viewpoints with specific entities generally for financial benefits, and otherwise, it is utilized for making manipulating mindsets, absurdity/spreading satire, and biased opinions. The occurrence is generally called as the fake news.

The fake news initially denotes false and frequently sensational data dispersed in the appearance of the related news. The fake news is determined as the news, that is demonstrably and intentionally false, or some data existing as news which is accurately incorrect and implemented to deceive the news user for considering it to be true [3]. The news content could be entirely fake, made for deceiving the user, or it is a complicated content that utilizes the mislead data for addressing a specific topic. It is possible for distinguishing the contents that simulates the open source however, the sources are not true. The spread patterns of the fake news on the social television are frequently investigated for identifying the features of the fake news that supports the discrimination among the legitimate and the fake news respectively [4]. The challenge in the detection of the fake news has been determined in various forms. The classification has been considered as the act of binary classification among true/false, rumour/not, hoax/not. The alternative method for defining the challenge is to execute a classification model for various classes like, true, nearly true, partly true, frequently false/false, or unproven rumour, true rumour, and false rumour/not. The major variance among the determination of the classification challenges is because of their distinct annotation systems/ application contexts in distinct datasets.

On the other hand, by extending the utilization of the social media, adversaries search for violating the secrecy of the other clients and misuse its names and credentials by the creation of fake accounts [5,6]. Henceforth, the social media providers involve in the task of detecting the adversaries and fake accounts for removing them from the social media platforms. The use of fake accounts in social media can cause more harm compared to the other cybercrimes. Eliminating the fake accounts has gained more interest among the scientists; therefore, wide-ranging studies have been performed on the detection of fake accounts in social media [7]. Distinct methods have been used for finding the fake accounts based on their feature similarities, comparability of friend networks, profile analyses for a time interval along with their IP address. [8] Provides an unsupervised 2-layer Meta classification technique that could identify the uncontrollable nodes in a difficult network by utilizing the extraction features of the graph topology. It is also verified that the presented technique is utilized for detecting both the fake and real clients in the network. [9] Offered a powerful and scalable defense system named "´Integro" that places the fake accounts with lower ranks at the utilization of the client rankings. [10] Presented a forward message tree with 6 efficient features for investigating the connections among the accounts and for identifying the suspected accounts.

This paper proposes a reliable deep learning (DL) based fake account and fake news detection (RDL-FAFND) model for the social networking sites. The presented RDL-FAFND model detects the fake account using the krill herd (KH) optimization based deep stacked Auto encoder (DSAE). The exploitation of the herding behavior of the krill's helps to properly adjust the hyper parameters of the DSAE model. In addition, the presented RDL-FAFND model involves an ensemble of the machine learning (ML) models with dissimilar linguistic features (EML-LF) for identifying the text as true or fake. A series of experimentations have been performed for guaranteeing the improved fake account and fake news detection performance of the RDL-FAFND model.

2 Related Works

The spreading of fake news has resulted in serious problems, containing the significant effects on the social activities. Therefore, the current research about fake news identification from social media has become a hot research topic and various investigations have tried to develop fake news classification methods using ML. Han et al. [11] developed a method for detecting the various fake news categories and linguistic features. They have calculated the efficiency of the baseline classification and the DL methods concerning the fake news recognition and related them for balancing the accuracy and light weights. Agarwal et al. [12] utilized the LIAR dataset from Kaggle for fake news classification, containing 20,801 news records from the USA. They extracted the reliability scores and another linguistic feature in the text, and both these datasets have been tokenized and normalized.

Wang et al. [13] established the WeFEND architecture for the automated annotation of the news articles that utilized the client information in WeChat as a kind of weaker supervision in the fake news identification. Various methods examine the importance of the textual and the linguistic features for fake news identification. Nikiforos et al. [14] established a new dataset, comprising of 2366 tweets in English, with respect to the Hong Kong protests. Both the linguistic features and the network accounts have been extracted from the tweets when various features have been recognized as a determining factor for the fake news recognition. This method has considered the SMOTE oversampling, and the binary classification for addressing the class imbalance. The SMOTE over-sampling and the feature extraction have been performed in the Rapid Miner Studio.

Jeronimo et al. [15] exploited a dataset comprising of 207,914 news articles of the two main conventional architectures in Brazil, gathered from 2014 to 2017, and 95 news of the two facts checking facilities in Brazil (fake news class). It is an accompanied classification with XGBoost, RF (by TF-IDF and Bag of Words demonstrating), attains high efficiency in the inter-field conditions. Mahyoob et al. [16] utilized twenty posts from PolitiFact as the actual news and twenty posts in Facebook as the fake news, totally acquiring 3 classes. It is an executed qualitative and quantitative data analyses with the QDA method, relating the posts based on its linguistic features. Shu et al. [17] proposed a new fake news data repository and a FakeNewsNet. It comprises of 2 datasets with several features, involving the spatiotemporal data, the social, and the news contents.

Kumar et al. [18] related the distinct ensembles for accomplishing the binary classification on 1356 news from Twitter and 1056 actual and fake news from PolitiFact. It can generate the dataset for every topic, and later it can be encoded and tokenized by themselves. Alves et al. [19] produced a new binary class datasets, comprising of 2996 articles expressed by the Brazilian Portuguese. The investigation has been carried out with the bi-directional and standard LSTM and the dense layers. Victor [20] utilized the LIAR and PHEME datasets, and carried out the research with deep 2 path CNN and bidirectional RNN for the unsupervised and the supervised learning. Miao et al. [21] developed a novel dataset of 4072 news articles from the Webhose. That is about the fake news regarding COVID-19. It utilized the linguistic features and performed the investigations with the baseline classifications like the dense layer and the LSTM.

3 The Proposed RDL-FAFND Model

The overall system architecture of the presented model involves two major operations namely the KH-DSAE based fake account detection model and the EML-LF based fake news detection model, as shown in Fig. 1. The detailed working of these two modules has been discussed in the subsequent sections.

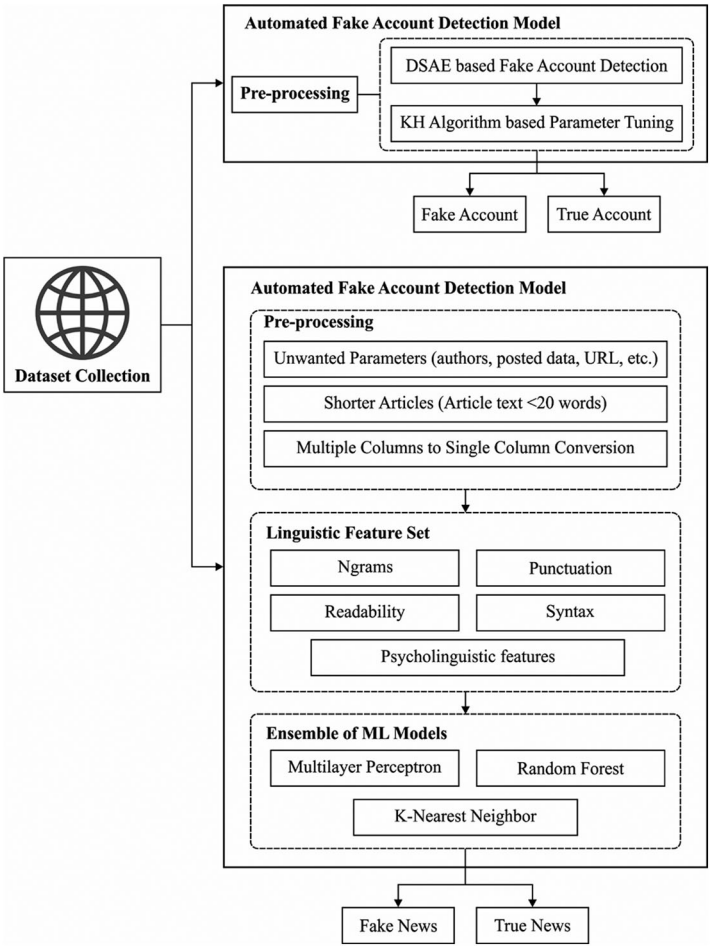

Figure 1: The Overall architecture of the proposed model

3.1 Automated Fake Account Detection Model

Primarily, the fake accounts in the social networking sites are detected using the KH-DSAE model. The KH-DSAE model initially receives the social networking data as the input and performs the DSAE based detection process. For increasing the detection efficiency of the DSAE model, the KH algorithm has been applied to it.

3.1.1 Architecture of DSAE for Fake Account Detection

The ANN model consists of 1 input layer, several hidden layers, and an output layer. Commonly, the amount of layers and the neurons would not be set at the beginning; rather, it is would be defined by the empirical techniques based on the difficulty of the problems. If there are excessive layers and neurons, it would consume excessive time durations for learning the instances; unlike, if there are excessive layers, the fault tolerance and the instance recognition efficiency would fall to a lower level. Fig. 2 shows the structure of the DSAE model.

The number of neurons in every hidden layer is normally fixed to (2, 4, 2) in the case of 3 hidden layers with the input neurons (containing 2 parameters). In the forward propagation, some weighted input z_j^l of the neurons, j in the layer l is calculated by the activation of the upper layer $a_j^{(l-1)}$ with weight W_{jk}^l among the nearby layers and the bias b_j^l represents the present layer [22]. Later, a sigmoid activation function $f(z)$ is

utilized for computing the activation of the present layer a_j^l:

$$z_j^l = \sum_k W_{jk}^l a_k^{(l-1)} b_j^l \tag{1}$$

$$a_j^l = f\left(z_j^l\right) \tag{2}$$

$$f(z) = \frac{1}{1+e^{-z}} \tag{3}$$

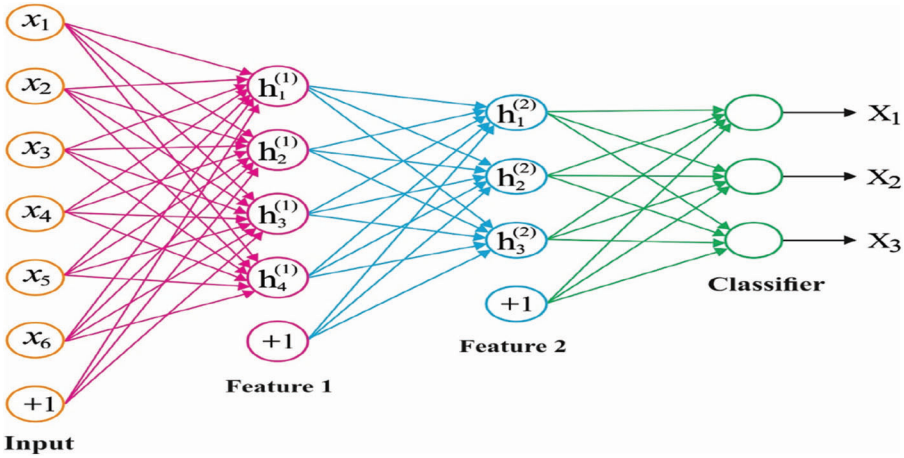

Figure 2: Network structure of DSAE model

where l represents the hidden layer count ($l \in [1,3]$), j denotes the neuron count in the present layer, and k indicates the quantity of the neurons in the upper layer. If l is equivalent to zero, the input layer and the values of a_j^0 are quantified by the user. The activation of the output layer d^L represents the output neuron value. When L is equivalent to four the hidden layer count becomes 3, as given in Eqs. (1)–(3).

The primary objective of the BP in the NN is to attain the expression for the partial derivatives $\partial C/\partial W$ and $\partial C/\partial b$ of the cost function C regarding the bias (b) and the weight (W). In this procedure, the NN adapts the bias and the weight values based on the errors among the desired and the modelled output till the error falls under a fixed threshold. The quadratic cost function is given by:

$$C = \frac{1}{2N}\sum_i (\hat{y}_i - y_i)^2, \tag{4}$$

where N represents the overall amount of the trained samples, $\hat{y}$ indicates the desirable output, and y denotes the model output from the NN. In the output layer, the error elements δ^L is represented as

$$\delta_j^L = \frac{\partial C}{\partial a_j^L} f'\left(z_j^{\mathrm{L}}\right) \tag{5}$$

The initial term on the right, $\partial C = \partial a_j^{\mathrm{L}} L$, measures the rapidness of the cost function that is altering at a_j^L, when the second term on the right, $f'\left(z_j^{\mathrm{L}}\right)$, measure the rapidness of the activation function that is altering at z_j^L. In several hidden layers, the error δ^l should be calculated from the succeeding layer δ^{l+1} is given by:

$$\delta_j^l = \left(\left(W_j^{l+1}\right)^T \delta_j^{l+1}\right) * f'\left(z_j^{\mathrm{L}}\right) \tag{6}$$

where $*$ denotes the Hadamard product that is the component wise product of the 2 vectors, and $\left(W_j^{l+1}\right)^T$ denotes the transposition of the weight matrix W_j^{l+1}. Afterward, it could attain the partial derivative of the cost function C regarding the weight and the bias as given by:

$$\frac{\partial W_{jk}^l}{\partial C} = a_k^{l-1}\delta_j^l \tag{7}$$

$$\frac{\partial b_j^l}{\partial C} = \delta_j^l \tag{8}$$

When several back and forward propagations exist, the error among the desirable output and the modelled output would be lesser compared to that of the fixed threshold. Also, the output layer neuron can attain saturation, the bias and the weight learning's would stop, and the bias b and the weights W of this method would be established.

3.1.2 Parameter Optimization Using KH Algorithm

For tuning the weight and the bias values of the DSAE model, the KH algorithm has been employed. The DSAE model undergoes training with the weight and the bias parameters. In addition, 10 fold cross-validation (CV) process has been employed for the evaluation of the fitness function. The FF can be determined as the 1-$CA_{validation}$ of the 10-fold CV technique on the training set, as given in Eqs. (9) and (10). In addition, the solution with maximum $CA_{validation}$ holds the smallest fitness value.

$$Fitness = 1 - CA_{validation} \tag{9}$$

$$CA_{validation} = 1 - \frac{1}{10}\sum_{i=1}^{10}\left|\frac{y_c}{y_c + y_f}\right| \times 100 \tag{10}$$

where y_c and y_f refers to the count of the true and false classifications correspondingly. KH [23] is a novel metaheuristic optimization approach commonly used for resolving the optimization processes. It is inspired from the herding of the krill swarm with some biological and environmental procedures. The time based location of a separate krill in a two-dimensional space has been determined using the following 3 key measures.

(i) Motion is influenced by another krill individual,

(ii) Foraging action,

(iii) Arbitrary diffusion.

The KH technique utilized the Lagrangian method in a d dimension decision space using Eq. (11):

$$\frac{dX_i}{d\mathrm{t}} = N_i + F_i + D_i, \tag{11}$$

where $N_\mathrm{i}, F_\mathrm{i}$, and D_i represent the movements directed by another krill individual, foraging movement, and physical diffusion of the ith krill individual, correspondingly. In the motion influenced by another krill individual, the movement direction, α_i, is nearly calculated by the repulsive (i.e., repulsive swarm density), target (i.e., target swarm density), and the local effects (i.e., local swarm density). For a krill individual, this motion can be determined by the following equation.

$$N_i^{\text{new}} = N^{\max}\alpha_{\text{i}} + \omega_n N_i^{\text{old}}, \tag{12}$$

and $N^{\max}$ represents the maximum induced speed, ω_n denotes the inertia weight of the movement induced in [0, 1], and $N_{\text{i}}^{\text{old}}$ indicates the latter movement induced.

The foraging movement is calculated by 2 major elements namely the food position and the previous knowledge on the food position. For the ith krill individual, this movement can be equated by:

$$F_? = V_f\beta_{\text{i}} + \omega_f F_{\text{i}}^{\text{old}}, \tag{13}$$

where

$$\beta_i = \beta_i^{\text{food}} + \beta_i^{\text{best}}, \tag{14}$$

and V_f represents the foraging speed, ω_f denotes the inertia weight of the foraging movement among 0 to 1, $F_{\text{i}}^{\text{old}}$ indicates the latter foraging movement. The arbitrary diffusion of the krill individual is assumed as an arbitrary procedure in the core. This movement is based on the maximum diffusion speed and an arbitrary vector direction. It is denoted by:

$$D_{\text{i}} = D^{\max}\delta, \tag{15}$$

where $D^{\max}$ represents the maximum diffusion speed, δ indicates the arbitrary vector direction and its array denotes the arbitrary values in $[-1,\ 1]$. According to the 3 aforementioned motions, by distinct variables of the movements in the time, the location vector of the krill individual's at the interval t to $t + \Delta t$ can be stated as follows:

$$X_i(\text{t} + \Delta\text{t}) = X_i(\text{t}) + \Delta t\frac{dX_i}{d\text{t}}. \tag{16}$$

It must be distinguished that Δt is an essential variable and it is fine-tuned based on the real time optimization problems. Fig. 3 illustrates the flowchart of the KH technique.

3.2 Automated Fake News Detection Model

At this stage, the automated fake news detection model can be designed by using the EML-LF model. The EML-LF model incorporates three major sub processes namely the pre-processing, the linguistic feature set, and the EML based classification.

3.2.1 Preprocessing

The data gathered from the social media would undergo the pre-processing procedure prior to its use as the input to the EML-LF model. The undesirable variables in the article like the author names, the published data, the URL, and the category would be discarded. The articles with no body text or with <20 words in the article body would be deleted. Then, the article in multiple columns would be converted into one column to maintain the consistency in its format and structure. These processes are thus carried out on the dataset to attain uniformity.

3.2.2 Linguistic Feature Set

When the data pre-processing is done, the subsequent stage is the process of extracting the linguistic features [24].

Ngrams: The unigrams and the bigrams are extracted from the bag of words representation of all the news articles. In case of infrequent variations in the content length, the features would be encoded as the tf-idf values.

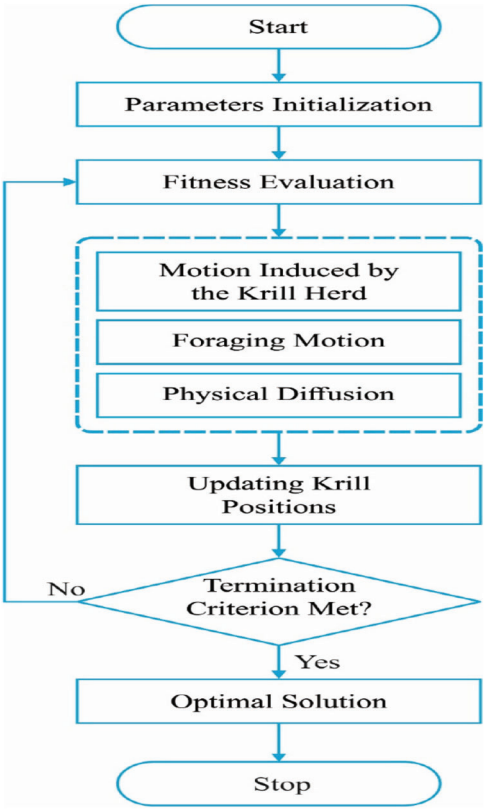

Figure 3: Flowchart of KH algorithm

Punctuation: A punctuation feature set comprising of 11 kinds of punctuations is generated from the Linguistic Inquiry and the Word Count software (LIWC, Version 1.3.1 2015). It includes the punctuation marks like comma, dash, question mark, exclamation mark, period, etc.

Psycholinguistic features. The LIWC lexicon is used for extracting the proportion of words which falls to the psycholinguistic classes. The LIWC depends upon the large lexicons of the word classes representing the psycholinguistic processes (for instances, positive emotions and perceptual processes), summary classes, and parts of the speech classes (article, verb). The individual LIWC classes are clustered into the feature sets as given here: summary categories (analytical thinking, emotional tones), linguistic process (function word, pronoun), and psychological process (*e.g.*, affective process, social process).

Readability. The features denoting the text understandability are also extracted. It comprises of the content features like character count, complex word, long word, syllable count, word type, and paragraph count, among the other content features. Some readability measures like Flesch-Kincaid, Flesch Reading Ease, Gunning Fog, and the Automatic Readability Index (ARI) are used.

Syntax. At last, a collection of features generated from the production rules depending upon the context free grammar (CFG) trees utilizing the Stanford Parser are extracted. The CFG comprises of the lexicalized production rules integrated into the parent and the grandparent nodes. They are found to be helpful for the linguistic deception detection.

3.2.3 Ensemble of ML Models for Fake News Detection

At this stage, the EML model is applied to categorize the news into true or fake news. The ensemble learning helps in improving the outcome of the ML by combining several techniques. These techniques

permit the generation of an enhanced predictive method over an individual method. Here, a Simple Majority Voting Ensemble or Voting Classifier is utilized for combining the predictive results from multiple ML techniques (MLP, RF, and KNN) for getting an enhanced integrated outcome. When the Voting Classifier is trained, it can be utilized for predicting the label of the novel samples depending upon the votes of the contributing models. For evaluating the efficiency of the individual and the ensemble methods, initially, it is trained and tested on the individual methods on the fake news datasets utilizing the10-fold CV. Afterwards, it is trained for the presented ensemble classifier on a similar analysis dataset utilizing the 10-fold CV.

The MLP, RF, and KNN are the familiar techniques which are extremely efficient for resolving the classification problems. The RF is commonly utilized as a baseline from the text classification problem by the researchers. It can be an ensemble learning technique to the classification task and functions by generating several DTs at the time of training and classifies the classes as decided by the contributing DTs [25]. The KNN technique operates by computing the distance (provided in Eqs. (17)–(19)) among the query and every instance from the data and by selecting the particular count of instances (K) that are closer to the query. The KNN distance can be written as:

$$Euclidean = \sqrt{\sum_{i=1}^{k} (xi - yi)^2}, \tag{17}$$

$$Manhattan = \sum_{i=1}^{k} |Xi - Yi|, \tag{18}$$

$$Minkowski = \sum_{i=1}^{k} (|xi - yi|^q)^{1.q}. \tag{19}$$

In the classification problem, the distinct K values in the KNN technique results in various classification outcomes; but, the optimal value of K is defined by performing experiments for several rounds with distinct values of K and by selecting the one that provides the optimal classification outcomes. The RF model is defined by establishing a number of DTs at the training time and predicts more classes as decided by the contributing DTs. The RF uses the Gini Index and the Entropy for the classification function as provided in the 2 subsequent formulas:

$$Gini\ Impurity = \sum_{i=1}^{c} fi(1 - fi), \tag{20}$$

$$Entropy = \sum_{i=1}^{c} -f \log(\mathrm{fi}). \tag{21}$$

The MLP, colloquially, that is frequently demonstrated to as the NNs is called as “vanilla,” specifically in the case of having one hidden layer. As mentioned above, this research has presented an ensemble learning method that combines the efficient ML techniques such as the RF, the KNN, and the MLP, and employs the linguistic feature sets for the fake news detection.

4 Performance Validation

This section validates the performance of the proposed model on fake account and fake news detection dataset. A detailed set of experimentations have been performed and the results have been compared with the

existing methods. Initially, the fake account detection performance can be validated using a fake account dataset from the Kaggle repository [26,27]. From the Fig. 4 and Tab. 1 showcases the fake account detection performance of the proposed KH-DSAE model with the other methods in terms of the area under curve (AUC), accuracy, false positive rate (FPR), and true positive rate (TPR) [28]. The experimental outcomes have stated that the Linear SVM model has obtained ineffective outcome with the AUC of 0.98, accuracy of 0.98, FPR of 0.4, and TPR of 0.96. At the same time, the Logistic Regression (LR) model has achieved a slightly increased outcome with the AUC of 0.96, accuracy of 0.970, FPR of 0.3, and TPR of 0.94. Followed by, the Medium Gaussian SVM model that has accomplished a moderate outcome with the AUC of 1, accuracy of 0.98, FPR of 0.2, and TPR of 0.97. Though the DSAE model has showcased near optimal results with the AUC of 1, accuracy of 0.985, FPR of 0.2, and TPR of 0.97, the presented KH-DSAE model has outperformed the DSAE model with the AUC of 1, accuracy of 0.991, FPR of 0.1, and TPR of 0.98.

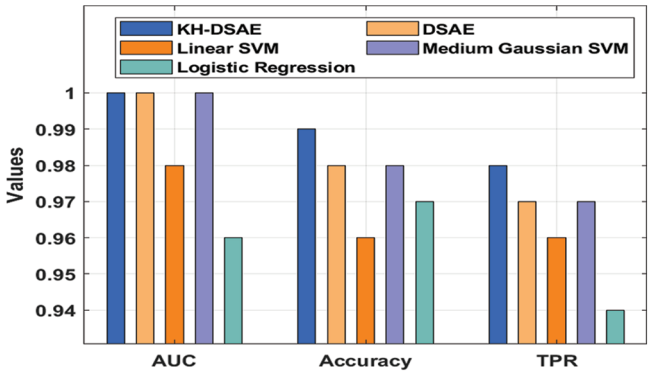

Figure 4: Result analysis of KH-DSAE model

Table 1: Result analysis of the existing method with the proposed DSAE method on fake account detection

Methods	AUC	Accuracy	FPR	TPR
KH-DSAE	1.00	0.991	0.1	0.98
DSAE	1.00	0.985	0.2	0.97
Linear SVM	**0.98**	**0.960**	**0.4**	**0.96**
Medium gaussian SVM	1.00	0.980	0.2	0.97
Logistic regression	**0.96**	**0.970**	**0.3**	**0.94**

Fig. 5 shows the ROC analysis of the proposed KH-DSAE model with the existing methods on the applied dataset. It is apparently visible that the KH-DSAE model outperforms the other methods by attaining a maximum ROC of 99.9955 whereas the DSAE, linear SVM, Medium Gaussian SVM, and LR models have showcased a slightly reduced ROC of 99.5252, 99.3455, 99.6210, and 99.2952 respectively.

A detailed results analysis of the EML-LF model on fake news detection dataset has been illustrated in Tab. 2 and Fig. 6. From the obtained results, it is evident that the SVM model has accomplished insignificant outcomes with the minimal average precision of 0.93, recall of 0.91, and F1score of 0.91. At the same time, the RF 1 model has obtained a slightly increased outcome over the SVM with the average precision of 0.94,

recall of 0.91, and F1score of 0.92. Meanwhile, the RF 2 model has depicted even better outcomes with the average precision of 1 and recall of 0.97. Concurrently, the DL-SMOTE technique has exhibited competitive outcomes with the average precision of 13, recall of 0.98, and F1score of 0.99. However, the EML-LF model has demonstrated superior results with the average precision of 1, recall of 0.99, and F1score of 0.99.

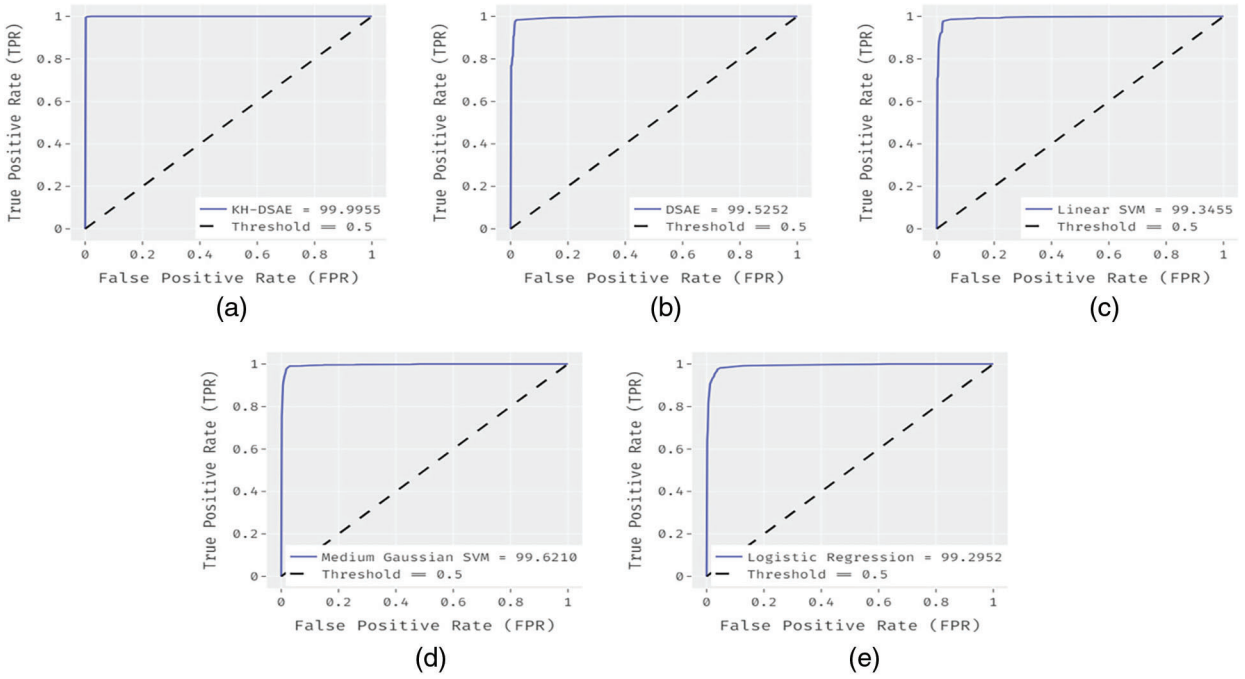

Figure 5: ROC analysis (a) False Positive Rate of KH-DASE (b) False Positive Rate of DSAE (c) False Positive Rate of Linear SVM (d) False Positive Rate of Medium Gaussian SVM (e) False Positive Rate of Logistic Regression

Table 2: Result analysis of the existing method with the proposed EML-LF method on fake news detection dataset

Methods	Tweet	Precision	Recall	F1 score
EML-LF	Fake	1.00	0.99	0.99
	Real	1.00	1.00	1.00
	Average	**1.00**	**0.99**	**0.99**
DL-SMOTE	Fake	1.00	0.96	0.98
	Real	1.00	1.00	1.00
	Average	**1.00**	**0.98**	**0.99**
Random forest 1	Fake	0.98	0.84	0.90
	Real	0.90	0.98	0.94
	Average	**0.94**	**0.91**	**0.92**
SVM	Fake	0.96	0.84	0.90
	Real	0.89	0.98	0.93
	Average	**0.93**	**0.91**	**0.91**

(Continued)

Table 2 (continued)

Methods	Tweet	Precision	Recall	F1 score
Naive Bayes	Fake	1.00	0.98	–
	Rea l	1.00	1.00	–
	Average	**1.00**	**0.99**	–
Random forest 2	Fake	1.00	0.94	–
	Real	0.99	1.00	–
	Average	**1.00**	**0.97**	–

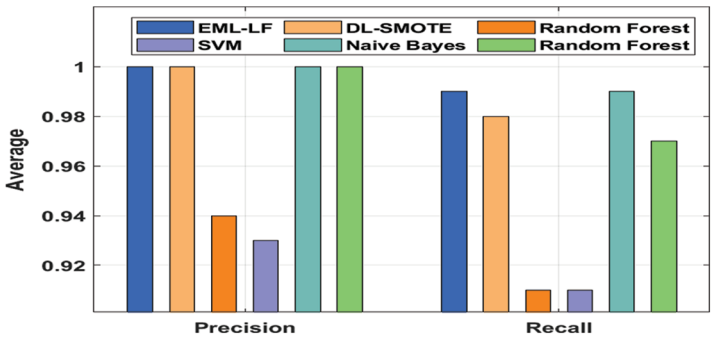

Figure 6: Average precision and recall analysis of the EML-LF model

In order to further validate the performance of the EML-LF model, another results analysis takes place on the Fake News Detection Liar benchmark dataset, as given in Tab. 3 and Fig. 7. The resultant values demonstrate that the NB model has showcased least performance with the accuracy of 72.6%, recall of 74.6%, precision of 91%, and F-score of 82%. Besides, the SSO algorithm has obtained better performance over the NB model with the accuracy of 78%, recall of 70.5%, precision of 100%, and F-score of 82.7%. Along with that, the DT model has demonstrated slightly enhanced outcome over the SSO algorithm with the accuracy of 79.8%, recall of 95.1%, precision of 83.2%, and F-score of 88.7%.

Table 3: Result analysis of the existing method with the proposed EML-LF method on fake news detection liar benchmark dataset

Methods	Accuracy	Recall	Precision	F-score
EML-LF	98.60	100.00	100.00	94.70
SSO	78.00	70.50	100.00	82.70
GWO	96.50	100.00	95.60	97.70
Decision tree	79.80	95.10	83.20	88.70
Naive Bayes	72.60	74.60	91.00	82.00
SVM	83.60	100.00	83.60	91.10
GBT model	79.80	95.50	82.90	88.80

(Continued)

Table 3 (continued)

Methods	Accuracy	Recall	Precision	F-score
Ridor	82.00	99.80	82.20	90.20
J48	82.20	100.00	82.30	90.30
SMO	82.30	100.00	82.30	90.30

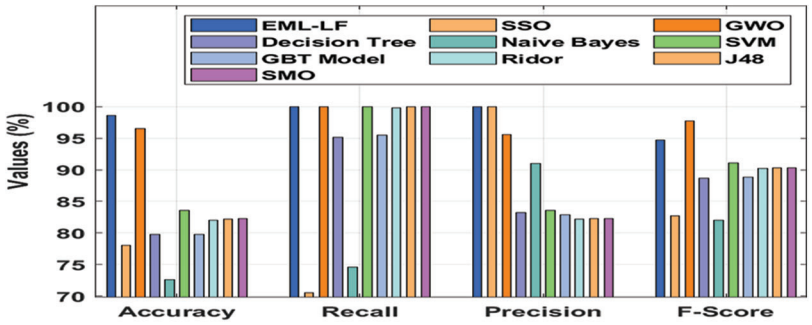

Figure 7: Comparative analysis of the EML-LF model with distinct measures

Next to that, the GBT model has attained moderate outcome with the accuracy of 79.8%, recall of 95.5%, precision of 82.9%, and F-score of 88.8%. Meanwhile, the Ridor model has obtained somewhat manageable outcome with the accuracy of 82%, recall of 99.8%, precision of 82.2%, and F-score of 90.2%. Simultaneously, the J48, SMO, and SVM models have portrayed reasonable outcome with the closer accuracy of 82.2%, 82.3%, and 83.6% respectively. Though the GWO algorithm has demonstrated near optimal results with the accuracy of 96.5%, recall of 100%, precision of 95.6%, and F-score of 97.7%, the presented EML-LF model has outperformed all the other methods with the accuracy of 98.6%, recall of 100%, precision of 100%, and F-score of 94.7%. From the above results, it is evident that the presented model is an appropriate tool for fake news and fake account detection on the social media.

5 Conclusion

In this paper, a new RDL-FAFND model has been developed for the identification of fake accounts and fake news on the social networks. The presented RDL-FAFND model involves two major operations namely the KH-DSAE based fake account detection model and the EML-LF based fake news detection model. The exploitation of the herding behavior of the krill's helps in adjusting the hyper parameters of the DSAE model. Similarly, the inclusion of the ensemble learning process helps in increasing the fake news detection rate. A series of experimentations have been performed for guaranteeing the improved fake account and fake news detection performance of the RDL-FAFND model. The detailed comparative results analysis has verified the supremacy of the presented RDL-FAFND model over the existing methods in terms of different measures. As a part of the future scope, the enrichment of the feature set from the social science knowledge domain (especially psychology) can be analyzed. It is believed that they can exhibit effective outcomes on the identification of fake accounts on the social networking sites.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Ahmad, M. Yousaf, S. Yousaf and M. O. Ahmad, "Fake news detection using machine learning ensemble methods," *Complexity*, vol. 2020, no. 8885861, pp. 1–11, 2020.

[2] S. Neelakandan, "Social media network owings to disruptions for effective learning," *Procedia Computer Science*, vol. 172, no. 5, pp. 145–151, 2020.

[3] N. R. D. Oliveira, P. S. Pisa, M. A. Lopez, D. S. V. de Medeiros and D. M. Mattos, "Identifying fake news on social networks based on natural language processing: Trends and challenges," *Information-an International Interdisciplinary Journal*, vol. 12, no. 1, pp. 38–51, 2021.

[4] S. Neelakandan, R. Muthukumaran and R. Annamalai, "Implementing campus indoor location tracking system," *International Journal of Engineering and Computer Science*, vol. 5, no. 5, pp. 16731–16735, 2016.

[5] M. Mohammadrezaei, M. E. Shiri and A. M. Rahmani, "Identifying fake accounts on social networks based on graph analysis and classification algorithms," *Security and Communication Networks*, vol. 4, no. 3, pp. 361–375, 2018.

[6] E. S. Madhan, S. R. Neelakandan and R. Annamalai, "A novel approach for vehicle type classification and speed prediction using deep learning," *Journal of Computational and Theoretical Nano science*, vol. 17, no. 5, pp. 2237–2242, 2020.

[7] J. Uthayakumar, D. Nivetha, D. Vinotha and M. Vasanthi, "Classification rule discovery using ant-miner algorithm: An application of network intrusion detection," *International Journal of Modern Engineering Research*, vol. 4, pp. 70–83, 2014.

[8] D. Kagan, Y. Elovichi and M. Fire, "Generic anomalous vertices detection utilizing a link prediction algorithm," *Social Network Analysis and Mining*, vol. 8, no. 1, pp. 27, 2018.

[9] Y. Boshmaf, D. Logothetis, G. Siganos, J. Leria, J. Lorenzo *et al.,* "Leveraging victim prediction for robust fake account detection in large scale OSNs," *Computers & Security*, vol. 61, no. 3, pp. 142–168, 2016.

[10] J. Cao, Q. Fu, Q. Li and D. Guo, "Discovering suspicious account in online social networks, information science," *Information Science*, vol. 3, no. 1, pp. 1–23, 2017.

[11] W. Han and V. Mehta, "Fake news detection in social networks using machine learning and deep learning: Performance evaluation," in *Proc. of the 2019 IEEE Int. Conf. on Industrial Internet (ICII)*, Orlando, FL, USA, vol. 11, pp. 375–380, 2019.

[12] A. Agarwal and A. Dixit, "Fake news detection: an ensemble learning approach," in *Proc. of the 2020 4th Int. Conf. on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, vol. 13, pp. 1178–1183, 2020.

[13] Y. Wang, W. Yang, F. Ma, J. Xu, B. Zhong *et al.,* "Weak supervision for fake news detection via reinforcement learning," in *Proc. AAAI Conf. on Artificial Intelligence*, New York, NY, USA, vol. 7, pp. 516–523, 2020.

[14] M. N. Nikiforos, S. Vergis, A. Stylidou, N. Augoustis, K. L. Kermanidis *et al.,* "Fake news detection regarding the Hong Kong events from tweets,in Proc," in *IFIP Int. Conf. on Artificial Intelligence Applications and Innovations*, Berlin/Heidelberg, Germany, Springer, vol. 3, pp. 177–186, 2020.

[15] C. L. M. Jeronimo, L. B. Marinho, C. E. Campelo, A. Veloso and A. S. Costa Melo, "Fake news classification based on subjective language," in *Proc. 21st Int. Conf. on Information Integration and Web-based Applications & Services*, Munich, Germany, vol. 2, pp. 15–24, 2019.

[16] M. Mahyoob, J. Al-Garaady and M. Alrahaili, "Linguistic-based detection of fake news in social media," *International Journal of English Linguistics*, vol. 11, no. 1, pp. 99–109, 2020.

[17] K. Shu, D. Mahudeswaran, S. Wang, D. Lee, H. Liu *et al.,* "A data repository with news content, social context, and spatiotemporal information for studying fake news on social media," *Big Data*, vol. 8, no. 3, pp. 171–188, 2020.

[18] S. Kumar, R. Asthana, S. Upadhyay, N. Upreti and M. Akbar, "Fake news detection using deep learning models: A novel approach," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, pp. 3676–3689, 2020.

[19] J. L. Alves, L. Weitzel, P. Quaresma and C. E. Cardoso, "A machine learning approach to analyse fake news," in *Proc. Iberoamerican Congress on Pattern Recognition*, Berlin/Heidelberg, Germany, Springer, vol. 11, pp. 72–84, 2019.

[20] U. Victor, "Robust semi-supervised learning for fake news detection," Ph.D Thesis, Prairie View A&M University, Prairie View, USA, 2020.

[21] X. Miao, H. Miao, Y. Jia and Y. Guo, "Using a stacked-autoencoder neural network model to estimate sea state bias for a radar altimeter," *PLOS ONE*, vol. 13, no. 12, pp. 208– 221, 2018.

[22] G. Wang, L. Guo, A. H. Gandomi, L. Cao, A. H. Alavi *et al.,* "Lévy-flight krill herd algorithm," *Mathematical Problems in Engineering*, vol. 38, no. 9, pp. 2454–2462, 2013.

[23] A. Thota, P. Tilak, S. Ahluwalia and N. Lohia, "Fake news detection: A deep learning approach," *SMU Data Science Review*, vol. 1, no. 3, pp. 1–10, 2018.

[24] M. Fayaz, A. Khan, J. U. Rahman, A. Alharbi, M. I. Uddin *et al.,* "Ensemble machine learning model for classification of spam product reviews," *Complexity*, vol. 12, no. 2, pp. 213–243, 2020.

[25] L. Liu, Y. Lu, Y. Luo, R. Zhang, L. Itti *et al*., "Detecting smart spammers on social network: a topic model approach," *Proceedings of NAACL-HLT*, San Diego, CA, pp. 1–28, 2016.

[26] T. Avudaiappan, Jenifer, S. Tumsa, S. Subashree and T. Jayasankar, "Twitter sentimental analysis using neural network," *International Journal of Scientific & Technology Research*, vol. 9, no. 2, pp. 2573–2577, 2020.

[27] M. Mohammadrezaei, E. Shiri and A. M. Rahmani, "Identifying fake accounts on social networks based on graph analysis and classification algorithms," *Security and Communication Networks*, vol. 12, no. 1, pp. 631–646, 2018.

[28] D. Mouratidis, M. N. Nikiforos and K. L. Kermanidis, "Deep learning for fake news detection in a pairwise textual input schema," *Computation*, vol. 9, no. 2, pp. 20–35, 2021.