Terrorism And Fake News Detection
Divya Tiwari, Surbhi Thorat
S. K. Somaiya Degree College of Arts, Science and Commerce, Somaiya Vidyavihar University, Mumbai, Maharashtra, India

ABSTRACT

Fake news dissemination is a critical issue in today's fast-changing network environment. The issues of online fake news have attained an increasing eminence in the diffusion of shaping news stories online. This paper deals with the categorical cyber terrorism threats on social media and preventive approach to minimize their issues. Misleading or unreliable information in form of videos, posts, articles, URLs are extensively disseminated through popular social media platforms such as Facebook, Twitter, etc. As a result, editors and journalists are in need of new tools that can help them to pace up the verification process for the content that has been originated from social media. existing classification models for fake news detection have not completely stopped the spread because of their inability to accurately classify news, thus leading to a high false alarm rate. This study proposed a model that can accurately identify and classify deceptive news articles content infused on social media by malicious users. The news content, social-context features and the respective classification of reported news was extracted from the PHEME dataset using entropy-based feature selection. The selected features were normalized using Min-Max Normalization techniques. The model was simulated and its performance was evaluated by benchmarking with an existing model using detection accuracy, sensitivity, and precision as metrics. The result of the evaluation showed a higher 17.25% detection accuracy, 15.78% sensitivity, but lesser 0.2% precision than the existing model. Thus, the proposed model detects more fake news instances accurately based on news content and social content perspectives. This indicates that the proposed classification model has a better detection rate, reduces the false alarm rate of news instances and thus detects fake news more accurately.

Keywords : Fake news, classification, stacking ensemble, news instances, news content, social-context features, social media.
I. INTRODUCTION

The research focuses on terrorism and fake news detection on social media. A growing interest related to fake news detection has attracted many researchers as fake information is circulated through online social media platforms such as Facebook, Twitter, etc. The fake content is spreading at a faster pace to gain popularity over social media, to distract people from the current critical issues. Most of the people believe that the information they receive from various social media sites is reliable and true, i.e., people are inherently truth-biased. Also, people easily trust and want to believe in what they actually interpret in them minds, i.e., confirmation-biased. In general, it has been analysed that human are unable to recognize deception effectively. Due to which a serious and negative impact of fake articles can be seen on society and individuals leading to an imbalance of the news ecosystem. It was observed that during US president election, most of the widely spread articles on social media were fake. Recently a fake video related to Kerela battling with floods was viral on social media platform (Facebook) claiming that the Chief Minister of the state is forcing the Indian Army to stop conducting the rescue operations in flooded regions of Kerela. Also, during India’s national election (2019), various WhatsApp groups (> 900,000) were created to disseminate the fake information regarding India’s ruling party. Most of the fake articles are created to confuse people and trigger their distrust. Such problems led researchers to look at some automated ways to access the ground truth values of fake text on the basis of the textual content posted in articles on social platforms. Social media enables to maintain and develop relations with others. It helps the users to present themselves by creating their profiles, sharing information through photos, images, and text to link with other members. Some of the most popular social media sites are Facebook, Twitter, Instagram, WhatsApp, LinkedIn, WeChat, Snapchat, Foursquare. With the popularity of social media sites level of usage to share content on online social media has increased. There are several reasons for the change in behaviour for such kind of consumptions. The content shared on social media platforms requires less time and cost than on newspapers or traditional news media. Easier to share content in the form of video, blogs, posts with friends or users. This gives the growth ease to the authors and publishers to publish their contents as articles on collaborative environments. There is 13% of the global increase in social media usage since 2017. Distribution and creation of news content in the form of posts, blogs, articles, images, videos, etc., have been spreading through social media websites. This increase in social media also gives rise in the spread of fake articles over the internet.

The researchers found that the hybrid algorithm performed slightly better than how they did individually.

From the literatures, it was established that the most effective approach to detect fake news based on news content and social content perspectives is by employing hybrid deep learning approaches. One of the recent and effective models was proposed in [24]. The model effectively minimized false positives as well as deliver better detection rates with an accuracy of 82% and intuitively identified relevant features associated with fake news stories without previous knowledge of the domain. However, the model being a supervised learning approach failed to construct a multitude decision at training time and also the variances used for classification of news was very high.
These resulted to high false positive instances in the prediction.

Therefore, an improved fake news detection classification model that would incorporate both reinforcement and supervised approach is highly needed. Thus, in this paper, an attempt was made to develop an improved model with the capability of accurately detecting fake news on the social media platform by classifying news content as either real news or fake news using a hybrid approach of supervised and reinforcement learning approaches.

**II. LITERATURE REVIEW**

The automated systems can play an important tool for identifying fake stories, articles, blogs, clicks which manipulate public opinion on social networking sites. Several hybrid algorithms have been developed for fake news detection using data mining methods. In [19], a framework was proposed by synergizing AdaBoost and SVM classifiers on topological, crowdsourced and content-based (Hashtags, Mentions, URLs, and Phrases with sentiment extraction) features to detect political misinformation at the early stage on Twitter. The classifier performed well as a supervised learning approach, but the extracted features were substituted for content.

This study showed that the only supervised learning approach is not adequate for accurate fake news detection. In, a hybrid deep model was proposed to address the timely problem of fake news detection by incorporating the text, the response an article receives, and the users who source it. The model was able to address the timely problem of fake news detection. Meanwhile, it was only based on user behaviour and does not incorporate reinforcement learning and humans in the learning process and thus affected the accuracy of the detection. In, the identification of fake news on Twitter was formulated as a binary machine learning problem. The result showed that instead of creating a small, but accurate hand-labelled dataset, using a large-scale dataset with inaccurate labels yields very good results. In, a tensor modelling of how to accurately distinguish different categories of fake news based mainly on the content, where latent relations between articles and terms were captured as well as spatial or contextual relations between terms, towards unlocking the full potential of the content was proposed.

The proposed algorithm, a supervised learning approach was able to identify different news categories with corpus with a percentage of 80%, but with high false positives rate. In, the tensor decomposition ensembles model was proposed by clustering the news content of fake news articles into different categories. They were able to do this by capturing spatial relations between terms for each article. This was able to identify all different categories of fake news within the dataset. Therefore, it was noted in and that they are mainly supervised learning approaches. Though they all yield a good detection rate, but they have not completely stopped the spread because of their inability to accurately classify news. In, a stacked ensemble of 5 independent classifiers in the context of the natural language processing was developed to detect fake news. The stack ensemble was a two-layer classifier architecture that leverages predictions from weaker slave classifiers as features to a stronger master classifier. The classification experienced a difficulty in which the test set was far greater than that of the development data split which impacted results. Also in some cases, multiple layers of neural networks are required for effective training of models. This revealed that a stack ensemble method of classifiers is appropriate to detect fake news accurately. In, a framework that detects and classifies fake news messages from Twitter posts using a hybrid of Convolutional Neural Networks and Long-Short...
Term Recurrent Neural Network models was proposed.

The proposed work using this deep learning approach achieves 82% accuracy and intuitively identified relevant features associated with fake news stories without previous knowledge of the domain. The dataset used was limited because deep learning models such as CNN and RNN require much larger datasets.

This framework revealed that accuracy of the fake news detection is better achieved using deep learning methods as compared to the conventional machine learning algorithms.

Despite all these encouraging results, there are still many open questions associated with fake news detection. One interesting direction would be to build models that will incorporate both unsupervised and reinforcement learning which could lead to more accurate and timely predictions.

III. METHODOLOGY

In this study, an improvement was made on the fake news identification on Twitter network model proposed by [24] in which the synergy of Convolutional Neural Networks and Long-Short Term Recurrent Neural Network models was proposed to detect fake news on twitter. A PHEME dataset containing 5,800 tweets was used. The model conceptualisation and the detailed algorithm of the proposed model are presented as follows:

A. Conceptual Model Description

This proposed model uses a stacking ensemble method of three machine learning algorithms namely: Support Vector Machines (SVM), Recurrent Neural Networks (RNN) and Random Forest which are supervised machine learning algorithms as against the existing model which made use of a hybrid of Convolutional Neural Network and Recurrent Neural Networks algorithms. This method was adopted to improve the prediction rate of the classification model.
which in turn improves the ability of the model to accurately classify news as either fake or real news. The proposed conceptual block diagram for the classification model for fake news detection on social media is shown in Fig. 1 and the block diagram for the entire classification process is shown in Fig. 2. These Figures shows the details of the data collection and pre-processing phases involved in the model. This proposed model uses a stacking ensemble method of machine learning and deep learning algorithms in order to improve the prediction rate of the classification model which in turn improves the ability of the model to accurately classify news as either fake or real news.

B. Model Development Process

The stages applied to the development of the model is as follows:

1. Dataset used was obtained from PHEME fake news dataset and analyzed to know the true state of the dataset, it was cleaned by removing special characters, html tags and other unclean texts.
2. Tfidf was used to convert the cleaned dataset into vector. The labelled feature which contains real news and fake news texts was converted to numerical format using categorical encoding algorithm as shown in Fig. 3. This algorithm was employed to handle this since ensemble algorithms cannot process categorical variables and the performance of the proposed model depends on the function of encoded variables.
3. The dataset features were then normalized to ensure that the features are in the same scale to enhance the performance of the model
4. Relevant features were selected from the normalized dataset using entropy-based feature selection process. The selected features were then fitted into Support Vector Machine, Random Forest, and Recurrent Neural Network learning algorithms separately to generate the base models. The base models were fitted into the meta-model to generate the final model which is the stack ensemble model.
5. The generated stack ensemble model now classifies the news instances into real or fake. The model was then tested with new network instances and the classification generated serves as the result of the model.

6. The performance of the model was then evaluated by benchmarking with the existing classification model [19] using detection accuracy, sensitivity, false alarm rate and precision as performance metrics.

a. Data Pre-processing

The PHEME dataset which contains five major news events was stored in .csv format. Pandas was used to combine all the news events; it has a total of 103212 news instances which is the combination of original tweets and user reaction to the tweets.

The dataset has 34 features including the date the news event was created. The features are; coordinates created, favorite_count, has_url, hashtags_count, id, in_reply_id in_reply_user, is_rumor, symbols_count, text, etc. The text features and target variable (is_rumour) was used cleaned to be used for the classification model.

b. Feature Selection

The dataset records used for this study is a multi-dimensional dataset containing features that are not relevant in formulating the proposed model. Thus, the need to do dimensionality reduction by selecting the best features from the high dimensional dataset. Mutual information gain features selection algorithm was employed in selecting the best features from the dataset based on the information gain.

c. Text to Vector Conversion

The bag of words generated after cleaning the dataset was further processed by converting to vectors using the Term Frequency-Inverted Document Frequency (Tfidf) tool as one of the texts to vector conversion tool in Python. This is an important step in developing a machine learning/deep learning model which will allow it to understand the dataset. The term frequency is the type of path that appropriates the counts of words present in the document and figures out the inequality between the documents. Each document is characterized by a vector that contains the word count. Each word count is
transformed into the possibility of such word current in the documents. The Tf-idf is a statistical measure used in this study to evaluate how important a word is to a document in the dataset. It was used to measure the frequency of the time in the collection for weighting and ranking for words in the bag of words. Tf-idf as used in this study measure the sum of term frequency like number multiplied by term importance.

d. Feature Normalization

The Vectorized dataset was normalized by giving all features an equal weight in order to decrease computation time and increase the detection accuracy of the proposed model in a pre-processing dataset for the machine learning model. The features are scaled into a specific range of 0 and 1 in order to ensure that all features are in the same scale. Min-Max normalization was used to scale the features from a range of values to a new range of values.

C. Model Formulation

The detailed algorithm of the proposed model formulation is as presented in Fig. 4. The formulation started with the identification of the spread of fake news as a problem on social media and ended with predictions of either fake or real news. The classification algorithm used to categorize each data into the class (Fake and real news) to identify the category or class to which each data will fall under is presented in Fig. 5. The algorithm of the stacking ensemble model, which revealed how the predictions from the individual algorithms are used as features to build the proposed model is also presented in Fig. 6. This algorithm averages out noise from the classifiers to enable improved predictive accuracy performance of the model. The Support Vector Machine (SVM) algorithm, a supervised learning algorithm used for classification analysis is shown in Fig. 7. The main reason for using SVM is because the problem of fake news detection is not linearly separable. SVM was used to find the best separating hyperplane also called decision boundary. Also, to design a hyperplane that classifies all dataset into two classes i.e., training and testing dataset. SVM helps to label the datasets appropriately since mislabeling can decrease model performance. Random Forest which was used as the reinforcement learning method of the ensemble model operates by constructing a multitude decision at training time and also used to reduce the variances used for classification of news. The algorithm is presented in Fig. 8. By incorporating the reinforcement learning into the modelling process will enhance the detection rate of the model. The RNN algorithm was employed to model the sequence of the data in order to remember the all the inputs throughout the time of modelling. This helps to address the problem of overfitting, underfitting and leakage of the training dataset, to improve the prediction accuracy of the model. Thus, the pre-processed dataset was used to train each of the algorithms individually as base-level classifiers. The predictions of the three models are then used as inputs in a Random Forest algorithm (meta-classifier) to form the final ensemble model.
Fig. 5. Proposed Model for fake News Detection

OUTPUT: Random Forest fake news classification model BEGIN
1. For each tree in the forest do
2. Sample N datapoints with replacement;
   For each internal node in the tree do
   Randomly sample m attributes (m = d)
   Select the feature from this randomly selected set that provides
   the most information gain
   end For
3. Return Fully grown decision tree
4. end
5. return Random Forest END

Fig. 6. Random Forest Classification

Fig. 7. Categorical Attribute Encoding Algorithm

IV. RESULTS AND DISCUSSION

The proposed model was simulated and evaluated using Python 3.7.3 programming language with its machine learning library (i.e., Scikit-learn library). Jupiter notebook was used for the coding while Panda, a data analysis library was used for the pre-processing of the dataset. The detailed results are presented as follows:

A. Data Pre-processing Results

The PHEME Dataset contains source tweets and user reactions to the tweets have a total number of 103,212 news instances which has been classified into 31,430 fake news instances and 71,782 real news instances as shown in Fig. 9. The graphical representation of the proportion of source tweets to the user reaction of each news event is also presented in Fig. 10. The overall dataset was divided into eighty percent as training dataset and twenty percent as test dataset which are 82,569 and 20,642 respectively. For validation of the dataset, cross- validation technique
was applied using the `train_test_split` function of the scikit-learn library. The eighty percent (82,569) of the dataset was further split into 66,055 (80%) and 16,514 (20%).

![Fig.8. Bar Chart Showing the Proportion of Fake News to Real News](image)

The result from the confusion matrix in Table 1 showed that the proposed model was able to correctly classify 12,544 (87% of real news instances) as real news (i.e., True Positives (TP)), while 4329 (70% of fake news instances) was correctly classified as fake news instances (i.e., True Negatives (TN)). The result also showed that 1,885 (13% of real news instances) were misclassified as fake news instances (i.e., False Positives (FP)), while 1,885 (30% fake news instances) were misclassified as real news instances (i.e., False Negatives (FN)). This shows that the proposed model detects fake news with a reduced false alarm rate.

The testing dataset was also fed into the existing model, the result from the confusion matrix as shown in Table 2, shows that 14,429 (100% of real news instances) were classified as real news. The existing model confusion matrix result also shows that the model was unable to detect any fake news instances as fake news, it then classified all 6,214 fake news instances as real news (i.e., False Positives), then, none of the real news instances were misclassified, this makes the existing model to predict with high-rate false alarm.

![Fig. 9. Bar chart showing the proportion of Source tweets and User reactions](image)

### Table 1. Confusion Matrix Result of the Proposed Model

| Actual (Real News) | Real News (Predicted) | Fake News (Predicted) |
|--------------------|-----------------------|-----------------------|
| 12544(TP)          | 1885(FN)              |
| 1885(FP)           | 4329(TN)              |

### Table 2. Confusion Matrix Result for the Existing Model

| Actual (Real News) | Real News (Predicted) | Fake News (Predicted) |
|--------------------|-----------------------|-----------------------|
| 14429(TP)          | 0(FN)                 |
| 6214(FP)           | 0(TN)                 |
The result of the study showed that the stack-ensemble of SVM, Random Forest and Recurrent Neural Network (base learners) have accuracy of 69.2%, 71.9% and 86.6% respectively while, Random Forest (meta-classifier) trained with the output of the predictions of the base learners has an accuracy and sensitivity of 81.9% and 82% respectively which is better than the existing model which has a percentage of 70%. The existing model was unable to detect any labelled fake news instances as fake news while the developed model recorded a precision of 82%. The simulation result showed that the developed model could detect more fake news instances than the existing model.

A. Model Evaluation Results
The performance of the proposed model was evaluated by benchmarking with the existing model [19] using detection accuracy, sensitivity, false alarm rate and precision as performance metrics according to [8]. All these performance metrics used were calculated using the result of the confusion matrix table which is categorized under true negative, true positive, false positive and false negative respectively as follows:

Accuracy=(TP+TN/TP+FP+TN+FN) *100 (1)
Sensitivity=TP/TP+FN (2)
Precision=(TP/TP+FN)*100 (3)

The result of the evaluation and their percentage difference is presented in Table 3. The table shows that the proposed model has a 17.25% higher detection accuracy and 15.78% sensitivity, but a lesser 22.2% precision than the existing model. The higher precision of the existing model emanated because the existing model was unable to detect any fake news instances as fake news, which led to the high positive rates.

Tables 4 and 5 show the screenshot of the classification for the proposed model and the existing model indicating precision, sensitivity, and f1-score. Fig. 11 showed the Area under Curve of 88% for the proposed model. Figs. 12 13 and 14 are the graphs for the precision and sensitivity that show the benchmarking results of the existing model and the proposed model respectively.

The evaluation results indicate that the proposed model is more sensitive and accurate to classify news as either fake or real than the existing model.

### Table 3. Percentage Difference between the Existing Model and Proposed Model

| S/N | Metrics      | Existing model | Proposed model | Percentage difference |
|-----|--------------|----------------|----------------|-----------------------|
| 1   | Accuracy     | 69.89%         | 81.9%          | 17.25%                |
| 2   | Precision    | 100%           | 82%            | -22.2%                |
| 3   | Sensitivity  | 70%            | 82%            | 15.78%                |

### Table 4. Classification Table for Proposed Model

|   | Precision | recall | F1-score | Support |
|---|-----------|--------|----------|---------|
| 0 | 0.87      | 0.87   | 0.87     | 14429   |
| 1 | 0.70      | 0.70   | 0.70     | 6214    |
| micro avg | 0.82    | 0.82  | 0.82     | 20643   |
| macro avg  | 0.78    | 0.78  | 0.78     | 20643   |
| weighted avg | 0.82   | 0.82  | 0.82     | 20643   |

### Table 5. Classification Table for Existing Model

|   | Precision | recall | F1-score | Support |
|---|-----------|--------|----------|---------|
| 0 | 1.00      | 0.70   | 0.82     | 20643   |
| 1 | 0.00      | 0.00   | 0.00     | 0       |
| micro avg | 0.70    | 0.70  | 0.70     | 20643   |
| macro avg  | 0.50    | 0.35  | 0.41     | 20643   |
| weighted avg | 1.00   | 0.70  | 0.82     | 20643   |

Fig.10. Area under Curve of the proposed model.
V. CONCLUSION

In this study, a classification model for fake news detection on social media using a stack ensemble method of three algorithms to increase the detection accuracy was developed. The proposed model was simulated and it was obvious in the results that the proposed model has a high reduction in the instances of false positives states and high detection accuracy and sensitivity rates, thus has a better performance in detecting fake news instances accurately. Therefore, the proposed model can be adapted by the social media administrators to combat the spread of fake news. The future works is directed to having a model that will the address the timely prediction of the fake news in social media. The proposed model was simulated and it was obvious in the results that the proposed model has a high reduction in the instances of false positives states and high detection accuracy and sensitivity rates, thus has a better performance in detecting fake news instances accurately. Many it companies has been working on stop hate spread but this is one step further which focuses to stops terrorist activities and fake news spreading through social media.

VI. REFERENCES

[1]. N. J. Conroy, V.L. Rubin, Y. Chen, Proceedings of the Association for Information Science and Technology 52(1), (2015)
[2]. Fake news on what's app. http://bit.ly/2miuv9j. Last accessed: 27-08-2019
[3]. K.R. Canini, B. Suh, P.L. Pirolli, in Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on (IEEE, 2011), pp. 1–8
[4]. H. Ahmed, I. Traore, S. Saad, in International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments (Springer, 2017), pp. 127–138
[5]. A. Gupta, H. Lamba, P. Kumara guru, in eCrime Researchers Summit (eCRS), 2013 (IEEE, 2013), pp. 1–12
[6]. A.H. Wang, in Security and cryptography (SECRIPT), proceedings of the 2010 international conference on (IEEE, 2010), pp. 1–10
[7]. F. Benvenuto, G. Magno, T. Rodrigues, V. Almeida, in Collaboration, electronic
messaging, anti-abuse and spam conference (CEAS), vol. 6 (2010), vol. 6, p. 12

[8]. I. Sen, A. Aggarwal, S. Mian, S. Singh, P. Kumara guru, A. Datta, in Proceedings of the 10th ACM Conference on Web Science (ACM, 2018), pp. 205–209

[9]. S.M. SIRAJUDEEN, N.F.A. AZMI, A.I. ABUBAKAR, Journal of Theoretical & Applied Information Technology 95(17) (2017)

[10]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, B.Y. Zhao, in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (ACM, 2010), pp. 35–47

[11]. P. Dewan, P. Kumara guru, in Privacy, Security and Trust (PST), 2015 13th Annual Conference on (IEEE, 2015), pp. 85–92

[12]. A. Aggarwal, S. Kumar, K. Bhargava, P. Kumara guru, (2018) 2

[13]. A. Gupta, H. Lamba, P. Kumara guru, A. Joshi, in Proceedings of the 22nd international conference on World Wide Web (ACM, 2013), pp. 729–736

[14]. A. Gupta, P. Kumara guru, in Proceedings of the 1st workshop on privacy and security in online social media (ACM, 2012), p. 2

[15]. News trends database. https://bit.ly/2zVRLxK. Last accessed: 18-10-2017

[16]. Kaggle database. https://bit.ly/2Ex5VsX. Last accessed: 24-10-2017

Cite this article as:

Divya Tiwari, Surbhi Thorat, "Terrorism And Fake News Detection", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 313-323, November-December 2021. Available at doi : https://doi.org/10.32628/CSEIT217670

Journal URL : https://ijsrcseit.com/CSEIT217670