

# Detection of fake news from social media using support vector machine learning algorithms

M. Sudhakar<sup>\*</sup>, K.P. Kaliyamurthie

*Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai, India*

## ARTICLE INFO

**Keywords:**  
 Fake news  
 Social media  
 Machine learning  
 Detection system  
 Classification  
 TF-IDF

## ABSTRACT

Never happened before in human history the spreading of fake news; now, the development of the Worldwide Web and the adoption of social media have given a pathway for people to spread misinformation to the world. Everyone is using the Internet, creating and sharing content on social media, but not all the information is valid, and no one is verifying the originality of the content. Identifying the content's essence is sometimes complicated for researchers and intelligent researchers. For example, during Covid-19, misinformation spread worldwide about the outbreak, and much false information spread faster than the virus. This misinformation will create a problem for the public and mislead people into taking the proper medicine. This work will help us to improve the prediction rate. Here we investigate the ability of machine learning classifiers and deep learning models: Naive Bayes, Logistic Regression, Support Vector Machine, Decision Tree, Random Forest and K-Nearest Neighbor. Deep learning models include Convolutional Neural Networks and Long Short-Term Memory (LSTM). The various types of machine learning and deep learning models will be trained and tested using the Covid-19 dataset (1,375,592 tweets).

## 1. Introduction

These days' fake news is continuously growing, and sometimes it is challenging to find harder and harder what is true and what is fake. After two weeks of the Russia and Ukraine war, many flows of false information happens. Some people began to spread the war is spoof a video of women and men having fake blood applied to their faces and shared on social media, and many people viewed their posts. People have hired them to act so that everyone has mercy on their country. Here the below picture shows an example of fake news (Fig. 1). But this video is not related to the war; this video was taken during the Ukraine Tv series in 2020.

The second post shows two Uk and Ukrainian men holding wooden which went on viral (Fig. 2).

This picture was taken during the training period of volunteers of Ukraine civilians. This type of fake news can create a problem inside and outside the community. The following picture shows that Ukraine's vice president's wife joined the Ukraine armed force to fight against the Russian armed force (Fig. 3). This is fake because Ukraine doesn't have a vice president.

The graph shows the Google search trends of fake news about the

Covid-19 pandemic—the misleading information spreading everywhere. Due to Covid-19, mass death happened in Iron, but this fake news was shared (Fig. 4). During Covid-19, social media content was analyzed from 87 countries and found much misleading information shared on social media. WHO guided the public in reporting the fake news the Covid-19. The government and other organizations in the world taken an effort to show people how to handle or identify fake news.

## 2. Background of fake news

Currently, fake news is more prevalent on social media channels as compared to traditional media [1]. As a result of this problem, many researchers are focusing on developing several fake news detection frameworks, which is a crucial and challenging task. A model to detect fake news aims to spot or identify misleading news by analyzing previously reviewed real and fake news. As a result, a high-quality and large-scale dataset is required to perform this task accurately and efficiently. Fake news and natural language processing (NLP) researchers face the difficult task of creating multi-language models that can be used in any of the world's 7000 + languages. Multimodal data from multiple languages can be challenging to collect and analyze simultaneously for a

\* Corresponding author.

E-mail addresses: [sudhakarmtech@gmail.com](mailto:sudhakarmtech@gmail.com) (M. Sudhakar), [kpkaliyamurthie@gmail.com](mailto:kpkaliyamurthie@gmail.com) (K.P. Kaliyamurthie).



**Fig. 1.** Fake image during Russia and Ukraine War.



**Fig. 2.** Fake guns were given to civilian.



**Fig. 3.** Fake pics of Ukraine VP.

given task, making it essential to employ a framework that allows for the manageable generalization of a visual language model [1]. In late 2019, the biggest pandemic around the globe Coronavirus Disease, known as COVID-19, generated a massive amount of informative data about COVID-19. Platforms for spreading such information, like mass media and social media, make it possible for the information to reach a large audience [2]. Unfortunately, not all of the information is accurate or trustworthy. Some of the information spreading around those platforms can be categorized as misleading or even identified as false news. Notably, various countries may have different situations and strategies to control the spread of COVID-19, which also leads to a considerable amount of inappropriate news sharing [3]. For example, “The spread of COVID-19 is linked to 5G mobile networks”, “Sunny weather protects you from COVID-19”, and “Place a halved onion in the corner of your

room to catch the COVID-19 germs”. Social media facilitated the rapid dissemination of this and similar false news stories. During the early stages of the pandemic, the wave of misinformation was so massive that the authorities had coined a word for it: “infodemic”. Meanwhile, a lot of fake news was produced in various languages to spread more easily to particular ethnic groups [4]. Thus, it is very challenging for authoritative organizations to respond promptly to the spread of fake news. Failing to detect and stop multilingual COVID-19 misinformation can lead to mistrust, panic buying, social distancing, and refusal to get tested and vaccinated.

Researchers have been focusing on machine learning-based NLP (Natural Language Processing) strategies to prevent the spread of misinformation. To identify misinformation, one study [5] employed twenty-three supervised machine learning models. Increasingly successful models based on deep learning approaches have recently been adopted to detect misinformation. For example, used BERT to identify misinformation for short text and had excellent results. Similarly [6], propose a model for detecting fake COVID-19 news. Research studies have demonstrated outstanding results in classifying COVID-19 news using machine learning methods.

Presented a detailed analysis of recent machine learning algorithms and their findings for fake news detection. This study provided the detail of datasets used for the experiments in terms of the efficiency and accuracy of the proposed models [7]. The author [8] used standard language features for multi-language sentiment analysis with high-accuracy results. The authors suggested that this is incredibly convenient for real-time applications. The author [9] proposed a technique for fake news detection based on the statement conflict to be classified as agree or disagree. The results showed the significance of the proposed technique and outperformed state-of-the-art methods using one dataset.

### 3. Related work

#### 3.1. Detecting fake news: social media

Fake news and hoaxes have been there since before the advent of the Internet. The authors suggest that the most widely agreed-upon definition of fake news is that counterfeit or twisted journals, articles, blogs, and news confuses fully confuse the readers or the audience between what is right and what is wrong. In this research, the authors analyze the prevalence of fake news considering the advances in communication made possible by the drastic rise of social networking sites [10]. The aim of this research work to develop a solution that users can utilize to detect and filter out sites containing false and misleading information. In conclusion, they use simple and costless selected titles and post features to identify fake posts accurately. The experimental results show a 99.4 % accuracy using the logistic classifier (Table 1). Artificial Intelligence and Neural networks were used to detect credit card fraud, and the dataset's distribution is highly imbalanced. Therefore, the authors designed and used under-sampling and oversampling techniques to balance the data. Again in their research, data mining techniques were also implemented to achieve more accuracy in the fraud detection system when they used a hybrid model combining pre-existing supervised and unsupervised learning techniques for more accuracy.

#### 3.2. Fake news detection based on machine learning and deep learning algorithms

In their research work, authors suggested that machine learning, data science, and deep learning will help us to credit card fraud detection, and these types of fallacious activities can be done. The advantages of these three combination models will help the banking sectors and financial institutions detect fraud as much as possible before theft. In the future, we have to use a combination of supervised and unsupervised learning approaches [11]. This paper proposes a model for recognizing

## Online searches for Misinformation, Disinformation and Fake news at all-time high during COVID-19

Google Trends Relative Popularity Index for the topics Misinformation, Disinformation and Fake news

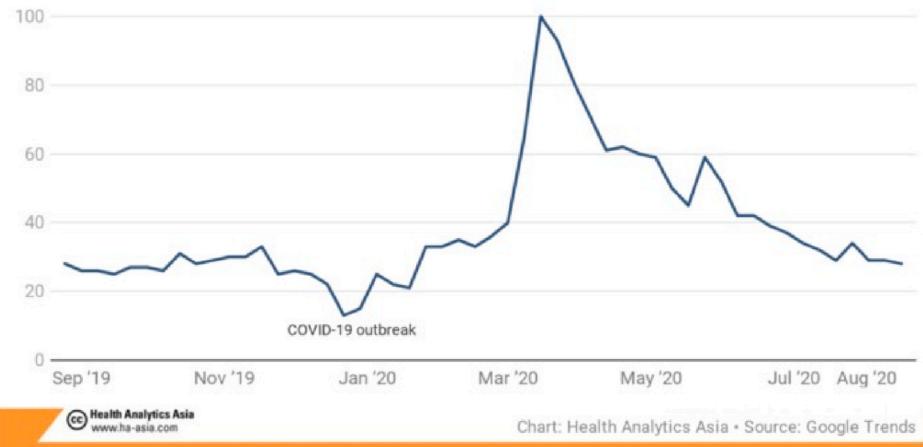


Fig. 4. Google search fake news about Covid-19.

**Table 1**  
Comparison results.

| Algorithms             | Precision | Recall | F1 Score | Accuracy |
|------------------------|-----------|--------|----------|----------|
| Logistic Regression    | 95.2 %    | 95.2 % | 95.2 %   | 95 %     |
| Naïve Bayes            | 79 %      | 73 %   | 71 %     | 74 %     |
| Long Short-Term Memory | 65 %      | 62 %   | 35 %     | 54 %     |
| Support Vector Machine | 98 %      | 98 %   | 98 %     | 98 %     |

forged news messages from Twitter posts by figuring out how to anticipate precision appraisals because of computerizing forged news identification in Twitter datasets [12]. As a result, the authors compared five well-known Machine Learning algorithms, like Support Vector Machine, Naïve Bayes Method, Logistic Regression, and Recurrent Neural Network models, separately to demonstrate the efficiency of the classification performance on the dataset. In conclusion, results obtained from

different learning algorithms were compared, and the result showed that SVM and Naïve Bayes classifier outperformed the other algorithms [13].

### 3.3. Which machine learning paradigm is for fake news detection?

The author introduces a new dataset, namely LIAR, that is used to detect fake news automatically. Compared with the previous data set, LIAR is an order of magnitude higher, making it possible to develop statistical and computational methods to see fake news. The different backgrounds of different speakers also contribute to extensive research on the development of counterfeit news detectors. We show that combining metadata with text can significantly improve particle holiday news detection. With detailed analysis reports and links to source documents in the data set, automatic fact-checking tasks based on redundant knowledge can also be explored in the future. Our corpus can also be used to classify NLP locations, extract parameters, model topics, etc.

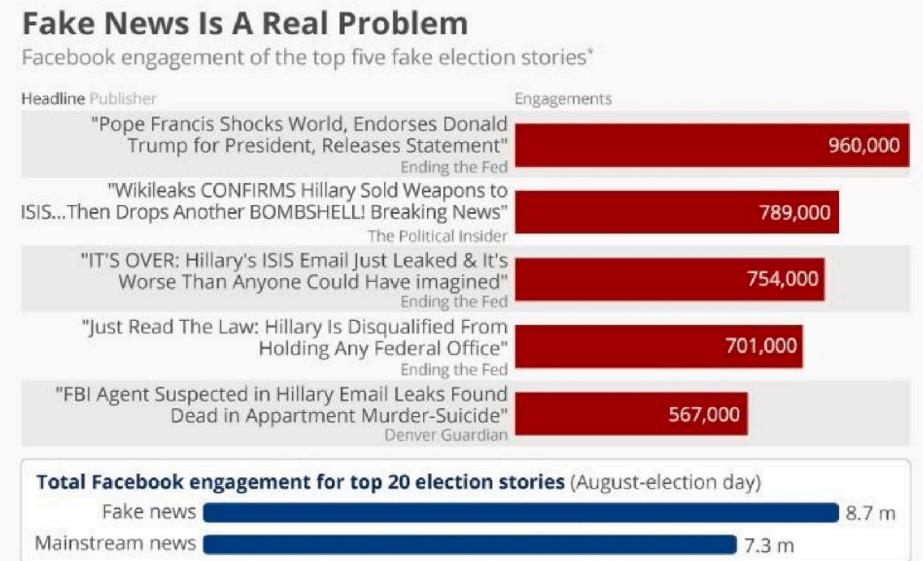


Fig. 5. Engagement is measured based on shares, comments, likes.

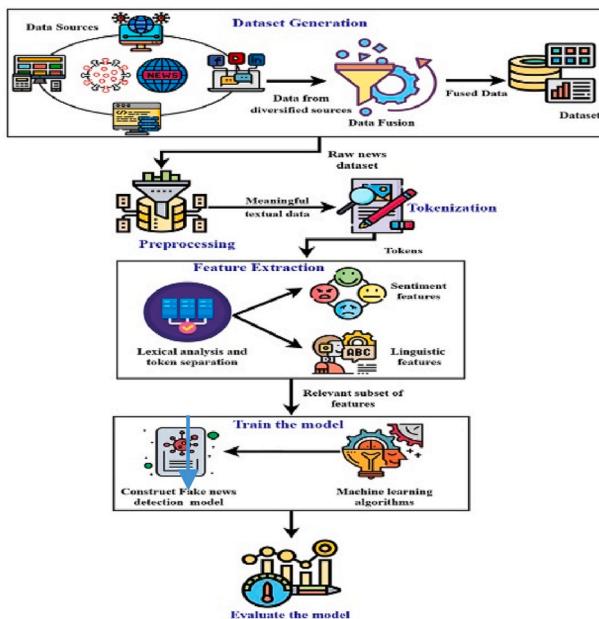


Fig. 6. Work flow of fake news detection.

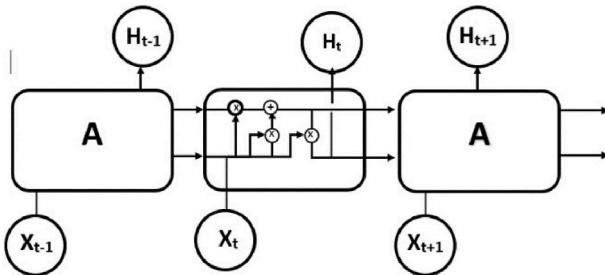


Fig. 7. LSTM architecture.

Rumour Investigation. The data are collected from the www, which includes articles from various news. The main aim of the author is to determine the pattern of distinguishing misinformation and real news. The author uses the LIWC tool to extract various text functions from the article and uses many functions as input to the model [14]. The model is trained, and parameters are fine-tuned to obtain the best accuracy [15]. We use several performance indicators to compare the results of each algorithm. Cooperative students performed better than individual students on all performance indicators.

#### 3.4. Detection of online fake news using N-gram analysis and machine learning techniques

Fake news significantly socioeconomic life, especially in the political world. Counterfeit news detection is an emerging research area gaining interest but involves some challenges due to limited available resources (i.e., datasets and published literature). In this paper, the author utilizes a fake news detection model that uses n-gram analysis and machine learning techniques. As a result, the author investigates and compares two different feature extraction techniques and six different machine classification techniques. Experimental evaluation yields the best performance using Term Frequency-Inverted Document Frequency (TF-IDF) as a feature extraction technique and Linear Support Vector Machine (LSVM) as a classifier, with an accuracy of 92 % [16] (see Fig. 5).

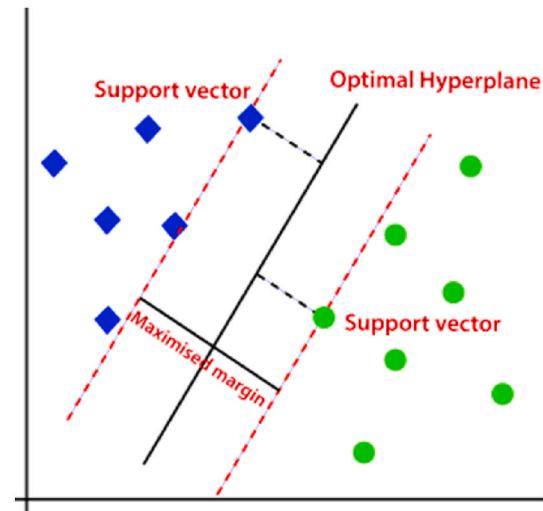


Fig. 8. SVM

## Classifier Prediction

|              | Positive       | Negative       |
|--------------|----------------|----------------|
| Actual Value |                |                |
| Positive     | True Positive  | False Negative |
| Negative     | False Positive | True Negative  |

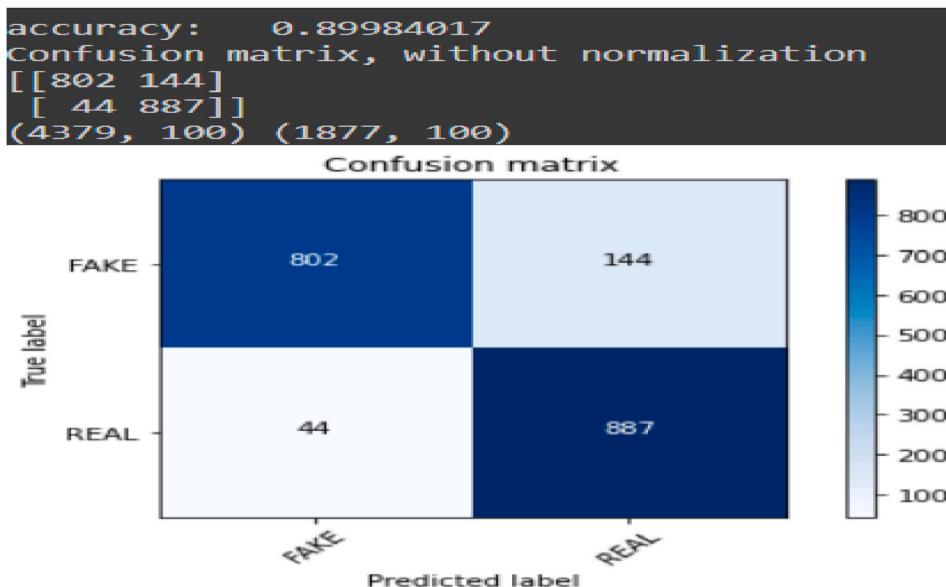
Fig. 9. Confusion matrix.

#### 4. Methods used to detect the fake news

Fig. 6 shows the entire workflow of the detection of fake news. All the experimental data was collected from Twitter in the selected areas [17]. We used normalization to manipulate the retrieved raw data. The next step we used was to remove the replication of data. In the final step, we used the machine learning method for classification (see Fig. 7–9).

The primary source of our data is coming from Twitter. We have given and created a Twitter developer account; after that, we have to start posting on Twitter. We can download many tweets based on the keywords, Id, name, and text; only the user verified from Twitter. Twitter will take a long process to verify the user, and if the user is confirmed, it will show as a blue tick on the user profile. Our dataset was collected from the message 948373. Twitter has two types of user accounts; the first one is the older version which consists of two character attributes it has 9 to 10 digits, and the second one is a new 18-digit number [14]. We have to convert verified user columns to labels. If the user is confirmed, it will indicate 0; otherwise, it will display 1.

Here punctuations are removed, and all of the datasets are converted into lowercase letters. Various punctuations and emotions users used in the tweets it will not help in the detection methods. Empty columns have been removed. Repeated post, characters, tags, and URL has been



**Fig. 10.** Confusion matrix of KNN classifier.

removed from our dataset.

Once our dataset is ready, it will give us a clear understanding and visualization of the graphs. This graph will show us a clear understanding of our dataset's categorization.

Here we used the tokenization function. This one will help us separate more important body messages into smaller words. Url will describe the location of the destination message, or it will not be like the destination message. Maybe this Url doesn't have value or has one or more values. Four types of messages will show to us here,

1. True Positive is the number of correct messages classified as believable messages.
2. True Negative is the number of correct messages classified as unbelievable messages.
3. False Positive is the number of incorrect messages classified as believable messages.
4. False Negative is the number of incorrect messages classified as unbelievable messages.

TF-IDF technique will help us to compute the weight of each word. This technique is primarily used in the retrieval of information and text-mining processes [18]. With the help of TF, we can summarize how often a given text appears in the given document. We are not going to use the entire data set for further analysis. Machine Learning Algorithms,

- Logistic Regression

This algorithm is used to predict the probability and categorize the dependent variable, and this dependent variable is based on binary. There are two types of binary variable codes 0 and 1. If the code is 1 means success and 0 means failure or no. It is a linear regression model used in the cost function and can be defined as a sigmoid function [19]. The cost function is between 0 and 1, so linear functions failed to represent the value as per the logistic regression hypothesis. So this is classified into binomial, multinomial and ordinal.

- Naïve Bayes

It is a simple probabilistic classifier model, and it is a simple technique for constructing a classifier model that assigns class labels to vectors of feature values and problem instances. Based on the calculated overall probability, we can get the approximate value and detect

whether the news is fake or accurate [20].

- ❖  $P(A|B)=P(B|A) \cdot P(A)/P(B)$ , (1)
- ❖  $P(A)$  = PRIOR PROBABILITY
- ❖  $P(A|B)$  = POSTERIOR PROBABILITY FINDING PROBABILITY:
- ❖  $P(A|B_1)=P(A_1||B_1) \cdot P(A_2||B_1) \cdot P(A_3||B_1)$  (2)
- ❖  $P(A|B_2)=P(A_1||B_2)$  (3)
- ❖ If the probability is 0
- ❖  $P(\text{Word}) = \text{Word count} + 1 / (\text{total number of words} + \text{No. of unique words})$
- Long Short-Term Memory

To learn long-term dependencies, we can use an RNN-based particular type of LSTM. LSTM will provide the best solution for the vanishing gradient problem. LSTM cell is replaced by LSTM-RNN hidden layer [21]. It preserves the error that can be backpropagated based on time and lower layer. The input will be in both directions simultaneously in bi-directional LSTM.

- Support Vector Machine

It will provide an accurate classification of linear data. If the given data is in non-linear form, we can use the data with the help of the kernel trick, and we can avoid complex transformations into a linear model. This algorithm will develop a hyperplane. The hyperplane in N-dimension space is dependent on the dimension of input fed during the training period of the model. The hyperplane will provide a boundary line between different groups [22]. The line will also help us point the maximum distance from the data points of each group and categorize the new input [23].

#### 4.1. Training & testing model

The data must go for training once the network builds for each algorithm.

We trained the algorithm to learn features from the dataset. Later, testing is performed to evaluate the performance of our built model using performance metrics, accuracy, precision score and recall. Below we have mentioned confusion matrix for the various machine learning algorithms.

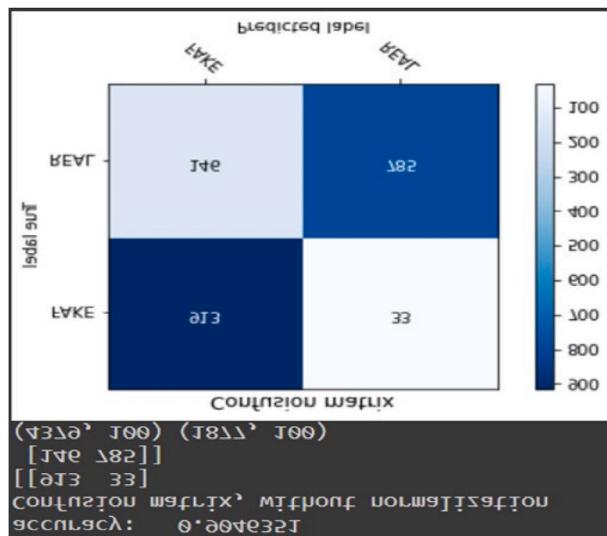


Fig. 11. Confusion matrix of logistic regression.

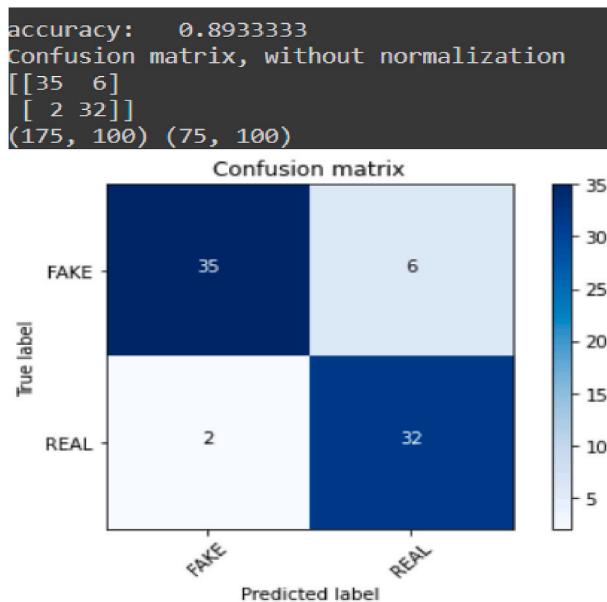


Fig. 12. Confusion matrix of SVM

## 5. Results

The dataset was extracted from Twitter and got the results. The reviews can be divided into two-part, one is reliable, and another is unreliable based on the text information. We used real-time tweets using some keywords to pre-process the tweets that we extracted from the dataset. Logistic regression is the first algorithm we used to perform the dataset. This one is the baseline model for machine learning and big data. This model is less prone to overfitting. This method will provide 95.2 %, as we expected.

Naïve Bayes is the following algorithm that we used to experiment with the dataset (see Fig. 10). Here we considered each variable independently, and its performance was better than expected. Unfortunately, due to zero frequency, the classifier achieved only 73.0 %. Fig. 11 is the description of our ROC curve for this model [24] (see Fig. 12).

Natural networks always have an issue with large datasets and storage. We used Long and, Short-Term Memory to overcome this problem to avoid this error. It uses memory blocks and gates for its

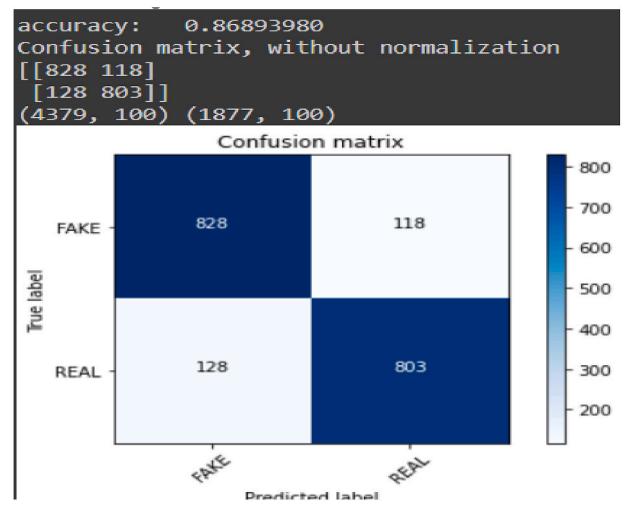


Fig. 13. Confusion matrix of Naive Bayes.

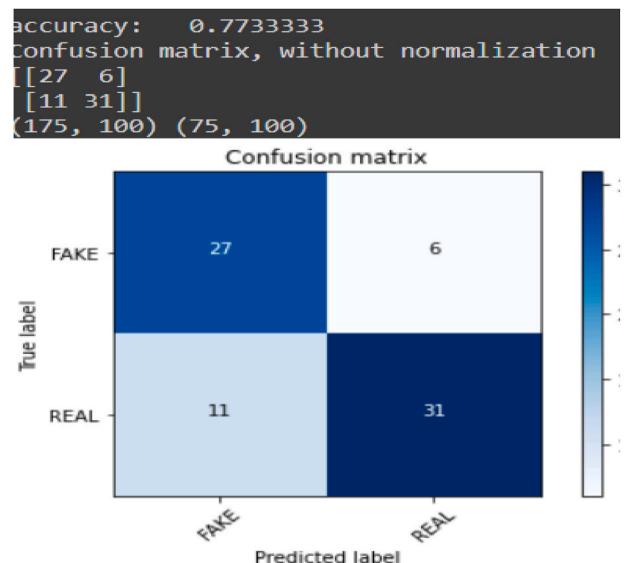


Fig. 14. Confusion matrix of decision tree.

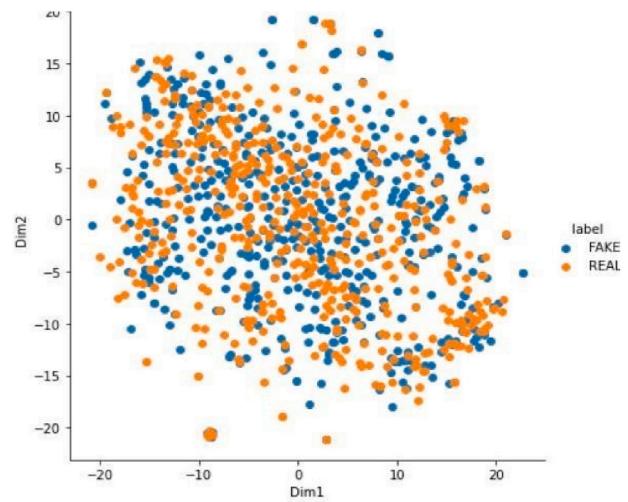


Fig. 15. Perplexity of a given dataset.

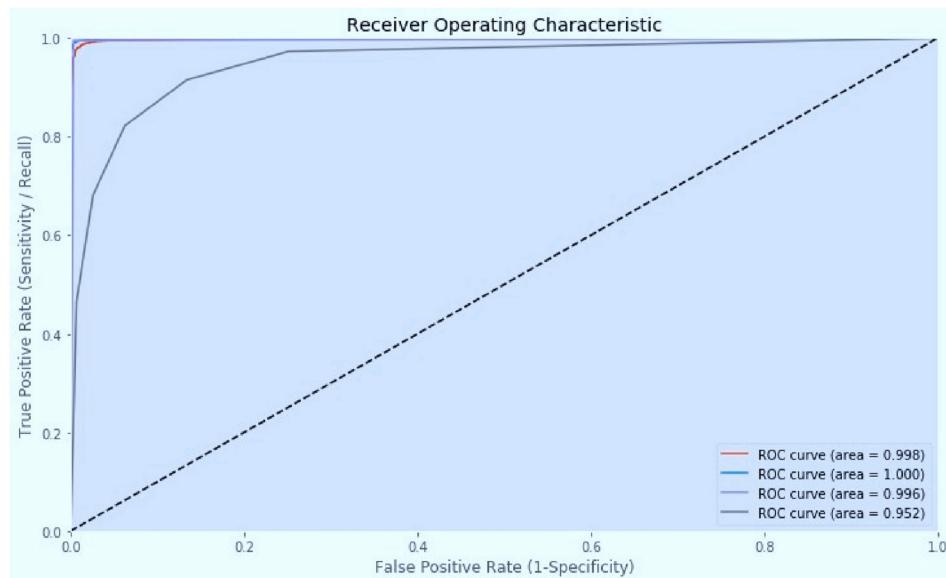


Fig. 16. Logistic Regression ROC curve.

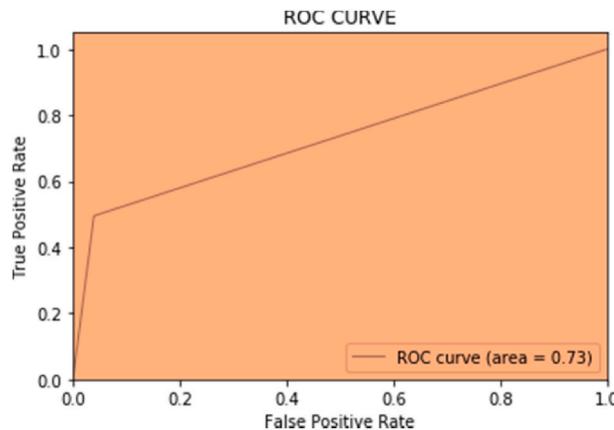


Fig. 17. Naïve Bayes ROC curve.

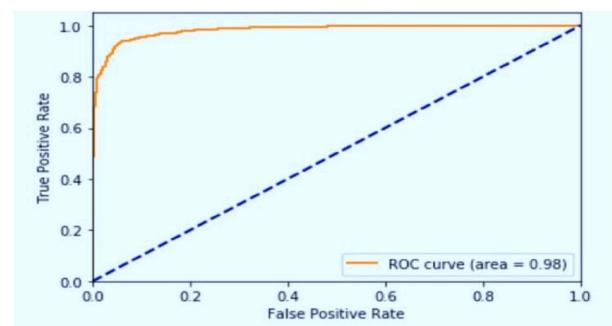


Fig. 19. ROC curve for support vector machine.

The latest algorithm which was performed on tweets to detect fake news was the Support Vector Machine. It uses deciding boundaries to separate two classes with the most considerable margin, also called the best hyperplane. Linear, SVM method was used to analyze the data extracted. SVM achieved a staggering 98 % accuracy which is the second-best accuracy achieved after logistic regression. Based on considerable research, SVM works wonders with linear and non-linear data and is more reliable in giving higher accuracy results. Below Fig. 13 depicts one of the best ROC curves in our analysis (see Fig. 14–19).

## 6. Conclusion

An online social network is widespread online news for various purposes. This will create more problems in the world affect the country's economy, change the political effects everywhere, and create panic among the people in the nation. To detect and avoid this type of fake news, we need a robust algorithm. The models there have manually labelled each tweet as real or fake news. This method will take a long time to predict whether the information is fake or real. We solved this problem; we collected the actual tweets and then applied the pre-processing of the data we collected. We used four machine learning algorithms to detect whether the news is fake or real. As a result, two algorithms provided a better solution for it. Logistic regression provided 95 % accuracy, and SVM provided 98 %. Many social media companies fight against fake news.

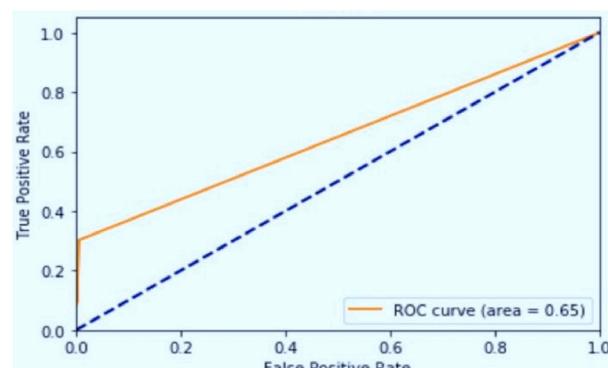


Fig. 18. ROC curve for long short-term memory.

functionality. Early Stopping was also used to restrict the model from overfitting. After running for five epochs, we got an accuracy of 65.0 %, the lowest among all our classifiers. This indicated that this type of data doesn't need neural networks and should be trained using a less complicated structure. Following is the figure that depicts the ROC curve of our LSTM model.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

No data was used for the research described in the article.

## References

- [1] R. Anandan, T. Nalini, Shwetambari Chiwhane, M. Shanmuganathan, P. Radhakrishnan, COVID-19 outbreak data analysis and prediction, Measurement: Sensors 25 (2023) 100585, <https://doi.org/10.1016/j.measen.2022.100585>. ISSN 2665-9174.
- [2] M. Cinelli, et al., The COVID-19 social media infodemic, Sci. Rep. 10 (1) (2020) 1–10, <https://doi.org/10.1038/s41598-020-73510-5>.
- [3] O.D. Apuke, B. Omar, Fake news and COVID-19: modelling the predictors of fake news sharing among social media users, Telematics Inf. 56 (2021) 101475, <https://doi.org/10.1016/j.tele.2020.101475>.
- [4] S. Daniya Sakkeena, S. Murugavalli, L. JabaSheela, V. Anitha, Ceaseless steganographic approaches in machine learning, Measurement: Sensors, Volume25 (2023) 100622, <https://doi.org/10.1016/j.measen.2022.100622>. ISSN2665-9174.
- [5] M.Z. Asghar, et al., Exploring deep neural networks for rumor detection, J. Ambient Intell. Hum. Comput. 12 (2021) 4315–4333, <https://doi.org/10.1007/s12652-019-01527-4>.
- [6] X. Sun, et al., Rumour detection technology based on the BiGRU\_capsule network, Appl. Intell. (2022) 1–17, <https://doi.org/10.1007/s10489-022-04138-3>.
- [7] T. Vo, An integrated topic modelling and graph neural network for improving cross-lingual text classification, Transactions on Asian and Low-Resource Language Information Processing (2022), <https://doi.org/10.1145/3530260>.
- [8] M.R. Kanfoud, A. Bouramoul, SentiCode: a new paradigm for one-time training and global prediction in multilingual sentiment analysis, J. Intell. Inf. Syst. 59 (2) (2022) 501–522, <https://doi.org/10.1007/s10844-022-00714-8>.
- [9] D. Zhang, et al., Fake news detection based on statement conflict, J. Intell. Inf. Syst. 59 (1) (2022) 173–192, <https://doi.org/10.1007/s10844-021-00678-1>.
- [10] M.I. Nadeem, S.A.H. Mohsan, K. Ahmed, D. Li, Z. Zheng, M. Shafiq, F.K. Karim, S. M. Mostafa, HyproBert: a fake news detection model based on deep hypercontext, Symmetry 15 (2023) 296, <https://doi.org/10.3390/sym15020296>.
- [11] M. Aldwairi, A. Alwahedi, Detecting fake news in social media networks, Procedia Comput. Sci. 141 (2018) 215–222.
- [12] S. Murugesan, K. Pachamuthu, Fake news detection in the medical field using machine learning techniques, International Journal of Safety and Security Engineering 12 (6) (2022) 723–727, <https://doi.org/10.18280/ijssse.120608>.
- [13] A. Kesarwani, S.S. Chauhan, A.R. Nair, G. Verma, Supervised machine learning algorithms for fake news detection, in: Advances in Communication and Computational Technology, Springer, Singapore, 2021, pp. 767–778.
- [14] Help.twitter.com, About verified accounts [online] Available at: <https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts>, , 2020.
- [15] Samiya Shakil, Deepak Arora, Taskeen Zaidi, Feature identification and classification of hand based biometrics through ensemble learning approach, Measurement: Sensors 25 (2023) 100593, <https://doi.org/10.1016/j.measen.2022.100593>. ISSN 2665-9174.
- [16] S. Murugesan, K.P. Kaliyamurthie, A machine learning framework for automatic fake news detection in Indian Tamil news channels, Ingénierie Des. Systèmes Inf. 28 (1) (2023) 205–209, <https://doi.org/10.18280/isi.280123>.
- [17] Google Trends, Google trends [online] Available at: <https://trends.google.com/trends/?geo=US>, 2020. (Accessed 1 April 2020).
- [18] Better Harder, Stronger Faster, The zero frequency problem (Part I) [online] Available at: <https://hbfs.wordpress.com/2014/09/23/the-zero-frenquency-problem-part-i/>, 2020.
- [19] M. Sudhakar, K.P. Kaliyamurthie, Effective prediction of fake news using two machine learning algorithms, Measurement: Sensors 24 (2022) 100495, <https://doi.org/10.1016/j.measen.2022.100495>. ISSN 2665-9174.
- [20] H. Rashkin, E. Choi, J.Y. Jang, S. Volkova, Y. Choi, Truth of varying shades: analyzing language in fake news and political fact-checking, in: EMNLP 2017 - Conf. Empir. Methods Nat. Lang. Process., 2017, pp. 2931–2937.
- [21] M. Sudhakar, K.P. Kaliyamurthie, Effective prediction of fake news using a learning vector quantization with hamming distance measure, Measurement: Sensors 25 (2023) 100601, <https://doi.org/10.1016/j.measen.2022.100601>. ISSN 2665-9174.
- [22] O. Aborisade, M. Anwar, Classification for authorship of tweets by comparing logistic regression and naive Bayes classifiers, in: 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, 2018, pp. 269–276.
- [23] T. Chauhan, H. Palvela, Optimization and improvement of fake news detection using deep learning approaches for societal benefit, International Journal of Information Management Data Insights 1 (2) (2021) 100051, <https://doi.org/10.1016/j.jjimei.2021.100051>.
- [24] Joshkelliott, One Hantavirus Death in China Sparks 'hysteria' over Old Disease, Retrieved from, 2020, March 24, <https://globalnews.ca/news/6724399/hantavirus-us-china-death-coronavirus/>.