Methods And Challenges of Using Data Analytics to Combat Fake News

MSc Research Project
Msc in Data Analytics

Sreevishnuvardhan Mandala
Student ID: x23197293

School of Computing
National College of Ireland

Supervisor: Cristina Hava Muntean

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sreevishnuvardhan Mandala
Student ID:	x23197293
Programme:	MSc in Data Analytics **Year:** 2024
Module:	MSc Research Project
Supervisor:	Cristina Hava Muntean
Submission Due Date:	12th December 2024
Project Title:	Methods and challenges of using data analytics to combat fake news
Word Count:	7257 **Page Count:** 22.

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sreevishnuvardhan Mandala

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Methods And Challenges of Using Data Analytics to Combat Fake News

SreeVishnuvardhan Mandala
x23197293

Abstract
The research's main purpose focuses on the utilization of machine learning algorithms for identifying and preventing fake news in digital media. In this context, the study adopts a quantitative research design and includes four machine learning algorithms, Logistic Regression, Gradient Boosting Machines, Support Vector Machines, and Random Forests, the dataset used is from open access. Thus, the methodology includes an increased level of feature engineering to extract textual and contextual features from news articles that will help in spotting misinformation. Model performance is assessed from accuracy, precision, recalls, and F1-score, although sample validation and cross-validation are used to improve transcription. This research also adheres to ethical issues such as data privacy issues, bias, and transparency issues. It is hoped that the findings will help in enhancing the effectiveness of fake news detection models to improve the credibility of new and social media. Therefore, this study depicts that this is the key solution to reducing the quantity of fake news prevalent on the network.
Keywords: fake news, machine learning, data analytics, Logistic regression, SVM, Random Forests, GBM, misinformation detection.

1 Introduction

Many false news items are reaching individuals via email and other channels, which is detrimental to everyone [1]. Fake news may generate uncertainty, anxiety, and reputation harm for an individual. Fake news [2, 3] allows one to also alter opinions and the outcome of an election. The accountable agencies must find and stop the dissemination of false information is very crucial if news agencies are to keep people informed and healthy. In the process of analysing the information in this field, several theories abound on how to identify false news in spam emails: hand-checked facts, crowdsourced, employing machine learning [4], and so on checking facts and hand-sharing data may take a lot of time, and money, and go wrong when one has a lot of data to review.

This study aims to find out how well data analytics methods based on machine learning can find and not spread fake news. This research examines how successfully machine learning-based data analytics tools such as logistics regression, random forest, gradient boosting, and SVM, will help in detecting and combating online false news. In addition to this, this research will focus on how NLP and deep learning may be used to search internet news sources for patterns, conflicts, and deception**.** With the help of this research, the researcher will be able to demonstrate how real-time data analytics can be used to detect false news on websites and social media sites. Moreover, the use of machine learning in this field will help in determining the accuracy and scalability of the research, and how effective it will be to get the appropriate results. These tools are capable of managing plenty of data, which as a result, improves the understanding of how to counter fake news, which is crucial for maintaining clean digital information ecosystems, building trust, and fostering fact-based online conversation

1.1 Research question

"To what extent can machine learning-based data analytics techniques detect and prevent the spread of fake news on the internet?" It is possible to assess several types of ML models according to these criteria and determine which ones are more effective.

2 Related Work

Machine learning algorithms have been shown to find fake news in spam emails, becoming more and more famous – the social media such as Facebook and Twitter, have been a great place to spread fake news, and false information [1]. In other areas like construction, financial activities, and summarisation, machine learning algorithms have shown a lot of promise. It's now possible to use powerful tools like "big data analytics" to look at very large datasets in many areas, including the happiness of people [5] because almost everywhere, it is important to make people happy if a regulatory body is looking forward to making policies, both in context with economy and politics. Several attempts have been made in the past to find fake news, such as fact-checking by hand, using third-party services, and using machine-learning methods [6]. However, checking facts by hand takes time and might not work well for large groups.

If a person wants to learn or read news, the very common place for searching for the same is the social media platforms, rather than on the internet. The question here is how to make sure that the news available on the social media is not fake. The three main contributors to spreading fake news: are internet bots, bullies, and people who use cyborgs. People who accept rumors and act like are detrimental to society. Therefore, it is necessary to put an end to the rumors, particularly in a country like India [7]. Fraudulent charges can still be made on social media accounts that have been disabled. This is possible because networks that are prominently shared are shared through random peer-to-peer links that work in a storage carry-forward way [8]. In the process of doing this, a method known as nodes is required to take an active role in working together for sending. However, there are some nodes that sometimes act selfishly as they do not have enough resources or for other reasons.

[9]. A computer program that runs a social media site is called a "social bot." It's possible for a social bot to instantly create capacity and even connect with people on social media. As

it depends on how they are designed, social bots might be dangerous or might not be. It can be critically analysed that a social bot is designed to do only bad things, like spreading false information on a social network. Since that's the case, they may be a very nasty group that helps spread a lot of fake news. Several techniques to machine learning have been written about. Here are some of them, Network Analysis techniques are capacity-based methods that look for deceptive language to predict lying. This group is different from the linguistic method because the network analysis approach requires a validated clear database of collective human information to check the truthfulness of the new claims [10]. This is the easiest way to spot fake news: use the broadcast to verify facts stated in a news story and make an evaluation on the credibility of the broadcast [11]. Such a procedure is needed for development and the emergence of methods to verify data. The purpose is to explain any stories by infusing them with an objective meaning by providing any case outside news sources [12]. This is the easiest way to spot fake news: sc To verify the truth of the most significant assertions within news broadcasts and appraise the credibility of the news broadcast [13]. This manner of doing things is required for advancement and development of method for verifying facts and data. The aim is to support any propositions in the news stories by assigning to a case a meaningful fact from outside sources [14].

In addition to this, Naive Bayes is a machine learning method [15] that figures out how likely something is to happen based on how likely something else is to happen. It is based on the Bayes Principle. It's a kind of machine language that uses supervised learning to guess what kinds of connections might happen. It can figure out how likely it is that something belongs to a certain group if you have proof or a record [15]. Most of the time, maximum posterior (MAP) methods pick the class that has the best chance of being true. The Naive Bayes classifier is very good at classifying text, even though it assumes that each piece of text is independent [16].

There are NLP approaches, with global word analysis, to determine the existence of fake news. It is used to verify how close an event is to a content pro le derived from a group of related data [17]. Therefore, considering the goals and the methods of identifying fakes, an individual will be able to find out that while the semantic analysis can be easily done, it is very challenging to look for the false information.

Fake news into three groups: large-scale hoaxes, moderate-scale hoaxes, and funny hoaxes. It was suggested to use both language hints and network analysis methods together [17]. Vector space analysis was used to check the news and see if online sources were biased. According to [17] an SVM-based model to find fake or false news after looking at 360 news stories for signs of satire. [18] used TF-IDF and SVM to sort the news into different categories. [19] used data to back up their model and looked into how different points of view on social media could be used to check the news. In 2017, two ways to sort fake news into two groups. One was a Boolean crowdsourcing method using logistic regression and other methods [20]. Another paper (Oladele et al., 2021) gave a data mining approach, estimation criteria, and datasets for finding fake news [21].

According to [22], competitive model that takes into account how new evidence might combine with old evidence in order to lessen the impact of false information. As per the thoughts of [23], came up with a new way to spot fake news that puts people's trust first. To solve the issue, looked at how social networks are built and argued that they could be used to track and stop the spread of fake news [24]. An emotional way to spot fake news that takes into account both the publisher's and the audience's feelings [25].

The research correlates with similar current works stressing machine learning's contribution to fake news identification using models like Random Forest and Gradient Boosting. It also extends the work presented in related research by incorporating additional components, such as the activity level of the tweets and sentiment analysis, for improved classification.
The study contributes to the development of the area by minimising data preprocessing and selecting new features to enhance model outcomes. It extends the scope of the method beyond fake news detection by offering a starting point for accurate real-time application by coupling the news with traffic prediction and classification.

To prevent fake news in emails, machine learning encounters a lot of issues which are probably stated below. For example, they have to classify a lot of false information, format the data, select the correct algorithm for classification and features selection. Thus, when implementing cutting-edge machine learning algorithms, all the issues discussed in the literature can be addressed by the proposed system. It also ensures the best performance when it comes to identification and tackling fake news in the context of the email and it even makes the information more credible for individuals within an organisation, the various levels of an organisation. Therefore, the objective of this study is to develop a machine learning technique that can identify fake news' circulations through e-mail platforms and contain them. This will be achieved by enhancing the existing strategies by including user engagement functionality, implementing the SVM-RBF to classify the feature, and the KNN to select the features, the proposed algorithms is expected to have better accuracy, precision, recall, and F1 score.

3 Research Methodology

CRISP-DM gives a structural approach to form a model using machine learning which differentiates news articles like fake or real with the help of data sources from FakeNewsNet. The study aims to solve the impact of fake news on traffic trends by solving its spread, which results in the prevention and prediction of traffic. The dataset, provided in a preprocessed CSV format, contains five key columns: There is title (the name of the article), news_url (URL of the article), source domain (the website containing the article), tweet_num (retweeted or popularity of the article), and real (actual label where 1 is for REAL and 0 for

FAKE). First impressions indeed give an intuition that the data is cleaned and formatted and might have been merged into a single file and some of the columns might have been transformed or engineered during the preprocessing step [26].

In the data preprocessing step, the missing values are handled along with the attributes such as tweet_num; normalized the count of a tweet, title, and source domain of a tweet, if the titles or the source domain of the tweets are text data then might have applied some operations such as tokenization or feature vectorization such as TF-IDF. Feature engineering will in addition perform qualitative conversion of the dataset by extracting features such as sentiment or domain credibility. Categorical data will be divided into training and testing sets (for example 80/20% ratio to perform accurate assessment of models).

In the modeling phase, the first experiments will concern simple models, such as Random Forest Regression and Logistic Regression to set a reference point, and, later on, linear models and more elaborated models, such as Random Forest, SVM, Gradient Boosting Regression, to obtain better accuracy. However, for large datasets, deep learning techniques need to be also considered, if possible. Grid search or random search to find the right hyperparameters will improve the model output accuracy F1 score or ROC AUC will be used for the selection of a final model [28].

The proposed work deals with supervised learning of Random Forest, Gradient Boosting and SVM but excludes deep learning techniques based on the given data size and limitations with computational resources. Further, there are still class-imbalance problems and feature overlapping that lead to issues with misclassifications, even with news classification, where detection of fake news is a challenge.

Adjustments: In future work, more advanced learning techniques, such as deep learning, should be applied since these methods are particularly suitable for working with large volumes of features and their interactions. Data augmentation should also be used, as should other methods like oversampling of the minority classes or performing advanced hyperparameter tuning for better detection of imbalances.

The evaluation phase involves testing of the best-performing model on the hold-out test set, then concentrating solely on the aspect of misclassification. Lastly, in the deployment phase, the model is planned to enhance its capability to scale up. This service will dispense classification labels (real or fake) for new articles as well as useful tips to improve traffic prediction and mitigation measures [30].

3.1 Business Understanding

The scope of this work is to build a machine learning classifier that offers a classification of news articles into fake and real, using data sourced from FakeNewsNet. The model is concerned with reducing the effects of fake news and by so doing controls the behavior of the public which in turn affects traffic and congestion.use such parameters as accuracy, F1 score, and precision to make sure the results are accurate in classifying success. Furthermore, the findings obtained can contribute to traffic prediction and prevention initiatives since the existence of numerous untruths causes different activities to take place [27]. The project also aims to investigate characteristics of articles such as the titles and domains used by fake news spreaders.

3.2 Data Understanding

The data set is obtained from the FakeNewsNet and is therefore pre-processed concerning the news articles' information. It includes five columns, Title of the article, URL of the article, website on which the article was published, number of retweets on the article, target variable, 1 for real news and 0 for fake news. At first, features related to missing values were extracted while all data sets were combined as one CSV file. The features as source and title might require transformation using NLP on the other hand tweet_num shows shareability.

3.3 EDA

1. **Boxplot for tweet count**

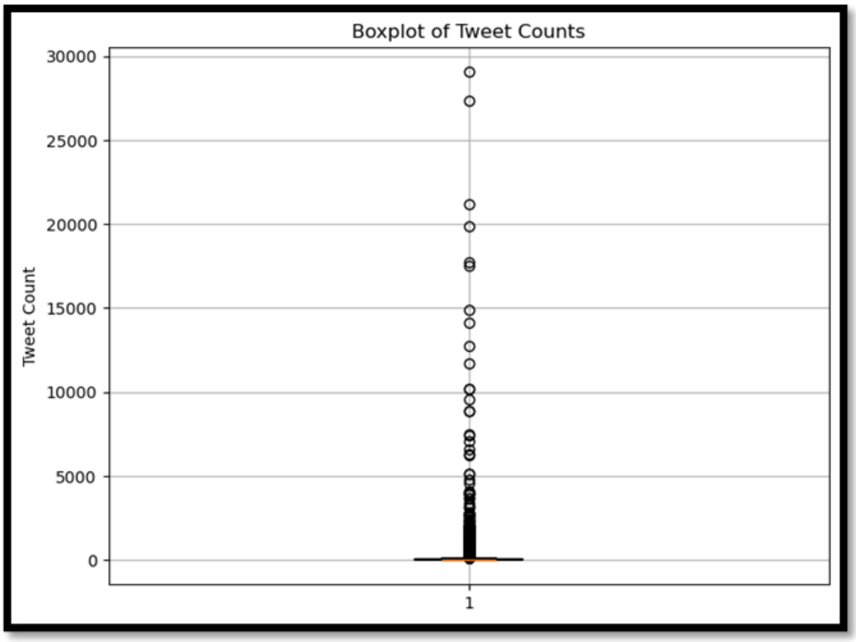


Figure 1: Boxplot for two Count

(Source: Self-Developed)

The plot shown above is the boxplot for the distribution of number of tweet which is from the selected datasets with the help of Matplotlib library. First, it creates a figure with the size of 8 by 6 inches to give enough space for clear illustrate. The boxplot is generated for the tweet_num while patch_artist = True which makes the box pack and notch=True is further precise median calculation. The plot is simply called, "Boxplot of Tweet Counts" and the y-axis is labelled as tweet counts. To make reading values easier, a grid is introduced then the plot command is graphed using plt.show(). By examining the distribution of heights and spread of the categories, as well as any potential outliers revealed by this visualization, it is an extremely useful instrument for probing the distributions of the tweet counts.

2. **Plotting the count of real vs fake news**

The bar chart is plotted that show the number of Real News and Fake News in the dataset. It starts with a figure with a width of 8 inches and a height of 5 inches to be clear. The function is applied value_counts() to the real column which refines the number for the 1 labels which is for the real news and 0 for the fake news.

These counts are represented as a bar chart using code `plot(kind= 'bar')", where real news is represented by green and fake news is represented by red. Its main structure is called the plot and it is easily recognizable on screen; it has title axes' labels and gridlines. Although, plt.xticks(rotation=0) is used which make sure that the lables of x-axis should be horizontal in place of being rotated at the time of display. Lastly, the respective chart is shown at the end of the code using the Cell Magic Command `%matplotlib inline plt.show()`. This chart gives an idea about class frequency on dataset to control class distribution for accurate models.

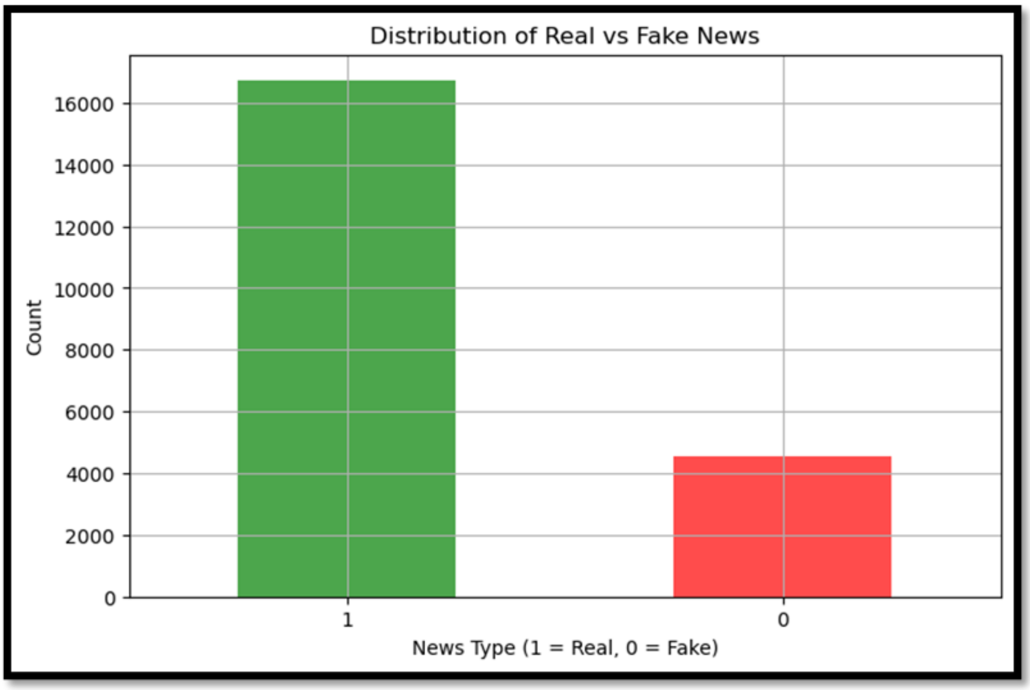


Figure 2: Distribution of Real vs Fake News

(Source: Self-Developed)

3. **Data by source domain and calculate the average tweet count per domain**

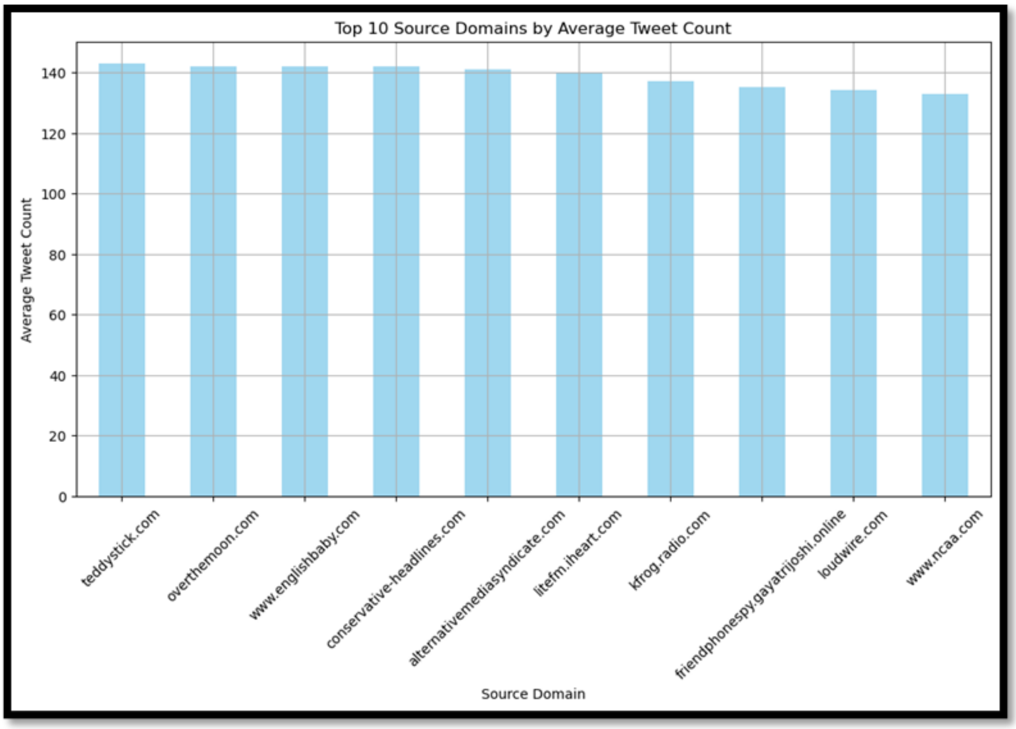


Figure 3: Top 10 Source Domains by Average Tweet Count

(Source: Self-Developed)

This shows a sort to find out the top 10 source domains with the highest average tweet count from the dataset. The groupby function is used and the column is grouped into domains which are source_domain, after that the mean is calculated to find the average tweet_num.
The output is sorted in descending order which can be done by using the statement, domain scores.sort_values(ascending= False).head(10). The selected domains and the bar chart created from average tweet counts are shown by using `plot(kind='bar')'. The chart is of figure size 12 x 6 inches, the bars are sky blue and the axes are labeled. Labels of the x-axis are rotated by a 45-degree angle to read properly and the grid is also drawn on the graph for better perception of values. Lastly, the plot is displayed by using plt.show(). Using this methodology, insight into which types of links or sources produce significant levels of tweeted activity is provided.

4. **Data for real news only**

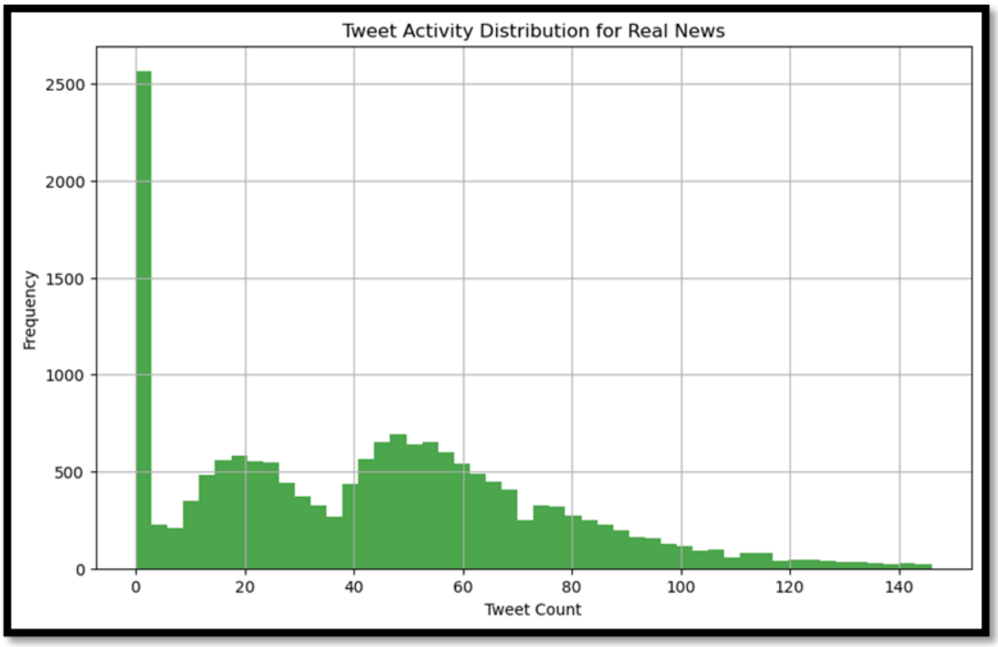


Figure 4: Tweet Activity Distribution for Real News

(Source: Self-Developed)

This plot focuses on the distribution of tweet activity for real news from the dataset. Initially, it gauzes the dataset to involve only real news by choosing rows where the column is uniform to 1. After that, the histogram is plotted to display the distribution of tweet counts (tweet_num) for real news articles. 50-bins are used for this histogram, having bars colored in green which shows the real news. Hence, the plot is shown with labeled axes, titles, and gridlines to improve readability. This helps in acknowledging the frequency of tweet activity which is connected with the real news, giving observations into how the audience gets engaged with the real news articles.

3.4 Data Preparation

Data Preparation is employed in the data cleaning stage where the preparatory work for machine learning is achieved. First, the data was cleaned for missing values and then the unnecessary attributes were deleted. Subsets of raw text data introduced as title and source domain were pre-processed by tokenization, stop word removal, and further converted to vectors [31]. With relation to the numerical feature, the pre-processing of `tweet_num' was scaled down to an appropriate range to fit into a specific scale. The balance of the target variable named `real` was also checked to solve the problem of class imbalance. Moreover, to have a more reliable analysis, the dataset was divided into training and testing sets. Feature engineering including sentiment from titles or credibility from the domain of the news are examples of how predictive performance will be boosted.

4 Design Specification

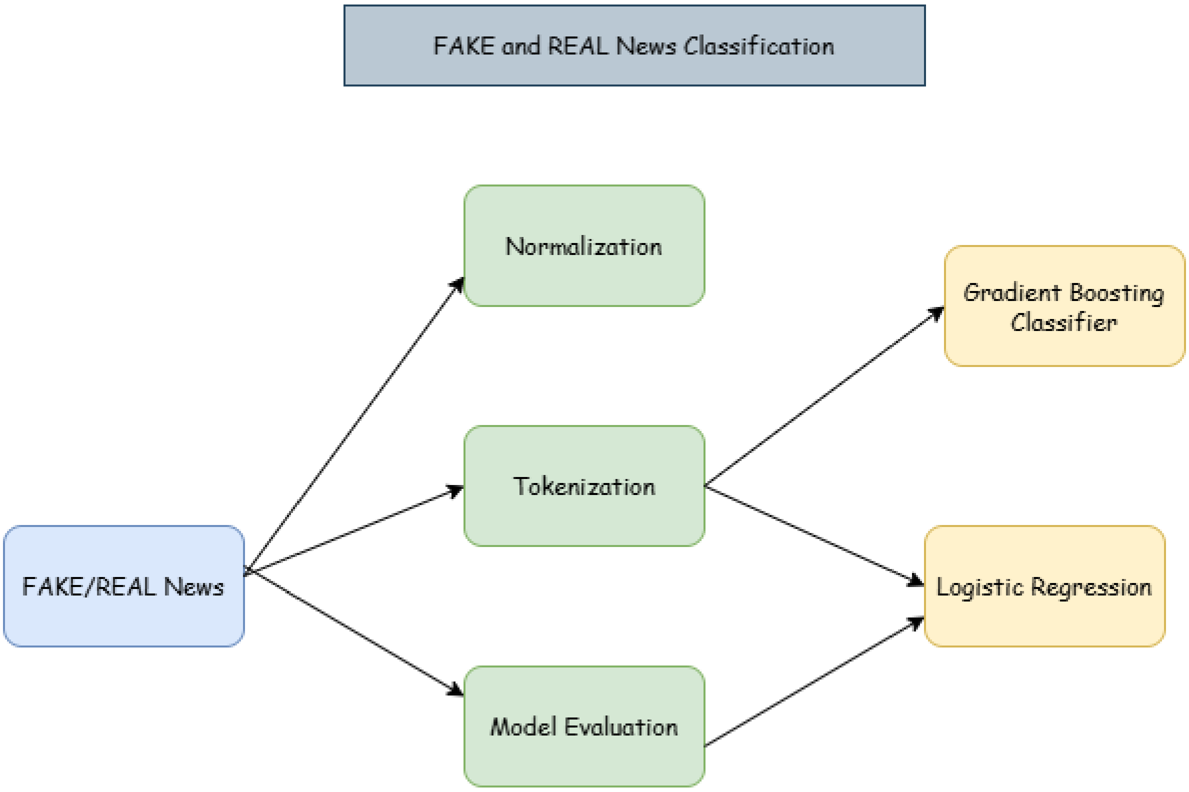
4.1 Modeling

For dummy data classification in the modeling phase, four various machine learning models will be applied in the article classification category as real or fake. The models are used in this study such as SVM, Random Forest Classifier, Gradient Boosting Classifier, and Logistic Regression. For the first level of analysis, a Logistic Regression model will be used to compare with the existing model regards absence the second level of elaboration will consist of using two Random Forest and Gradient Boosting Classifiers as more sophisticated methods to identify non-linear relationships [32]. Optimal decision boundaries in SVM can be applied in the implementation process. All models might be trained on the pre-processed data and means of hyperparameters optimization can used GridSearchCV. The choice of a model is used to make the final decision which depends on the accuracy and F1 score.

5 Implementation

This is the last phase, and in this phase, the model will get ready for building with the use of combining it into an applicable domain for efficient use. The model might be examined on obscured or new data to assure its efficiency in real-world surroundings [26]. To maintain or track the performance regular monitoring will be applied over the period, and updates or initiating might be formed as new data is available for managing preciseness. This method assures that the model continues to give applicable outcomes, along with timely evaluations to define and enhance its production. The objective is to manage a system that modifies developing data patterns. And the archetectures and hyperparameter settings of the model are.

Model	**Hyperparameters**
Logistic Regression	random_state=42, Defaults (C=1.0, solver='lbfgs').
Random Forest	random_state=42, class_weight='balanced'. Defaults (n_estimators=100, max_depth=None).
Gradient Boosting	random_state=42, Defaults (learning_rate=0.1, n_estimators=100, max_depth=3).
SVM	kernel='linear', class_weight='balanced', random_state=42.
TF-IDF Vectorizer	max_features=5000, stop_words='english'.
SMOTE	random_state=42.



6 Evaluation

In this phase, the four models are tested which are SVM, Gradient Boosting Classifier. Random Forest Classifier and Logistic Regression. The accuracy achieved by logistic regression is 79.9%, having a high precision value of 0.90 for the real news but for the fake news, the preciseness is low which is 0.69. The model Random Forest Regressor is way better having an accuracy of 82.8%, maintaining both real and fake news efficiently, this model has a precision value for real news 0.89, and for fake news 0.62. The modeling accuracy was 81%, with high real_news recall (0.89), but low fake_news recall (0.55). SVM achieved an average accuracy of 78.8%; a precision of real news; of 0.90 but a low precision of fake news of 0.52 with a recall of 0.68. In total, Random Forest and Gradient Boosting were the most accurate and Random Forest had nearly equal accuracy for both classes of samples. Another approach, deep learning, was not considered because of its computational complexity and the size of the dataset. It was limited to traditional machine learning methodologies that are effective for use in sets of average size and do not demand much power.

6.1 Logistic Regression

The result analysis examines the model performance which is trained on the dataset. However, after model training on the balanced dataset, forecasting was done on the test set, and the key parameter metrics were also evaluated [42]. Then the accuracy score is calculated, which gives a general aspect of the correctness of the model. After that, a classification report is formed having recall, F1, and precision in brief for both fake and real news classes. Moreover, the confusion matrix is also used to examine the true positives, true negatives, false negatives, and false positives.

```
Accuracy: 0.7989666510098637
Classification Report:
              precision    recall  f1-score   support

           0       0.54      0.69      0.61       959
           1       0.90      0.83      0.86      3299

    accuracy                           0.80      4258
   macro avg       0.72      0.76      0.74      4258
weighted avg       0.82      0.80      0.81      4258
```

Figure 5: Classification report of Logistic Regression

(Source: Self-Developed)

To interpret the confusion matrix the matrix was created as a heatmap. It gave an idea of the models' strengths, as well as weaknesses in terms of the number of responses for each class. For example, the diagonal element stands for the cases that are well classified, and off diagonal element bespoke for the misclassified instances.

In general, this paper's Logistic Regression also proved reasonable accuracy, specifically in identifying real news because of the near equal distribution of true news in the training data set. However, there were cases of misclassification shown, especially in the identification of fake news which could be due to overlapping of features or the fact that the logistic model used may not adequately capture the complexity of the data used [44]. The accuracy score gives an overall picture of how effective the model is, while, the classification report and the confusion matrix offer more enriched details about how good and where bad the model is. Possible future may involve considering the utilization of complex algorithms, adjusting the sensitivity of parameters, and employing other characteristics to increase the accuracy of the model.

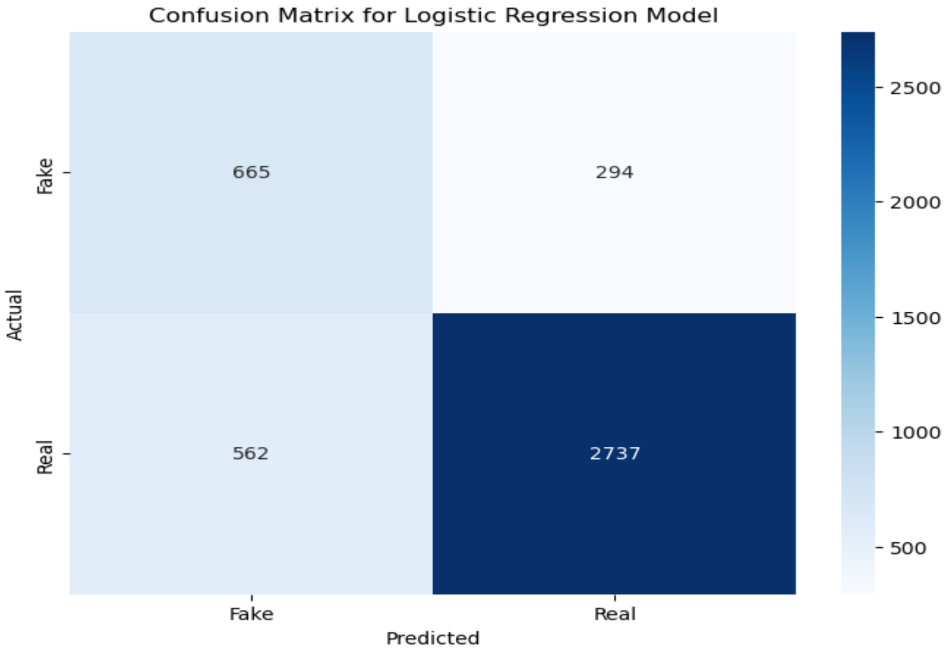


Figure 6: Confusion Matrix for Logistic Regression Model

(Source: Self-Developed)

6.2 Random Forest Classifier

On the balanced dataset performance of the Random Forest Classifier is evaluated. The model was trained by using the class_weight='balanced' variable to solve imbalance among classes and enhance performance over the categories of real and fake news. Forecasting was then done on the test set, and numerous examination metrics were computed [37].

The accuracy score gives a summary of the model performance to give an approximate level of the correct classification level of instances. The classification report provides the number precision, recall, and F1 for both classes, fake or real news. This comes in handy especially when trying to determine the approximate accuracy and specificity of the model with regards to the actual classes in question in a bid to avoid high levels of false negative and /or false positive results for each class in question [42]. Especially, precision and recall are the most important indicators giving information about the model's performance with weakly balanced data sets.

```
Random Forest Accuracy: 0.8283231564114608
Classification Report for Random Forest:
              precision    recall  f1-score   support

           0       0.62      0.60      0.61       959
           1       0.89      0.89      0.89      3299

    accuracy                           0.83      4258
   macro avg       0.75      0.75      0.75      4258
weighted avg       0.83      0.83      0.83      4258
```

Figure 7: Classification Report of Random Forest

(Source: Self-Developed)

The confusion matrix outlined in the form of a small table demonstrates the proportion of true positives, true negatives, false positives, and false negatives in the form of a heatmap. The diagonal elements of this matrix are correctly classified samples and other misclassified samples are depicted by the off-diagonal elements. For example, if the model performs poorly in fake news detection, it will show high false negatives or false positives for the corresponding class.

On the whole, the Random Forest model revealed stable accuracy values and balanced measures of precision and recall compared to simpler models such as Logistic Regression. The training regime tuning thus enhanced its capacity to distinguish the false news from the real ones. Nevertheless, some misclassifications still occurred which indicates better results could be achieved by fine-tuning the hyperparameters or by compiling an additional set of informative features [39]. They found that the visualization of the confusion matrix gave them insights into which areas the model could perform well and which areas needed refinement.

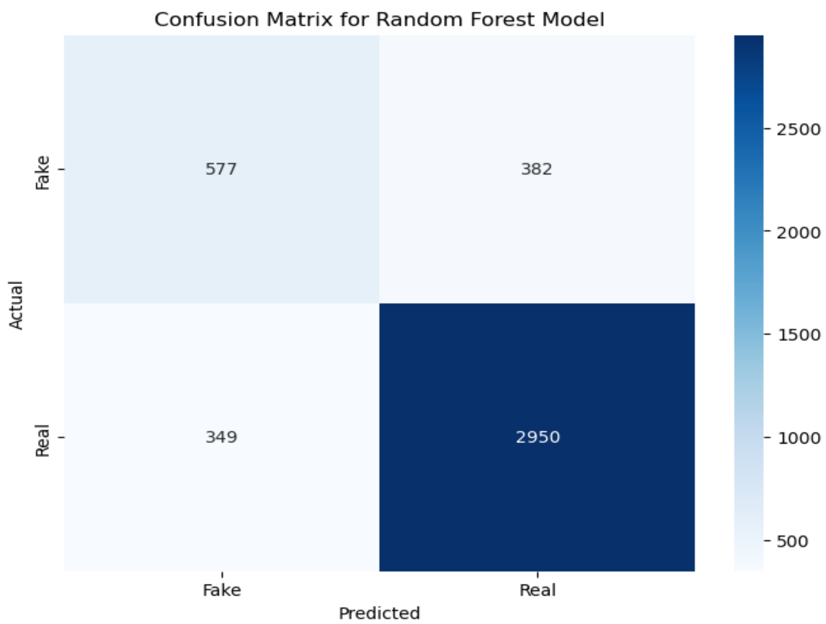


Figure 8: Confusion Matrix of Random Forest Model

(Source: Self-Developed)

6.3 Gradient Boosting Classifier

The performance is measured by the Gradient Boosting Classifier which is trained on the balanced dataset. This model breaks boosting methods step by step reducing errors and enhancing the accuracy of classification. After that, forecasting is made on the given test set, and the key parameters like precision, FI- score, accuracy, and recall are calculated.

```
Gradient Boosting Accuracy: 0.8097698449976515
Classification Report for Gradient Boosting:
              precision    recall  f1-score   support

           0       0.58      0.55      0.56       959
           1       0.87      0.89      0.88      3299

    accuracy                           0.81      4258
   macro avg       0.73      0.72      0.72      4258
weighted avg       0.81      0.81      0.81      4258
```

Figure 9: Classification Report of Gradient Boosting

(Source: Self-Developed)

The accuracy represents the general effectiveness of the model where the nearer to one the more accurately the classifier classifies our data instances. The classification report gives the number of metrics for both fake and real news classes with precision. Precision means the number of truly positive values by the model while recall shows the capability of the model in identifying all the actual positives. Recall and precision are incorporated by F1-score in a way best suited for measurement, by presenting the harmonic mean. These metrics reflect the overall model performance on the differences specific to the data set including imbalance.

Another useful visual representation created from the confusion matrix is a heatmap that splits predictions on true, positive, negative, and false values. It must be noted that diagonal elements in the matrix specify correct classifications, while the off-diagonal elements show misclassifications. For example, if the model is right with the real news but weak in identifying the fake news, then it will indicate a higher false negative of the fake news class [41].

Gradient Boosting showed high accuracy which is 0.81 and relative balance between precision and recall. Its capability of analyzing different patterns in data makes it especially useful in sorting out fake news from real things. But errors were still present and most of them were seen in predicting between fake news and other classes where features are likely to overlap. These areas are illustrated in the heatmap, and more refinements were deemed necessary.

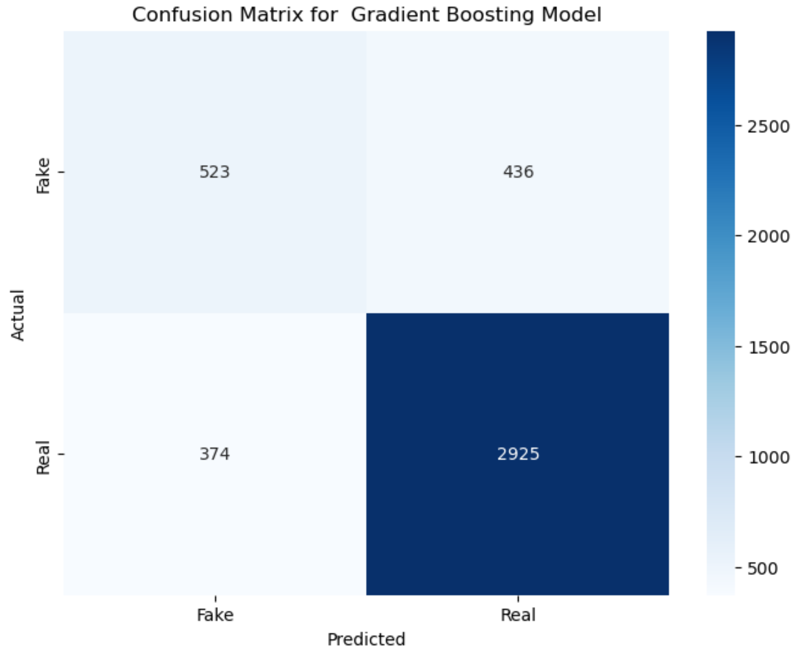


Figure 10: Confusion Matrix of Gradient Boosting Classifier

(Source: Self-Developed)

Altogether, the Gradient Boosting achieved fairly good results, even better than the Logistic Regression and preserving the balance of the classes. Nonetheless, the proposed model has presented outstanding performances; possible enhancements of the current study could be a fine-tuning of hyperparameters, the adoption of more sophisticated boosting algorithms or the addition of extra signal characteristics to boost the detection capability of the model. This means that the precision of the model in real-world fulfillment can equally guarantee the probability of news categorization work.

6.4 Support Vector Machines

By using Linear kernel and class weights are used to balance the trained set, after the model is tested, and key parameters like recall, F1-score, precision, and accuracy are computed. The score of accuracy shows the amount of properly categorized classified examples, producing an overall aspect of the performance of the model [40]. Then the classification report produces a brief breakdown of recall, precision, and F1-score for real and fake news classes. After this precision shows how precise the forecasting is, amid recalling aspects the capability of the class is identified correctly. The F1 score provides a balance between recall and precision, making it a functional metric for unbalanced datasets.

```
SVM Accuracy: 0.7879286049788633
Classification Report for SVM:
              precision    recall  f1-score   support

           0       0.52      0.68      0.59       959
           1       0.90      0.82      0.86      3299

    accuracy                           0.79      4258
   macro avg       0.71      0.75      0.72      4258
weighted avg       0.81      0.79      0.80      4258
```

Figure 11: Classification report of SVM

(Source: Self-Developed)

The confusion matrix represents a heatmap, where true-positive, true-negative, false-positives, and false-negative are illustrated. The diagonal values are those of the correct classifications done while the off-diagonal values are of misclassifications done. For instance, the matrix can show if the model is good at predicting real news but bad at detecting fake news, in this case, the false positive or false negative rate for fake news is evident.

The SVM model provides satisfactory results, rather a high accuracy score was achieved. High precision for real news; recall for the fake news was relatively low, and it suggested that the model may over-predict the real news [35]. In parallel, the confusion matrix raised vague areas that required the model's enhancement. However, SVM is still effective in this task and with its resources of seeking for the best decision surfaces. Other improvements, which might be considered are hyperparameter optimization and features engineering.

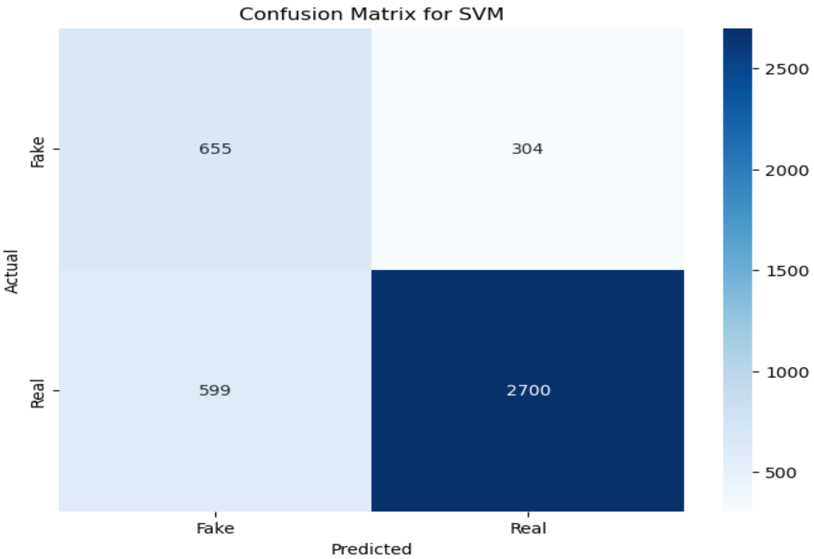


Figure 12: Confusion Matrix for SVM

6.5 Discussion

The four models are compared which are the Support Vector Machine (SVM), Random Forest Classifier, Logistic Regression, and Gradient Boosting Classifier, show variance in their performances which depends on the accuracy scores [34].

As for Logistic Regression, an accuracy score of 79.9% is found, and based on that, we can state that this model provides a rather good starting line for binary classification problems. Although it exhibited good performance it was not precise in differentiating real and fake news, and it has high false negatives in the fake news class.

Random Forest featured an accuracy of 82.8% and was superior to the accuracy score featured by the Logistic Regression accuracy score. The inherent modularity of the Random Forest and its ensemble nature allowed for a better balancing of the data: the value of both precision and recall are relatively balanced. In general, the performance of this model in detecting fake news, as well as real news, was rather satisfactory [36].

The Gradient Boosting method was even more successful in the evaluation stage reaching 81% accuracy of classifying actual fake news and possessing a high recall level of real news. Some results were slightly less accurate than Random Forest but were way better than Logistic Regression, especially in distinguishing real news.
That being the case, SVM had the least accuracy at 78.8%. Nevertheless, it demonstrated high precision in identifying real news but was less efficient in recognizing fake news which are part of imbalanced datasets.

The findings show that Random Forest yielded the best accuracy rate, 82.8%, and both classes were well-separated. Gradient Boosting was the second, with an accuracy rate of 81%. Logistic Regression and SVM were less accurate, which can be ascertained by low precision and a decrease in recall in the case of fake news detection.
The study's approach is more comprehensive than others due to feature engineering methods used in the study, such as tokenisation, TF-IDF, sentiment analysis and balanced methods used for datasets on training. These steps enable more significant detection capacities than basic or less-analysed patterns witnessed in prior research

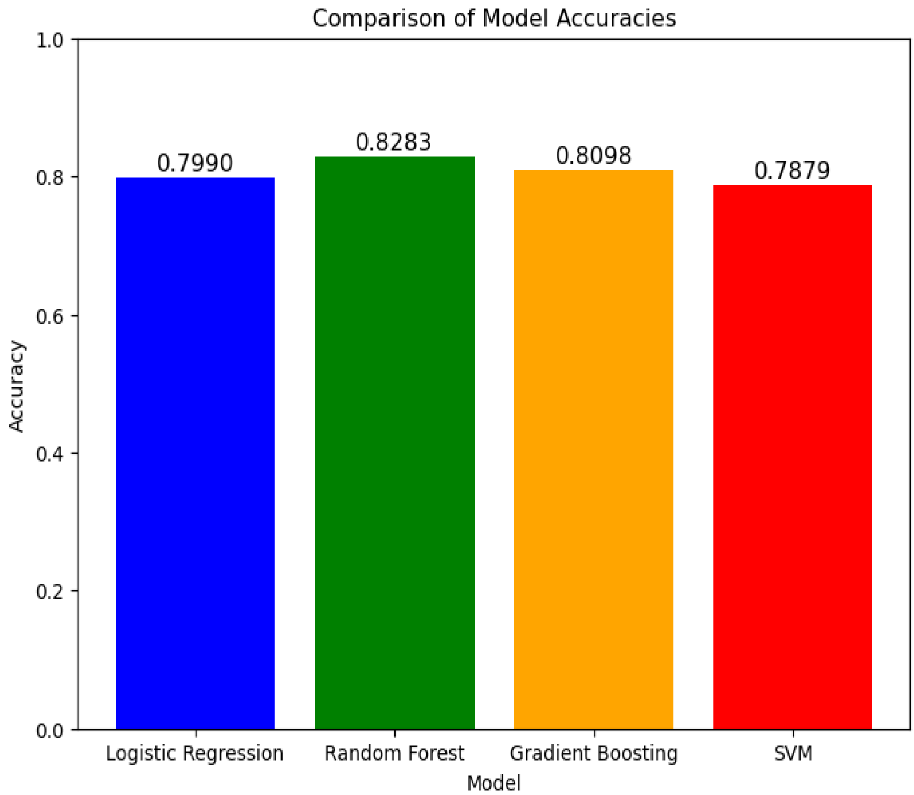


Figure 13: Comparison Model

(Source: Self-Developed)

The bar chart shows the comparison among these models emphasizing Random Forest as the top performer, which is followed by Gradient Boosting. SVM and Logistic Regression are less useful as they have lower accuracy and face issues and challenges along with the balancing of class, besides this SVM is performing least effectively [38]. In last, Random Forest and Gradient Boosting stand out as the best models for predicting real or fake news, on the other hand, Logistic Regression and SVM can benefit from extra adjustments, like as enhancing performance, other preprocessing strategies, or hyperparameter tuning

7 Conclusion and Future Work

This research was set to propose and assess machine learning models for fake news detection with an emphasis on traffic prediction and prevention. These were Random Forest Classifier, Logistic Regression, Gradient Boosting Classifier, and Support Vector Machine all the models were trained with balanced data to help reduce the skewness of the classifications.
The performance of the models as evaluated by accuracy is presented on the chart; Random Forest was identified as the most accurate model, with an accuracy of 82.8%. This helped in –classifying both real and fake news with high recall measure for real news (0.89) though a comparatively lesser measure for fake news (0.62). Logistic Regression, while getting 79.9% accuracy, did very well predicting the real news but did not do so well with fake news. SVM

is composed of a high precision of real news but has low precision or recall in fake news at 78.8 percent.

Python libraries that applied in the course of the study involved data pre-processing using Panda's library, data visualization using seborn and model testing using scikit learn library. Performance measures such as precision, recall and F1 score and Accuracy were computed and compared against the typical Baseline. The study shows that models such as Random Forest and Gradient Boosting yielded good results, but there is need for enhanced enhancements to enhance the classification of fake news more effectively, especially for models like SVM and Logistic Regression in imbalanced precision and recall.

8 References

[1] Zhang, X. and Ghorbani, A.A., 2020. An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, *57*(2), p.102025. https://doi.org/10.1016/j.ipm.2019.03.004

[2] Gradoń, K., 2020. Crime in the time of the plague: Fake news pandemic and the challenges to law-enforcement and intelligence community. *Society Register*, *4*(2), pp.133-148. 10.14746/sr.2020.4.2.10

[3] Guo, Q. and Zhong, J., 2022. The effect of urban innovation performance of smart city construction policies: evaluate by using a multiple period difference-in-differences model. *Technological Forecasting and Social Change*, *184*, p.122003. https://doi.org/10.1016/j.techfore.2022.122003

[4] Chen, M.Y., Lai, Y.W. and Lian, J.W., 2023. Using deep learning models to detect fake news about COVID-19. *ACM Transactions on Internet Technology*, *23*(2), pp.1-23. https://doi.org/10.1145/3533431

[5] Li, L., Wu, X., Kong, M., Liu, J. and Zhang, J., 2023. Quantitatively interpreting residents happiness prediction by considering factor–factor interactions. *IEEE Transactions on Computational Social Systems*, *11*(1), pp.1402-1414. 10.1109/TCSS.2023.3246181

[6] Babaei, M., Kulshrestha, J., Chakraborty, A., Redmiles, E.M., Cha, M. and Gummadi, K.P., 2021. Analyzing biases in perception of truth in news stories and their implications for fact checking. *IEEE Transactions on Computational Social Systems*, *9*(3), pp.839-850. 10.1109/TCSS.2021.3096038

[7] Jain, A., Shakya, A., Khatter, H. and Gupta, A.K., 2019, September. A smart system for fake news detection using machine learning. In *2019 International conference on issues and challenges in intelligent computing techniques (ICICT)* (Vol. 1, pp. 1-4). IEEE. 10.1109/ICICT46931.2019.8977659

[8] Xiong, Z., Li, X., Zhang, X., Deng, M., Xu, F., Zhou, B. and Zeng, M., 2023. A comprehensive confirmation-based selfish node detection algorithm for socially aware networks. *Journal of Signal Processing Systems*, *95*(12), pp.1371-1389.

[9] Zenggang, X., Mingyang, Z., Xuemin, Z., Sanyuan, Z., Fang, X., Xiaochao, Z., Yunyun, W. and Xiang, L., 2022. Social similarity routing algorithm based on socially aware networks in the big data environment. *Journal of Signal Processing Systems*, *94*(11), pp.1253-1267.

[10] de Souza, J.V., Gomes Jr, J., Souza Filho, F.M.D., Oliveira Julio, A.M.D. and de Souza, J.F., 2020. A systematic mapping on automatic classification of fake news in social media. *Social Network Analysis and Mining*, *10*, pp.1-21.

[11] Shahzad, K., Khan, S.A., Iqbal, A., Shabbir, O. and Latif, M., 2023. Determinants of fake news diffusion on social media: A systematic literature review. *Global Knowledge, Memory and Communication*.

[12] Mishra, S., Shukla, P. and Agarwal, R., 2022. Analyzing machine learning enabled fake news detection techniques for diversified datasets. *Wireless Communications and Mobile Computing*, *2022*(1), p.1575365. https://doi.org/10.1155/2022/1575365

[13] Marwick, A.E., 2018. Why do people share fake news? A sociotechnical model of media effects. *Georgetown law technology review*, *2*(2), pp.474-512.
[14] Mishra, S., Shukla, P. and Agarwal, R., 2022. Analyzing machine learning enabled fake news detection techniques for diversified datasets. *Wireless Communications and Mobile Computing*, *2022*(1), p.1575365.
[15] Jain, A. and Kasbe, A., 2018, February. Fake news detection. In 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-5). IEEE.
[16] Stahl, K., 2018. Fake news detection in social media. *California State University Stanislaus*, *6*, pp.4-15.
[17] Nordberg, P., Kävrestad, J. and Nohlberg, M., 2020. Automatic detection of fake news. In 6th International Workshop on Socio-Technical Perspective in IS Development, virtual conference in Grenoble, France, June 8-9, 2020 (pp. 168-179). CEUR-WS.
[18] Dogru, H.B., Tilki, S., Jamil, A. and Hameed, A.A., 2021, April. Deep learning-based classification of news texts using doc2vec model. In *2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)* (pp. 91-96). IEEE.
[19] Zhao, J., Zhao, Z., Shi, L., Kuang, Z. and Liu, Y., 2023. Collaborative mixture-of-experts model for multi-domain fake news detection. *Electronics*, *12*(16), p.3440.
[20] Tajrian, M., Rahman, A., Kabir, M.A. and Islam, M.R., 2023. A review of methodologies for fake news analysis. *IEEE Access*.
[21] Oeldorf-Hirsch, A., Schmierbach, M., Appelman, A. and Boyle, M.P., 2020. The ineffectiveness of fact-checking labels on news memes and articles. *Mass Communication and Society*, *23*(5), pp.682-704.
[22] Liu, Y. and Wu, Y.F.B., 2020. Fned: a deep network for fake news early detection on social media. *ACM Transactions on Information Systems (TOIS)*, *38*(3), pp.1-33.
[23] Shu, K., Mahudeswaran, D., Wang, S., Lee, D. and Liu, H., 2020. Fakenewsnet: A data repository with news content, social context, and spatiotemporal information for studying fake news on social media. *Big data*, *8*(3), pp.171-188.
[24] Shu, K., Bernard, H.R. and Liu, H., 2019. Studying fake news via network analysis: detection and mitigation. *Emerging research challenges and opportunities in computational social network analysis and mining*, pp.43-65.
[25] Guo, Q. and Zhong, J., 2022. The effect of urban innovation performance of smart city construction policies: evaluate by using a multiple period difference-in-differences model. Technological Forecasting and Social Change, 184, p.122003.
[26] Khan, T., Michalas, A. and Akhunzada, A., 2021. Fake news outbreak 2021: Canstop the viral spread?. Journal of Network and Computer Applications, 190, p.103112.
[27] Shahzad, K., Khan, S.A., Ahmad, S. and Iqbal, A., 2022. A scoping review of the relationship of big data analytics with context-based fake news detection on digital media in the data age. Sustainability, 14(21), p.14365.
[28] Choraś, M., Demestichas, K., Giełczyk, A., Herrero, Á., Ksieniewicz, P., Remoundou, K., Urda, D. and Woźniak, M., 2021. Advanced Machine Learning techniques for fake news

(online disinformation) detection: A systematic mapping study. Applied Soft Computing, 101, p.107050.
[29] Ahmed, A.A.A., Aljabouh, A., Donepudi, P.K. and Choi, M.S., 2021. Detecting fake news using machine learning: A systematic literature review. arXiv preprint arXiv:2102.04458.
[30] Tajrian, M., Rahman, A., Kabir, M.A. and Islam, M.R., 2023. A review of methodologies for fake news analysis. IEEE Access.
[31] Alonso, M.A., Vilares, D., Gómez-Rodríguez, C. and Vilares, J., 2021. Sentiment analysis for fake news detection. Electronics, 10(11), p.1348.
[32] Mridha, M.F., Keya, A.J., Hamid, M.A., Monowar, M.M. and Rahman, M.S., 2021. A comprehensive review on fake news detection with deep learning. IEEE access, 9, pp.156151-156170.
[33] Ansar, W. and Goswami, S., 2021. Combating the menace: A survey on characterization and detection of fake news from a data science perspective. International Journal of Information Management Data Insights, 1(2), p.100052.
[34] Alghamdi, J., Luo, S. and Lin, Y., 2024. A comprehensive survey on machine learning approaches for fake news detection. Multimedia Tools and Applications, 83(17), pp.51009-51067.
[35] Merryton, A.R. and Augasta, G., 2020. A survey on recent advances in machine learning techniques for fake news detection. Test Eng. Manag, 83, pp.11572-11582.
[36] Aïmeur, E., Amri, S. and Brassard, G., 2023. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, *13*(1), p.30.
[37] Waghmare, A.D. and Patnaik, G.K., 2021. Fake news detection of social media news in blockchain framework. *Indian J. Comput. Sci. Eng*, *12*(4), pp.972-980.
[38] Ali, I., Ayub, M.N.B., Shivakumara, P. and Noor, N.F.B.M., 2022. Fake news detection techniques on social media: A survey. *Wireless Communications and Mobile Computing*, *2022*(1), p.6072084.
[39] Harrag, F. and Djahli, M.K., 2022. Arabic fake news detection: A fact checking based deep learning approach. *Transactions on Asian and Low-Resource Language Information Processing*, *21*(4), pp.1-34.
[40] Khan, S.A., Shahzad, K., Shabbir, O. and Iqbal, A., 2022. Developing a framework for fake news diffusion control (FNDC) on digital media (DM): a systematic review 2010–2022. *Sustainability*, *14*(22), p.15287.
[41] da Silva, F.C.D., Garcia, A.C.B. and Siqueira, S.W.M., 2022, May. A systematic literature mapping on profile trustworthiness in fake news spread. In *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 275-279). IEEE.
[42] Yuan, L., Jiang, H., Shen, H., Shi, L. and Cheng, N., 2023. Sustainable development of information dissemination: A review of current fake news detection research and practice. *Systems*, *11*(9), p.458.

[43] Ruffo, G., Semeraro, A., Giachanou, A. and Rosso, P., 2023. Studying fake news spreading, polarisation dynamics, and manipulation by bots: A tale of networks and language. *Computer science review*, *47*, p.100531.
[44] Papageorgiou, E., Chronis, C., Varlamis, I. and Himeur, Y., 2024. A survey on the use of large language models (llms) in fake news. *Future Internet*, *16*(8), p.298.
[45] Hamed, S.K., Ab Aziz, M.J. and Yaakub, M.R., 2023. A review of fake news detection approaches: A critical analysis of relevant studies and highlighting key challenges associated with the dataset, feature representation, and data fusion. *Heliyon*.
[46] Hangloo, S. and Arora, B., 2021. Fake News Detection Tools and Methods--A Review. arXiv preprint arXiv:2112.11185.
[47] Stitini, O., Kaloun, S. and Bencharef, O., 2022. Towards the detection of fake news on social networks contributing to the improvement of trust and transparency in recommendation systems: trends and challenges. *Information*, *13*(3), p.128.
[48] De Beer, D. and Matthee, M., 2021. Approaches to identify fake news: a systematic literature review. *Integrated science in digital age 2020*, pp.13-22.
[49] Awajan, A., Alazab, M., Khurma, R.A., Alsaadeh, R. and Wedyan, M., 2022. Fake news detection and prevention using artificial intelligence techniques: A review of a decade of research. *International Journal of Computer Information Systems and Industrial Management Applications*, *14*, pp.12-12.