

# Defensive Modeling of Fake News through Online Social Networks

Ms. B Lokeswari

Department of Computer Science, Sri Venkateswara University, Tirupati

**Abstract**— Online social networks (OSNs) have become an integral mode of communication among people and even non-human scenarios can also be integrated into OSNs. The ever-growing rise in the popularity of OSNs can be attributed to the rapid growth of Internet technology. OSN becomes the easiest way to broadcast media (news/content) over the Internet. In the wake of emerging technologies, there is dire need to develop methodologies, which can minimize the spread of fake messages or rumors that can harm society in any manner. In this article, a model is proposed to investigate the propagation of such messages currently coined as fake news. The proposed model describes how misinformation gets disseminated among groups with the influence of different misinformation refuting measures. With the onset of the novel coronavirus-19 pandemic, dubbed COVID-19, the propagation of fake news related to the pandemic is higher than ever. In this article, we aim to develop a model that will be able to detect and eliminate fake news from OSNs and help ease some OSN users stress regarding the pandemic. A system of TF IDF is used to formulate the model. The Logistic Regression is a Machine Learning classification algorithm that is used to predict the probability of a categorical dependent variable. In logistic regression, the dependent variable is a binary variable that contains data coded as 1 (true) or 0 (fake).

## I. INTRODUCTION

In the 20th century, the Internet has become the most powerful tool for communication. It facilitates efficient and effective transfer of media from one location to another. With the development of Internet technology, social networks such as Facebook, WhatsApp, Twitter, Instagram, and Google plus have become a vital platform for information exchange. Nowadays, people are connected through online social networks (OSNs) and exchange information in a cost-efficient manner through data transfer. However, information exchanged on OSN platforms may comprise rumors that may affect the social lives of people. Take COVID-19 as an example, where the proliferation of fake news related to the virus has left many people skeptical of any information; they read information related to the virus on social media [3]. Some recent fake news related to a cure for COVID-19 has spread through Facebook. Due to this type of misinformation, people from different corners of the world died. The impact of fake news on people related to a well-known Zika virus case study was presented by Sommariva *et al.* The authors found that the speed of fake news spread on OSNs is tremendous and tends to cover large audiences.

One major challenge that is associated with OSNs is verification of messages exchanged as well as the authenticity of users. Some messages that are spread through these social networks may create horrible situations regarding peace and harmony in society. Such messages, currently coined as fake news, can also be life-threatening. These kinds of messages are in essence just rumors/misinformation which are propagated through different means either just for entertainment or maliciously as well. Due to such messages, unnecessary anxiety uprise among the public and countries may also face economic loss seen currently with COVID-19. This can be attributed to the fact that the rate of information dissemination on OSNs is very quick and information can spread globally within seconds. Several instances exist where the spread of fake news on OSNs created undesirable and detrimental situations for society.

There exists, different mathematical models, to study the behavior of message dynamics in social networks. In the wake of the wide scope and significance of social networks, rumor and fake news identification have become a potentially strong area of research. This urges for the development of the various mathematical models for rumor dissemination. TF IDF model a problem with scoring word frequency is that highly frequent words start to dominate in the document (e.g., larger score), but may not contain as much “informational content” to the model as rarer but perhaps domain specific words.

One approach is to rescale the frequency of words by how often they appear in all documents, so that the scores for frequent words like “the” that are also frequent across all documents are penalized.

This approach to scoring is called Term Frequency – Inverse Document Frequency, or TF-IDF for short, where:

- Term Frequency: is a scoring of the frequency of the word in the current document.
- Inverse Document Frequency: is a scoring of how rare the word is across documents.

The scores are a weighting where not all words are equally as important or interesting.

The scores have the effect of highlighting words that are distinct (contain useful information) in a given document.

## II. LITERATURE REVIEW

### **Fake News Detection on Social Media: A Data Mining Perspective**

*Kai Shu, Kai Shu, Suhang Wang, Jiliang Tang, Huan Liu*

Social media for news consumption is a double-edged sword. On the one hand, its low cost, easy access, and rapid dissemination of information lead people to seek out and consume news from social media. On the other hand, it enables the wide spread of "fake news", i.e., low quality news with intentionally false information. The extensive spread of fake news has the potential for extremely negative impacts on individuals and society. Therefore, fake news detection on social media has recently become an emerging research that is attracting tremendous attention. Fake news detection on social media presents unique characteristics and challenges that make existing detection algorithms from traditional news media ineffective or not applicable. First, fake news is intentionally written to mislead readers to believe false information, which makes it difficult and nontrivial to detect based on news content; therefore, we need to include auxiliary information, such as user social engagements on social media, to help make a determination. Second, exploiting this auxiliary information is challenging in and of itself as users' social engagements with fake news produce data that is big, incomplete, unstructured, and noisy. Because the issue of fake news detection on social media is both challenging and relevant, we conducted this survey to further facilitate research on the problem. In this survey, we present a comprehensive review of detecting fake news on social media, including fake news characterizations on psychology and social theories, existing algorithms from a data mining perspective, evaluation metrics and representative datasets. We also discuss related research areas, open problems, and future research directions for fake news detection on social media.

### **Beyond News Contents: The Role of Social Context for Fake News Detection**

*Kai Shu, Suhang Wang, Huan Liu*

Social media is becoming popular for news consumption due to its fast dissemination, easy access, and low cost. However, it also enables the wide propagation of fake news, i.e., news with intentionally false information. Detecting fake news is an important task, which not only ensures users receive authentic information but also helps maintain a trustworthy news ecosystem. The majority of existing detection algorithms focus on finding clues from news contents, which are generally not effective because fake news is often intentionally written to mislead users by mimicking true news. Therefore, we need to explore auxiliary information to improve detection. The social context during news dissemination process on social media forms the inherent tri-relationship, the relationship among publishers, news pieces, and users, which has the potential to improve fake news detection. For example, partisan-biased publishers are more likely to publish fake news, and low-credible users are more likely to share fake news. In this paper, we study the novel problem of exploiting social context for fake news detection. We propose a tri-relationship embedding framework TriFN, which models publisher-news relations and user-news interactions simultaneously for fake news classification. We conduct experiments on two real-world datasets, which demonstrate that the proposed approach significantly outperforms other baseline methods for fake news detection.

### **A Hybrid Deep Model for Fake News Detection**

*Natali Ruchansky, Natali Ruchansky, Sungyong Seo*

The topic of fake news has drawn attention both from the public and the academic communities. Such misinformation has the potential of affecting public opinion, providing an opportunity for malicious parties to manipulate the outcomes of public events such as elections. Because such high stakes are at play, automatically detecting fake news is an important, yet challenging problem that is not yet well understood. Nevertheless, there are three generally agreed upon characteristics of fake news: the text of an article, the user response it receives, and the source users promoting it. Existing work has largely focused on tailoring solutions to one particular characteristic which has limited their success and generality.

In this work, we propose a model that combines all three characteristics for a more accurate and automated prediction. Specifically, we incorporate the behavior of parties, users and articles, and the group behavior of users who propagate fake

news. Motivated by the three characteristics, we propose a model called CSI which is composed of three modules: Capture, Score, and Integrate. The first module is based on the response and text; it uses a Recurrent Neural Network to capture the temporal pattern of user activity on a given article. The second module learns the source characteristic based on the behavior of users, and the two are integrated with the third module to classify an article as fake or not. Experimental analysis on real-world data demonstrates that CSI achieves higher accuracy than existing models, and extracts meaningful latent representations of both users and articles.

### **Fake News: Fundamental Theories, Detection Strategies and Challenge**

*Xinyi Zhou, Huan Liu, Reza Zafarani*

The explosive growth of fake news and its erosion to democracy, justice, and public trust increased the demand for fake news detection. As an interdisciplinary topic, the study of fake news encourages a concerted effort of experts in computer and information science, political science, journalism, social science, psychology, and economics. A comprehensive framework to systematically understand and detect fake news is necessary to attract and unite researchers in related areas to conduct research on fake news. This tutorial aims to clearly present (1) fake news research, its challenges, and research directions; (2) a comparison between fake news and other related concepts (e.g., rumors); (3) the fundamental theories developed across various disciplines that facilitate interdisciplinary research; (4) various detection strategies unified under a comprehensive framework for fake news detection; and (5) the state-of-the-art datasets, patterns, and models. We present fake news detection from various perspectives, which involve news content and information in social networks, and broadly adopt techniques in data mining, machine learning, natural language processing, information retrieval and social search. Facing the upcoming 2020 U.S. presidential election, challenges for automatic, effective and efficient fake news detection are also clarified in this tutorial

### **The Role Of User Profiles For Fake News Detection**

*Kai Shu, Xinyi Zhou, Suhang Wang, Huan Liu*

Consuming news from social media is becoming increasingly popular. Social media appeals to users due to its fast dissemination of information, low cost, and easy access. However, social media also enables the widespread of fake news. Due to the detrimental societal effects of fake news, detecting fake news has attracted increasing attention. However, the detection performance only using news contents is generally not satisfactory as fake news is written to mimic true news. Thus, there is a need for an in-depth understanding on the relationship between user profiles on social media and fake news. In this paper, we study the problem of understanding and exploiting user profiles on social media for fake news detection. In an attempt to understand connections between user profiles and fake news, first, we measure users' sharing behaviors and group representative users who are more likely to share fake and real news; then, we perform a comparative analysis of explicit and implicit profile features between these user groups, which reveals their potential to help differentiate fake news from real news. To exploit user profile features, we demonstrate the usefulness of these user profile features in a fake news classification task. We further validate the effectiveness of these features through feature importance analysis. The findings of this work lay the foundation for deeper exploration of user profile features of social media and enhance the capabilities for fake news detection.

### **Problem Statement**

- The ever- growing rise in the popularity of OSNs can be attributed to the rapid growth of Internet technology.
- To develop a model that will be able to detect and eliminate fake news from OSNs and help ease some OSN user's stress.

### **III. PROPOSED WORK**

- Our proposed system involves TF IDF Algorithm in Machine Learning concept used to implement the model.
- Grid Searching is used to scanning the data to configure optimal parameters for a given model.
- Random forest Classifier uses meta estimator that fits a number of decision tree classifier on various sub-samples of the data set and uses averaging to improve the predictive accuracy and control over fitting.

## Advantages

- Easy detection of the fake news with the concluded technique.
- Time consuming.
- Best accuracy Model help to find the true news.

## IV. METHODOLOGY

### 4.1 Dataset Collection

A dataset (or data set) is a collection of data, usually presented in tabular form. Each column represents a particular variable. Each row corresponds to a given member of the dataset in question. It lists values for each of the variables, such as height and weight of an object. Each value is known as a datum.

We have chosen to use a publicly-available social media dataset which contains a relatively small number of inputs and cases. The data is arranged in such a way that will allow those trained data in disciplines to easily draw parallels between familiar statistical and novel ML techniques. Additionally, the compact dataset enables short computational times on almost all modern computers.

### 4.2 Pre-Processing

The sklearn. preprocessing package provides several common utility functions and transformer classes to change raw feature vectors into a representation that is more suitable for the downstream estimators.

In general, learning algorithms benefit from standardization of the data set. If some outliers are present in the set, robust scalers or transformers are more appropriate. The behaviours of the different scalers, transformers, and normalizers on a dataset containing marginal outliers is highlighted in.

### 4.3 EDA (Exploratory data/Visualized Analysis)

Exploratory Data Analysis or (EDA) understands the data sets by summarizing their main characteristics often plotting them visually. This step is very important especially when we arrive at modelling the data in order to apply Machine learning. Plotting in EDA consists of Histograms, Box plot, Scatter plot and many more. It often takes much time to explore the data. Through the process of EDA, we can ask to define the problem statement or definition on our data set which is very important. So in this tutorial, we will explore the data and make it ready for modelling.

#### 1. Importing the required libraries for EDA

The libraries that are used in order to perform EDA (Exploratory data analysis)

#### 2. Loading the data into the data frame.

Loading the data into the pandas data frame is certainly one of the most important steps in EDA, as we can see that the value from the data set is comma-separated. One thing to remember in this step is that uploaded files will get deleted when this runtime is recycled.

#### 4.3.1 Checking the types of data

The datatypes because sometimes the MSRP or the price of the car would be stored as a string or object, if in that case, we have to convert that string to the integer data only then we can plot the data via a graph.

#### 4.3.2 Dropping irrelevant columns

This step is certainly needed in every EDA because sometimes there would be many columns that we never use in such cases dropping is the only solution. In this case, the columns such as Engine Fuel Type, Market Category, Vehicle style, Popularity, Number of doors, Vehicle Size doesn't make any sense to me so I just dropped for this instance.

#### 4.3.3 Renaming the column

In this instance, most of the column names are very confusing to read, so I just tweaked their column names. This is a good approach it improves the readability of the data set.

#### 4.3.4 Dropping the duplicate rows

This is often a handy thing to do because a huge data set as in this case contains more than 10,000 rows often have some duplicate data which might be disturbing, so here I remove all the duplicate value from the data-set. For example, prior to removing I had 11914 rows of data but after removing the duplicates 10925 data meaning that I had 989 of duplicate data.

#### 4.3.5 Dropping the missing or null values.

An outlier is a point or set of points that are different from other points. This is mostly similar to the previous step but in here all the missing values are detected and are dropped later. Now, this is not a good approach to do so, because many people just replace the missing values with the mean or the average of that column

#### 4.3.6 Detecting Outlier

Sometimes they can be very high or very low. It's often a good idea to detect and remove the outliers. Because outliers are one of the primary reasons for resulting in a less accurate model. Hence, it's a good idea to remove them. The outlier detection and removing that I am going to perform is called IQR score technique. Often outliers can be seen with visualizations using a box plot.

#### 4.4 Implement the model

The **implementation model** represents how a system (application, service, interface, etc.) works. It is often described with system diagrams and pseudo code to be later translated into real code. It is shaped by technical, organizations, and business constraints. Here we use TF IDF, Grid Search, Simple imputer, Logistic regression, Random Forest Classifier, Dummy Classifier.

##### 4.4.1 TF IDF

TF IDF model a problem with scoring word frequency is that highly frequent words start to dominate in the document (e.g., larger score), but may not contain as much "informational content" to the model as rarer but perhaps domain specific words.

One approach is to rescale the frequency of words by how often they appear in all documents, so that the scores for frequent words like "the" that are also frequent across all documents are penalized.

This approach to scoring is called Term Frequency – Inverse Document Frequency, or TF-IDF for short, where:

- Term Frequency: is a scoring of the frequency of the word in the current document.
- Inverse Document Frequency: is a scoring of how rare the word is across documents.
- The scores are a weighting where not all words are equally as important or interesting.
- The scores have the effect of highlighting words that are distinct (contain useful information) in a given document.

##### 4.4.2 Grid Search:

Grid Searching is used to scanning the data to configure optimal parameters for a given model. It is also used to calculate the best parameters.

##### 4.4.3 Simple Imputer:

If "mean" replace missing values using the mean along the axis. If "median" replace missing values using the median along the axis. If "most frequent" then replace missing values using the most frequent value along the axis.

##### 4.4.4 Random Forest Classifier:

Random Forest classifier is the meta estimator that fits a number of decision tree classifier on various sub-samples of the data set and uses averaging to improve the predictive accuracy and control over fitting.

##### 4.4.5 Logistic Regression:

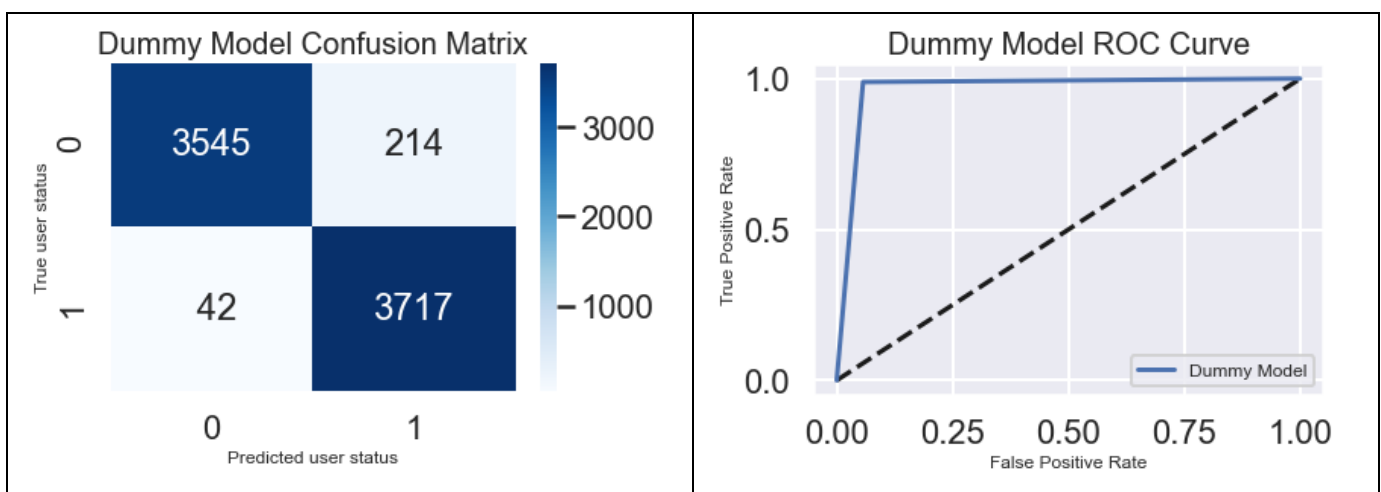
In this model the probability of a certain class or event (pass/fail, true/false, healthy/sick). It detected that the image would be assigned a probability between 0 and 1 (form of binary regression).

#### 4.5 Evaluation

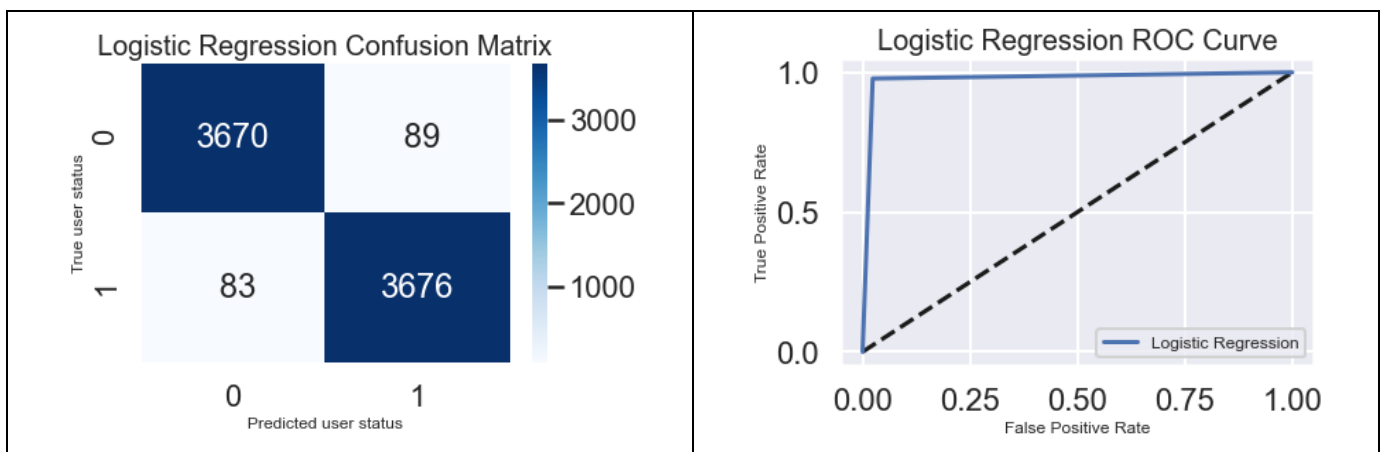
Model evaluation aims to estimate the generalization accuracy of a model on future (unseen/out-of-sample) data. In this model precision, support, accuracy and confusion matrices are used to evaluate the fake news.

### V. IMPLEMENTATION

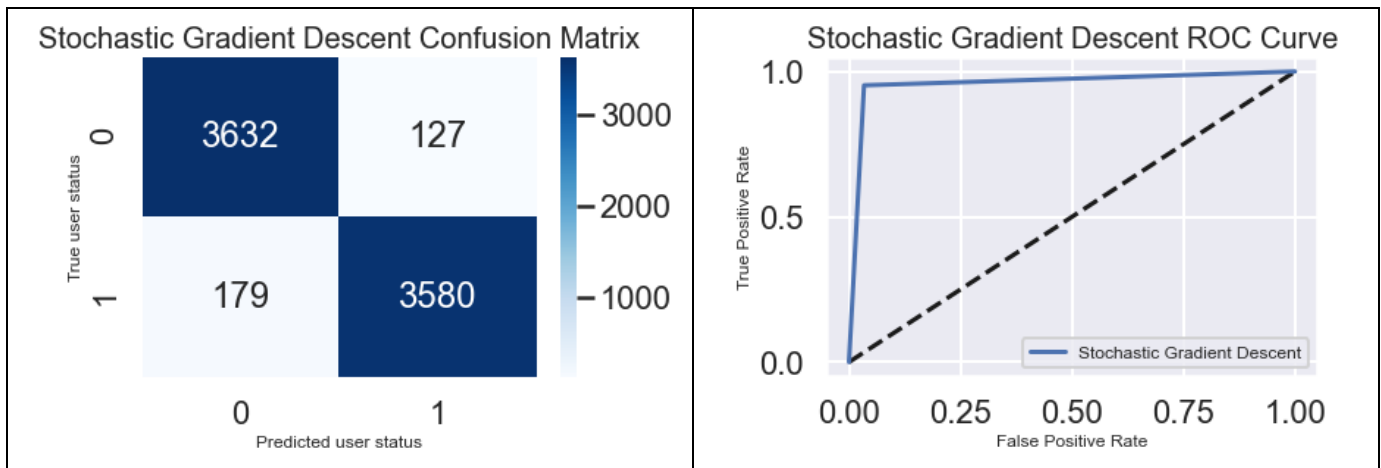
MultiNomial Naive Bayes	Precision	Recall	F1-Score	Support
0	0.99	0.94	0.97	3759
1	0.95	0.99	0.97	3759
Accuracy			0.97	7518
Macro Avg	0.97	0.97	0.97	7518
Weighted Avg	0.97	0.97	0.97	7518



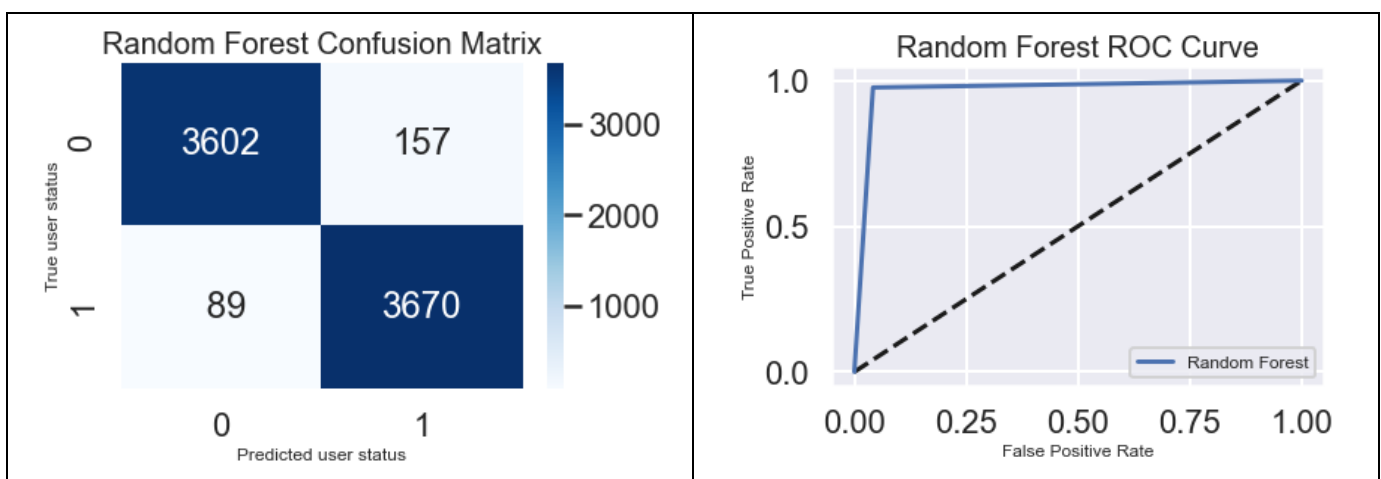
Logistic Regression	Precision	Recall	F1-Score	Support
0	0.98	0.98	0.98	3759
1	0.98	0.98	0.98	3759
Accuracy			0.98	7518
Macro Avg	0.98	0.98	0.98	7518
Weighted Avg	0.98	0.98	0.98	7518



Stochastic Gradient Descent	Precision	Recall	F1-Score	Support
0	0.95	0.97	0.96	3759
1	0.97	0.95	0.96	3759
Accuracy			0.98	7518
Macro Avg	0.96	0.96	0.96	7518
Weighted Avg	0.96	0.96	0.96	7518



Random Forest Classifier	Precision	Recall	F1-Score	Support
0	0.98	0.96	0.97	3759
1	0.96	0.98	0.97	3759
Accuracy			0.97	7518
Macro Avg	0.97	0.97	0.97	7518
Weighted Avg	0.97	0.97	0.97	7518



## VI. MODEL SUMMARY

From the 4 models it is observed that the exception of Naive Bayes all of them have very few mis-classification.

The ROC\_AUC score is 0.964 which is exceptionally well for text classification.

The top three models are:

- 1) Logistic Regression
- 2) Stochastic Gradient Descent
- 3) Random Forest

Random Forest, SGD and Logistic Regression has comparable ROC-AUC score.

Logistic Regression has the highest ROC-AUC score it trained only a  $\max\_df = 0.25$ . This means the modelled ignored terms that have a document frequency strictly lower than the given threshold. Random Forest is more scalable, and interpretable and also performs better with noisy data. Considering these, we chose Random Forest as the best model. Feature Importance of the model shows that 'president Donald Trump', Washington 'President Obama' were given the highest importance. This is in alignment with the fact that this dataset is indeed a representation of the news during the 2016 US Presidential Election. Disadvantages: -We need a bigger dataset covering a wide range of news for both TRUE and FAKE labels to make a more generalized model.

## VII. CONCLUSION AND FUTURE WORK

The research work presented in this article proposes a mathematical model to study the dynamic spreading and controlling activities of message transmission in OSNs. The proposed model employs differential equations for investigating the effect of verification and blocking of users and the spread of messages on OSNs. The expression for basic reproduction  $R_0$  is obtained, which is used to analyze the status of rumor in the social network. Results obtained indicates that if  $R_0$  is less than 1, then rumors and fake news will be eliminated and OSNs gets stabilized locally. The local stability of rumor-free equilibrium is established by the Jacobian matrix. It is found that if the eigenvalues of the matrix are less than zero then the network will be asymptotically stabilizing locally in nature and free from the rumors. The Lyapunov function used to establish the global asymptotic stable status of the social network. Mathematical analysis has been performed to depict the accuracy of the rumor-free equilibrium. The activities of different classes of users have also been examined in the social network. In future, the method of latent and isolation can be used for the prevention of social network from rumor spread and fake news propagation. The issues examined in this article are of direct current concern, and the pandemic COVID-19 is creating a global crisis in rumors and fake news propagating freely on OSNs which may continue until it is cured/handled. Real-world data clearly show that fake news propagation can be harmful for people, businesses, and many other facets of society. The results in this article therefore, may help solve some of the current global issues related to fake news spread.

## REFERENCES

- [1] Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, and Huan Liu. "Fake news detection on social media: A data mining perspective." *ACM SIGKDD explorations newsletter* 19, no. 1 (2017): 22-36.
- [2] Shu, Kai, Suhang Wang, and Huan Liu. "Beyond news contents: The role of social context for fake news detection." In *Proceedings of the twelfth ACM international conference on web search and data mining*, pp. 312-320. 2019.
- [3] Ruchansky, Natali, Sungyong Seo, and Yan Liu. "Csi: A hybrid deep model for fake news detection." In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, pp. 797-806. 2017.
- [4] Reis, Julio CS, André Correia, Fabrício Murai, Adriano Veloso, and Fabrício Benevenuto. "Supervised learning for fake news detection." *IEEE Intelligent Systems* 34, no. 2 (2019): 76-81.
- [5] Shu, Kai, Xinyi Zhou, Suhang Wang, Reza Zafarani, and Huan Liu. "The role of user profiles for fake news detection." In *Proceedings of the 2019 IEEE/ACM international conference on advances in social networks analysis and mining*, pp. 436-439. 2019.
- [6] Karimi, Hamid, Proteek Roy, Sari Saba-Sadiya, and Jiliang Tang. "Multi-source multi-class fake news detection." In *Proceedings of the 27th international conference on computational linguistics*, pp. 1546-1557. 2018.
- [7] Pérez-Rosas, Verónica, Bennett Kleinberg, Alexandra Lefevre, and Rada Mihalcea. "Automatic detection of fake news." *arXiv preprint arXiv:1708.07104* (2017).
- [8] Zhou, Xinyi, and Reza Zafarani. "Network-based fake news detection: A pattern-driven approach." *ACM SIGKDD Explorations Newsletter* 21, no. 2 (2019): 48-60.
- [9] Granik, Mykhailo, and Volodymyr Mesyura. "Fake news detection using naive Bayes classifier." In *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, pp. 900-903. IEEE, 2017.
- [10] Parikh, Shivam B., and Pradeep K. Atrey. "Media-rich fake news detection: A survey." In *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, pp. 436-441. IEEE, 2018.
- [11] Singhania, Sneha, Nigel Fernandez, and Shrishra Rao. "3han: A deep neural network for fake news detection." In *International Conference on Neural Information Processing*, pp. 572-581. Springer, Cham, 2017.