

FAKE NEWS DETECTOR

Problem Statement :

Often sensational news is created and spread through social media to achieve intended end. On the other hand, it may also involve narration of a true fact however being deliberately exaggerated. This may also affect the importance of serious news media. The problem is to identify the authenticity of the news and online content. Equally important problem is to identify the bots involved in spreading false news



Introduction :

In recent times we have come across many instances of fake news popping up in our Facebook and Twitter feeds from time to time. Not only social media sites suffer from this menace but even sites of popular newspaper publications provide its readers with fake information many a times. This is a major problem which needs to be addressed because fake news is misleading and tends to create unrest among common people. The

best case of this fake news problem emerged in the 2016 US Presidential Elections where a number of political pundits claimed that the rise of significantly biased and/or untrue news influenced the election and hence may have been one of the major deciding factors for the result of the elections.

Obviously, a deliberately misleading story is “fake news” but lately blathering social media discourse is changing its definition. Some now use the term to dismiss facts counter to their preferred viewpoints, which is especially seen in the political scenario and such a vaguely-defined term is ripe for cynical manipulation.

Back here in India we have been facing similar problems. Indians and the ‘Indian National Anthem’ being adjudged the best by UNESCO is probably the most common fake news going around the Internet. While this false information may have been innocuous, it captures the larger menace we face today. With the advent of new age digital and social media, fake news has pervaded all spheres of life, political and social

Fabricated and manipulated content are gaining steam, leading to the possibility of potential violence and impacting society. The rise of digital and social media as powerful platforms has only magnified the effect of fake and false news. Umpteen number of news/information portals are being set up as there are few entry barriers unlike in the traditional media. In addition, growing polarisation of society on ideological lines has made the job of spreading fake news easier. Content that denigrates leaders/groups of the opposite ideology based on falsehoods, deepens communal polarisation or incites hatred have gained traction in the last few years. In the past, communal violence in India was a localised affair. Today, it is extensively being fed and triggered through the Internet. Provocative content, inaccurate information, doctored videos, and pictures are being disseminated through various online and mobile platforms. The platforms serve like nodal agencies distributing unverified information.

While media researchers around the world are investigating the fake news scene, little credible information is available on the creators and the intention behind it. But if what has been found is true, it is purely a way to make advertising money through click baits, enticing people to click and continue reading, and is organised by political or other social groups. In India, numerous sites are set up to peddle fake news with click bait headlines. They are also very well organised with multiple linked pages on social media platforms that are used to make the content go viral.

The advent of fake news is not new or recent, only its potential to reach people has amplified due to online platforms and applications that are free. the sheer expanse of

the Internet and the anonymity it grants makes it difficult to track down people. Unlike mainstream media that falls under comprehensive regulation, online platforms have scope for wrongdoing due to the lack of binding rules, and the ability to keep owners and editors private like in the case of fake news sites. In the absence of such crucial information, there is no understanding of the liability and the credibility of the information that is being hosted on their respective sites. This is the main strength of the creators of fake news, the ability to remain anonymous in the guise of a media outlet. Most digital media outlets do not have basic information regarding editors, publishers or the physical address of the registered entity. We could do well to begin with some basic regulation for digital media outlets like compulsory and online registration of details.

Hence, we can conclude that detecting fake news is the need of the hour and here we have tried to create our own approach towards tackling the problem and have proposed a proper solution extensively documented below.

Approach :

Our implementation contains 3 search fields which are :-

- 1)Search by article content.
- 2)Search using key terms.
- 3)Search for website in database.

In the first search field we have used **Natural Language Processing** for the first search field to come up with a proper solution for the problem, and hence we have attempted to create a model which can classify fake news according to the terms used in the news paper articles. Our application uses NLP techniques like **CountVectorization** and **TF-IDF Vectorization** before passing it through a **Passive Aggressive Classifier** to output the authenticity as a percentage probability of an article.

The second search field of the site asks for specific keywords to be searched on the net upon which it provides a suitable output for the percentage probability of that term actually being present in an article or a similar article with those keyword references in it.

The third search field of the site accepts a specific website domain name upon which the implementation looks for the site in our true sites database or the blacklisted sites database. The true sites database holds the domain names which regularly provide proper and authentic news and vice versa. If the site isn't found in either of the databases then the implementation doesn't classify the domain it simply states that the news aggregator does not exist



Technology Stack :

Python 3.x has been used to implement the model using a lot of various packages. The model uses the Passive Aggressive Classifier available in the popular Scikit-learn distribution for machine learning. Other Python packages used have been listed below:-

- 1) Pandas - for handling data and it's manipulation.

<http://scikit-learn.org/stable/install.html>

- 2) Django - for the web based deployment of the model, provides client side implementation using HTML, CSS and Javascript.

<https://www.djangoproject.com/download/>

- 3) Beautiful Soup (bs4)

<https://www.crummy.com/software/BeautifulSoup/bs4/doc/#installing-beautiful-soup>

- 4) Requests

<http://docs.python-requests.org/en/master/user/install/>

Working :

The problem can be broken down into 3 statements :-

- 1) Use NLP to check the authenticity of a news article.
- 2) If the user has a query about the authenticity of a search query then we he/she can directly search on our platform and using our custom algorithm we output a confidence score.
- 3) Check the authenticity of a news source.

These sections have been produced as search fields to take inputs in 3 different forms in our implementation of the problem statement.

1ST Search Field:

The dataset available to us is split into the test and training sets using the `train_test_split()` function of Scikit-learn. To get an idea if the words and tokens in the articles have a significant impact on whether the news in it is actually fake or real, we use `CountVectorizer` and `TfidfVectorizer`. For the `tfidf_vectorizer` the threshold is set to 0.7 which means that the words which appear more than 70% of the time in the articles are not counted in. The `stop_words` parameter is used for avoiding the various stop words used commonly in the English language.

In simple words Articles can be analyzed by feeding them to a machine learning model (Passive Aggressive Classifier) which predicts the reliability of the content after it's trained through predefined datasets of classified real vs fake news.

It seemed like the SVM(Support Vector Machine) would outperform any other model, but as we tested the test data set with Bayesian classifiers such as MultinomialNB, Passive Aggressive Classifier simply outperformed them. The model was tested with Calibrated Classifier CV for both “isotonic” and “sigmoid” methods both of which provided accuracy scores of close to but below 90%, as well as ensemble based classifiers such as the Random Forest Classifier which couldn't provide a higher accuracy on the test data set even when the number of decision trees used for it was significantly increased. Simply increasing the number of trees increased the accuracy very slightly whereas the execution time increased significantly. Therefore we decided that Passive Aggressive Classifier was our best option as it was providing accuracy scores as high as 93% on the test data set. Apart from its relative simplicity it is also much faster when compared to all the above machine learning models mentioned.

2ND Search Field:

The second search field asks for keywords to be searched on the net to find sources for those particular keywords in articles. For this the python package requests is used to pull and provide the HTML and then another python package BeautifulSoup to parse the HTML to extract the headers and the body of the links. Search terms can be analyzed by doing a Google search (first 100 entries) and ensuring if the news corresponding to the keywords have been covered by reliable news sources and aggregators. For every search term covered by a reliable news source it receives a score of +1, while we heavily penalize fake sources. If multiple fake sources cover the news then we penalize the truth score even harder. We also look for keywords like 'hoax', 'fake', etc in the payload content.

3RD Search Field:

The third search field asks for a domain name from the user and tells him/her if the domain is reliable or not. The domain name is taken as input and the implementation searches for it in manually created databases of blacklisted sites which have a high probability of providing fake news and another database containing the domains which provide reliable news and information.