Comparative Analysis of Fake News Detection using Machine Learning and Deep Learning Techniques

Miss. Puja Sunil Erande¹, Prof. Monika Rokade²
PG Student, Sharadchandra Pawar College of Engineering, Junnar Pune, India¹
Assistant Professor, Sharadchandra Pawar College of Engineering, Junnar Pune, India²

ABSTRACT: The transmission of erroneous information has increased dramatically in recent years. Due to its growing popularity in many study communities, issues relating to the transmission of fake news via several social media platforms as well as random web sites from the internet have received huge importance from contemporary day journalism. The goal of creating and disseminating fake news articles is to mislead readers and convince them to trust false information. It's tough to tell the difference between false material and news stories in our daily lives, because most phoney pieces are meticulously constructed to persuade readers to trust their claims. As a result, fake news cannot be classified merely on the basis of content; we must additionally analyse a variety of factors such as the source of the news, user engagements, the legitimacy of the individual sharing the news, and so on. We have proposed applications of NLP and Neural Networks approaches for detecting ‘fake news’ in this study. We can only get a certain level of accuracy using a count vectorizer (using word tallies) or a (Term Frequency Inverse Document Frequency) tfidf matrix (word tallies relative to how often they're used in other articles in your dataset), because they don't take into account the interdependency between a variety of features present in the news content, as well as the content's order. To do so, we offer a system that combines a deep learning unit called LSTM with neural networks and tries to generate comparative analyses.

KEYWORDS: Social Media, Twitter, NLP, Neural Networks, Deep Learning Models, RNN, LSTM

I. INTRODUCTION

The goal of fabricating false news is to deceive individuals by exposing them to a range of hoaxes, propaganda, and inaccurate information. There are some stories that are absolutely untrue or are merely random opinion pieces masquerading as news. Facebook, Twitter, Whatsapp, Reddit, and other social media sites have all been used to distribute fake news. False news frequently attempts to imitate actual headlines and distort the content. In today's world, most businesses use social media and so have accounts on Twitter, Facebook, and Instagram for a variety of commercial purposes such as announcing company news, advertising new product releases, and so on. Consumers, investors, and other stakeholders treat these news signals with the same respect as any other kind of mainstream media. Detecting false information on social media is a critical issue that is also technically difficult to solve. The problem originates from the fact that even the human eye cannot tell the difference between truthful and fake news. During the 2016 US Presidential Elections, the prevalence of fake news had a significant impact on the entire democracy. Later reports said that the fact that many US adults utilise social media to get news was a major factor in Donald Trump's victory over Hillary Clinton. With multiple events in 2019, including the general elections and the Pulwama attack, the scrapping of Article 370 and ongoing protests against the Citizenship Amendment Act, as well as the recent crisis exacerbated by the spread of the Corona Covid-19 virus, the spread of fake news in India has reached a new high. As a result of all of these events, there has been a significant proliferation of false news and viewpoints throughout different social media sites. We present a method for detecting fake news utilising Keras and a few Machine Learning algorithms such as Nave-Bayes, Support Vector Machine (SVM), Logistic Regression, and Deep Learning algorithms such as LSTMs and Neural Networks. Our project is divided into two sections: We compare different methods, such as Nave-Bayes, SVM, Neural Networks utilising Keras, and Recurrent Neural Networks, in the first section (LSTM). In the second portion, we utilise the Logistic Regression Classifier to obtain real-time tweets from Twitter and classify them as suspicious or non-suspect based on content and user characteristics.
II. LITRATURE SURVEY

In [1] construct real-world datasets measuring users trust level on fake news and selectrepresentative groups of both “experienced” users who are able to recognize fake news items asfalse and “naïve” users who are more likely to believe fake news. We perform a comparativeanalysis over explicit and implicit profile features between these user groups, which reveal theirpotential to differentiate fake news. The findings of this paper lay the foundation for futureautomatic fake news detection research. Fake News Detection on Social Media According to thesources that features are extracted from, fake news detection methods generally focus on using news contents and social contexts. Visual features identify fake images that are intentionally created or capture specific characteristics of images in fake news. Social context basedapproaches incorporate features from user profiles, post contents and social networks.

In [2] the problem of understanding and exploiting user profiles on social media for fake newsdetection. In an attempt to understand connections between user profiles and fake news, first, wemeasure 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 fakenews detection.

In [3] RumorSleuth, a multitask deep learning model which can leverage both the textual information and user profile information to jointly identify the veracity of a rumor along with users’ stances. Tests on two publicly available rumor datasets demonstrate that RumorSleuthoutperforms current state-of-the-art models and achieves up to 14% performance gain in rumor veracity classification and around 6% improvement in user stance classification. A multi-task learning approach to jointly learn the rumor class and stances. Multi-task learning refers to learning two or more tasks together leveraging shared structures and correspondences.

In [4] model data is collected from the users’ posts of two popular social media websites: twitter and facebook. Depression level of a user has been detected based on his posts in social media. The standard method of detecting depression of a person is a fully structured or a semi-structured interview method (SDI). These methods need a huge amount of data from the person. Micro blogging sites such as twitter and facebook have become so much popular places to express peoples’ activity and thoughts. The data screening from tweets and posts show the manifestation of depressive disorder symptoms of the user. In this research, machine learning is used to process the scrapped data collected from SNS users. Natural Language Processing (NLP), classified using Support Vector Machine (SVM) and Naïve Bayes algorithm to detect depression potentially in a more convenient and efficient way.

In [5] conduct a three-phase methodology to detect click farming. We begin by clustering communities based on newly-defined collusion networks. We then apply the Louvain community detection method to detecting communities. We finally perform a binary classification on detected-communities. Our results of over a year-long study show that (1) the prevalence of click farming is different across CGSNs; (2) most click farmers are lowly-rated; (3) click-farming communities have relatively tight relations between users; (4) more highly-ranked stores have a greater portion of fake reviews. The develop a web crawler to analyze HTML structure of store pages and user pages on Dianping. Over the past few years, the success of CGSNs has attracted the attention of security researchers. Review-spam detection can be considered as a binary classification or ranking problem. Previous research provides several approaches of detection.

In [6] A model has been suggested to describe the burden of social information as people seek, through social media tweets or mails, to express their feelings. The Twitter dataset is used for user behavior and CNN for training content classification. CNN is used for classification. Since it is very difficult to identify big data files with a conventional approach, social media data is used to describe the training file. Class 0, class 1, and class 2 of the tests of the tweet uses. Class 0 suggests a positive stress level, Class 1 displays negative stress levels and Class 2 corresponds to neutral stress level.

According to [7] attended to an increasing interest in detecting fake profiles and investigating their behaviors. Questions like who are impersonators? What are their characteristics? And are they bots? Will arise. To answer, we begin this research by collecting data from three important communities on Instagram including “Politician”, “News agency”, and
“Sports star”. Inside each community, four verified top accounts are picked. Based on the users who reacted to their published posts, we detect 4K impersonators. Then we employed well-known clustering methods to distribute impersonators into separate clusters to observe obscure behaviors and unusual profile characteristics. We also studied the cross-group analysis of clusters inside each community to explore engagements. Finally, we conclude the study by proposing a complete investigation of the bot-like cluster. 

Identification of impersonators of top verified figures in three major communities on Instagram including “Politician”, “News Agency”, and “Sports Star”. Perform an unsupervised clustering approach to find inner groups of impersonators based on profile metrics. Provide a comparison of clusters in terms of profile characteristics and user behavior activities to no impersonator accounts. Cross category analysis of clusters to understand the distribution of activities and hidden actions. Provide a comprehensive study of the bot-like cluster to understand how they are operating on these communities.

In [8] a method based on unsupervised clustering which analyses the reactions of users called smileys. The reactions are profiled and by applying similarity measures and unsupervised clustering techniques, they are further classified. This approach reveals the behavior of immediate emotional responses of users to the various posts in Facebook. Since reactions are immediate, the analysis of these reactions provides important information to find anomalous behavior in Facebook accounts. The ever increasing use of OSNs has attracted researchers to study about Online Social Networks and its security.

In [9] reviewed and introduced the main concepts of anomalies on the online social networks. Also, presented different types of anomalies and grouped the type of anomalies into six categories; based on nature of anomalies, based on dynamic/static nature of graph structure, based on information available in graph structure, based on behavior, based on structural operations on graph structure and based on interaction pattern in graph structure. Moreover, we highlighted the approaches of anomaly detection, and the literature review has presented the previous works that exactly focused on anomaly detection methods in social networks. Through the Internet. Based on the previous studies the best anomaly detection method in OSN identify rely on the type of anomalies.

In [10] it establishes a worldwide connectivity environment where communities of people share their interests and activities, or who are interested in interests and activities of others. Although social networks have given immense benefits to people at the same time harming people with various mischievous activities that take place on social platforms. This causes significant economic loss to our society and even threatens the national security. All the social networks Facebook, Twitter, LinkedIn, etc. are highly susceptible to malware activities. Twitter is one of the biggest microblogging networking platforms, it has more than half a billion tweets posted every day in average by millions of users on Twitter. Such a versatility and widespread use, Twitter easily get intruded with malicious activities. Malicious activities include malware intrusion, spam distribution, social attacks, etc. Spammers use social engineering attacks to send spam tweets, spam URLs, etc. This made Twitter an ideal arena for proliferation of anomalous spam accounts. The impact stimulates researchers to develop a model that analyzes detects and recovers from defamatory actions in Twitter. Twitter network is inundated with tens of millions of fake spam profiles which may jeopardize the normal user’s security and privacy. To improve real user safety and identification of spam profiles become key parts of research.

Monika Rokade and Yogesh Patil [11] proposed a system deep learning classification using anomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr. Yogesh Patil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy on KDDCUP and NSLKDD dataset.

Sunil S. Khatal and Yogeshkumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal.

Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogeshkumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatral and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly.

### III. COMPARATIVE ANALYSIS

This will be our first level of implementation, in which we will use four distinct methods to classify the dataset. Each algorithm's output will be displayed along with its own accuracy score. The following four algorithms will be used: LSTM employing Recurrent Neural Networks, Nave-Bayes, Support Vector Machine, and Random forest.

![Flowchart for Comparative Analysis](Figure 1 :Flowchart for Comparative Analysis)
Dataset:

The dataset used to test the model's performance was created by kaggle and contains 25000 news articles. Business, politics, science and technology, entertainment, and health were among the news categories included in this dataset. This Kaggle dataset was noisy and needed to be cleaned up. Id, title, author, content, and classification as "fake" or "genuine" were the major features included in each row of the data. The corpus was split into two datasets: training and testing. The training data contains a corpus of 20000 news articles, whereas the testing data contains a corpus of 5000 news items.

Data Pre-Processing

The data from the dataset was subjected to a variety of pre-processing procedures in this section. There was a lot of raw data in the kaggle dataset, including missing rows and columns. As a result, we must first process this data before dividing it into train and test data sets. Stopwords removal, stemming, tokenization, and POS tagging are some of the common data processing techniques we used in our project.

Stemming: In Natural Language Processing, Stemming can be referred to as a process of reducing different forms of a word to a core root. Words that are derived from one another can be mapped to a central word or symbol, especially if they have the same core meaning. This works as an information retrieval setting and boosts the algorithm's recall.

Tokenization: Tokenization is a process in which the sequence of string is broken into pieces such as keywords, words, phrases, symbols, etc. called as tokens. In the process of tokenization, some characters like punctuation marks are discarded. All characters within contiguous strings are part of the token.

Part-Of-Speech Tagging (POS): The POS tagging is a process of assigning corresponding part of speech like noun, verb, adjective, verb to each word present in the sentence. The tag may indicate one of the parts-of-speech, semantic information and so on. In our project POS tagging is applied to language grammatical rules to parse meanings of sentences and phrases present in our news corpus.

Feature Extraction

We've listed the many feature selection approaches we've used with the sci-kit learn python libraries in this section.

The Count Vectorizer is a basic tool for tokenizing a collection of text documents and creating a vocabulary of known terms, as well as encoding new documents using that vocabulary. The result is an encoded vector with the whole vocabulary's length and an integer count of how many times each word appears in the document.

IV. RESULTS AND DISCUSSION

In this section, we calculate the accuracies of the various models described in the comparison analysis and analyse the results. Confusion matrices can be used to calculate accuracy, precisions, and the f1 score. We created the graph in Figure 2 by plotting various algorithms on the X-axis and accuracy on the Y-axis. It is deduced that RNN has the maximum accuracy of 93 percent, followed by LSTM with a 90.3 percent accuracy, SVM with an 85 percent accuracy, and finally Nave Bayes with a 68 percent accuracy.
V. CONCLUSION

We describe a model for detecting fake news using a range of machine learning and deep learning methods in this research. Furthermore, we investigated the four alternative classifiers and compared their accuracies at the first level of implementation. The model with the highest accuracy score is RNN, which obtains a score of 93%. Fake news identification is a prominent and hotly debated research topic with a limited number of datasets. The current model, which we built, is tested against the existing dataset, suggesting that it performs well.

At the next level, we looked at real-time data from Twitter. Due to the RNN's inability to perform well over real-time tweets of a significant length, we used the logistic regression approach to train our model. The accuracy of utilizing Logistic Regression to classify tweets was found to be around 87%. In the future, n-gram models could be used in conjunction with classifiers to improve the accuracy and precision of real-time tweet classification. Another constraint is the Twitter dataset's size, which is limited to 500 tweets. This is a relatively tiny sample size, which has a significant impact on the test data accuracy ratings.

REFERENCES


INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH
IN SCIENCE | ENGINEERING | TECHNOLOGY

Impact Factor: 7.512

9940 572 462  6381 907 438  iijirset@gmail.com
www.ijirset.com