ISSN No:-2456-2165

# HAWKSEYE - A Machine Learning-Based Technique for Fake News Detection with IoT

Ann Maria Babu
Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, India

Catharine J P
Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, India

Divya K J
Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, India

Alisha Joffi
Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, India

**Abstract - Nowadays the tendency of people to believe in a piece of news that's coming on social media is very high and during this pandemic, it is more difficult to know if news heard is fake or not. The role of news in our lives has a great impact at present and also in the past years. Especially today, amid the pandemic, social media platform is being used to spread misinformation or the fake news at lightning speed and causes adverse effects in our lives. This approach helps to overcome this challenge and helps recognize or differentiate between true and false news. The data is collected and the content in the data is used for feature extraction using natural learning processing (NLP) by the technique of vectorizer. The extracted features are then classified using the algorithm passive-aggressive classifier a machine learning algorithm, here the input data successively approaches the algorithm and the machine learning algorithm is been upgraded one by one and not using the batch learning where the whole dataset is evaluated in one single step. This algorithm is suitable for huge datasets since this keeps updating the machine learning model at every step. The main challenge of this project is the real-time dataset collection and we are working on it. The output from the machine learning is then updated in IoT implemented NodeMCU an easy open-source platform for IoT application users and it is a hardware module with inbuilt Wi-Fi that is connected to the cloud so that the operators can access it and then using IoT the fake producers get notified as an alert that the news produced from their site is fake.**

***Keywords***:- *Fake News, vectorizer, Machine learning algorithm, IoT.*

## I. INTRODUCTION

In recent years, the eradication of fake news is becoming very difficult and has been adversely affecting the lifestyle of people. The fake news or the misinformation in the social media are proliferating day by day with profound implication

On the public disclosure, political integrity, election and so on. The potential for circulation, acceptance, and destruction of fake news poses them as one of the greatest threats to the concept of logical truth. Fake news hampers the Quality of Trust (QoT) applied to news, that is, how much a person trusts in the content of a particular source. Therefore, people lose their trust in the news that appears on social media.This leads people having the reluctance to accept news that is not fake too. The quality of news has decreased when compared to the traditional ones, resulting in large amounts of fake news. Detecting fake news becomes very important and should be taken care of with more attention due to the inimical effects on individuals and society. We perform classification on the dataset and therefore find if the news is fake or not.

The main motive of the project is to identify the fake news in the social network platform and help people to identify the fake and the real news.

Fake news can be divided into three aspects:
(i)Those of a purely swindling nature, whose intention is to deceive the reader by leading him to confusion.
(ii)Rumors, which are information with uncertain truth but publicly accepted.
(iii)Those with humorous character using sarcasm and irony.

The input dataset is collected from different sites and using the tf-idf vectorizer the feature extraction takes place that tokenizes the data, learn the data, and finds term frequency and the inverse document frequency to produce new data. The term frequency denotes the summarization of the data that how often a word comes in a document and also inverse document frequency refers to the reduction of the words they repeat frequently in the data. By using the machine learning algorithm on these extracted features. That is the common stop words such as "the", "where", "when", etc. are removed and only the words that have the least no of count can be included in the dataset.

Passive-aggressive classifier has used in this project as the machine learning algorithm for the classification of the data. here the input data successively approaches the algorithm and the machine learning algorithm is been upgraded one by one and not using batch learning where the whole dataset is evaluated in one single step. This algorithm is suitable for huge datasets since this keeps updating the machine learning model at every step Machine learning plays a major role in the classification process to develop the classification of the news on social media. Machine learning has many algorithms but after our analysis, we found out that passive-aggressive classifier has more accuracy and precision when a large dataset is been considered.

IoT is been used to send the output to the cloud and thereby send an alert message to the fake news source. There is a hardware module NodeMCU (inbuilt Wi-Fi) that connects to the cloud and allows access to the webserver users or operators. Therefore, using this information, the notification is been send by the operator.

## II. LITERATURE SURVEY

[1]In Mariam M. N. Aboelwafa and Karim G. Seddik base paper called machine learning-based technique for false data injection attacks detection in industrial IoT, it detects the FDI attack. The False data injection attack (FDI) creates false sensor measures in industrial fields. In this paper we detect the false data attack using the Autoencoders (AE), the performance of this method is better than the support vector machine. In the training time of detection using Autoencoders, they do not require labeled data and they can detect a wide variety of attacks. Attacks can modify the predefined situations these attacks can found using AE based attack detection algorithm. Autoencoders represent the set of data by removing the noise. This algorithm removes noise and preserves useful information of the state that we are processing with less occurrence of errors.

[2]D. Viji, Nikhil Asawa ,and Tanay burreja proposed a base paper based on Fake Reviews of Customer Detection Using Machine Learning Models. nowadays online marketing influences society a lot. For checking the quality of products in that particular site the customers depend on the reviews of that product. Because of the false review make the customer fell into the trap of the loss and they did not get the expected outcome that they imagine on that product. So that D. Viji, Nikhil Asawa ,and Tanay burreja proposed a method to detect the fake reviews posted on a particular site that we are checking using the amazon dataset. Amazon datasets contain product reviews and metadata from amazon. That Metadata comprises descriptions, price, sales rank, brand info, and co-purchasing link. It is done using Support Vector Machine and the accuracy of this is 84.88%

[3]In Sensitive Stylistic Approach to Identify Fake News on Social Networking Nicollas R. de Oliveira, Dianne S. V. Medeiros and Diogo M. F. Mattos proposed a method to detect fake news in the social media extracted text. For this, they selected the news from Twitter and checked the information is true or false. In their approach to this detection, they achieved 86% of accuracy with minimum overhead. In this paper, it uses three different methodologies to classify the real and false news. The first two methodologies implement the machine learning algorithm for unsupervised clustering and classification to predict the news. Then the third methodology expands the detection process considering the representation in the vector space of frequency word. The first step in the fake news revelation in the social media is extracting data from Twitter, then the three methodologies are implemented and the news is tested to detect fake or real.

[4] Fake News Detection using Passive Aggressive and TF-IDF Vectorizer introduced by Jayashree M Kudari, Varsha V, Monica BG ,and Archana R proposed a fake news detection method. This paper is giving more importance to fake news detection with their effects on social media and to differentiate between fake and real news. This paper says that passive- aggressive and TF-IDF vectorizer is efficient and through this, we get 90% accuracy. Passive-aggressive learning is the family of large-scale learning and they do not require any learning rate.

## III. EXISTING SYSTEM

In the existing system, we have provided only to detect fake news. The detection of fake news alone cannot stop the spread of fake news. There has to be some method to block the producers of such fake news. The is no such system in the existing system.

## IV. PROPOSED SYSTEM

The proposed system has a technology to identify the fake news and then send a warning to the person producing the fake news. If the person again spreads the fake news, then his details will be shared with higher authorities so that his account can be blocked. We are using Natural Language Processing (NLP) for feature extraction using the TFIDF vectorization technique. These extracted features are then classified using the algorithm "Passive-aggressive classifier". IoT is also implemented in which the command that is detected about news whether it is fake or not is given to node mcu then stored in the cloud and the fake news producer is notified by a warning.

Advantages of the proposed system:
•It helps to detect fake news with the highest accuracy.
•It gives warning to the people spreading the fake news for the first time.
•Provides the details of the people spreading the fake news on social media to the authorities so that action can be taken against them.

## V. METHODOLOGY

Our project contains a login wherein the user will log in through. The news that is to be identified is entered and therefore using the algorithm it displays if the news provided is fake or true. If the entered news is fake then a warning is given to the user and also displays the details of the fake news producer. These internal and external agents are referred to as actors. Use case diagrams consist of actors, use cases ,and their relationships. The diagram is employed to model the system/subsystem of an application. one use case diagram captures a specific functionality of a system. Hence to model the whole system, a variety of use case diagrams are used. Three actors are involved in the use case model illustrated in the figure (the user, user, and the authorities). The web user enters news, the algorithm is the program module that monitors the user's activities and reports appropriately and provides information in the news true or not, while the authorities display the activities of fake news for appropriate prosecution and also provide warning for them regarding the wrong news that's been generated.

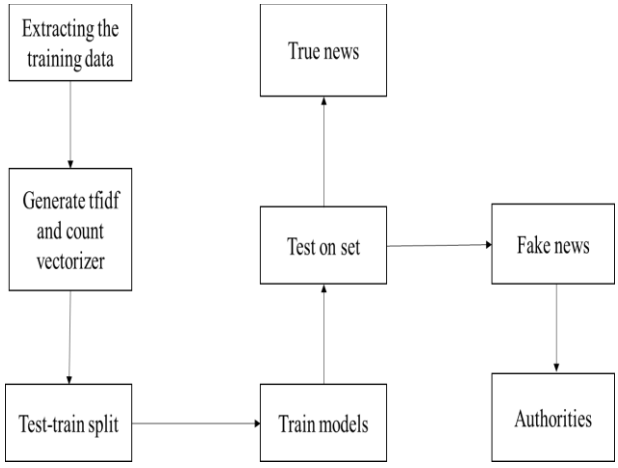

Figure 1. Block Diagram

### A. Machine Learning

Machine learning (ML) is that the study of computer algorithms that improve automatically through experience. Machine learning algorithms build model supported sample data, referred to as "training data", to form predictions or decisions without being explicitly programmed to try to do so. In this project first of all we extract the training data. Then we generate the tfidf and count vectorizer. Then the test-train data split is done. Now we train the models. After the training is completed, we give news as input. If the news is true, then it is displayed to the people. If it is fake, then the details are sent to higher authorities. In this project, we make use of passive- aggressive classifier as well as natural language processing.

a. Passive-aggressive classifier: Passive-Aggressive algorithms are generally used for large-scale learning. it's one among the few online-learning algorithms. Passive-Aggressive algorithms are somewhat almost like a Perceptron model, within the sense that they are doing not require a learning rate. However, they are doing include a regularization parameter.
b. Natural Language Processing: Natural Language Processing (NLP) may be a branch of AI (AI) that studies how machines understand human language. Its goal is to create systems that will add up text and perform tasks like translation, grammar checking, or topic classification. Companies are increasingly using NLP-equipped tools to realize insights from data and to automate routine tasks.

### B. Internet of Things (IoT)

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In our project, we implement IoT using a nodemcu to transfer the details of the fake news producer into an app. The nodemcu is a wifi module that can transfer data. Here we use an app so that the details about the fake news producer can be viewed by the authorities.

## VI. IMPLEMENTATION AND RESULTS

In this project, we have considered different algorithms and found out that passive-aggressive classifier gives the highest accuracy when compared to all other algorithms.

| Algorithm used | Accuracy |
|---|---|
| Autoencoders, SVM | 88% |
| Matrix Transformation | 86% |
| Passive-aggressive classifier | 92% |
| TF-IDF, SVM | 84% |

Table 1: Comparison of different models

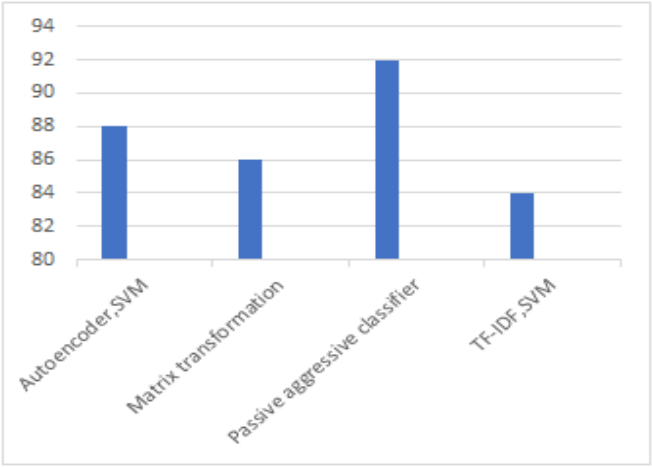

Figure 2: Graphical representation of accuracy

From both the table and the graph, we can understand that all other models have lesser accuracy when compared to the passive-aggressive classifier. So, we used this classifier in our project and obtained an accuracy of 92%.

## VII. CONCLUSION

The task of classifying news manually requires in-depth knowledge of the domain and expertise to identify anomalies in the text. In this research, we discussed the problem of classifying fake news using human knowledge. The data we used in our work is collected from the World Wide Web and contains news articles from various domains to cover most of the news rather than specifically classifying political news. In our project, we introduce a system for detecting fake news that is seen on social media. The machine learning concepts are used to distinguish between fake news and true news. Different algorithms are used to identify the characteristics of fake news. After the distinguishing process, the true news is only given to the people. Through this, we will be able to give the correct information and block the fake news from spreading through social media. The primary aim of the project is to identify patterns in text that differentiate fake articles from true news. So, we use machine learning techniques to check fake news using IoT. IoT is implemented in which the command that is detected about news whether its fake or not is given to node and then stored in the cloud and fake news producer is notified by a warning. Fake news detection has many open issues that require the attention of researchers. For instance, to reduce the spread of fake news, identifying key elements involved in the spread of news is an important step. Fake news plays a very major role in one's life and has detrimental effects so the eradication of fake news is very important. A fake news detection approach using the machine learning algorithm and tf-idf vectorizer provides more accuracy when compared to other machine learning algorithms. This approach enables to identification of the fake news produced and reduce them. IoT helps to send the notification to the fake news sources. The dataset that is been collected will be made more real-time by including the real time news as our future extension. Further up-gradation will be made in the future by blocking the site that produces the fake news.

## ACKNOWLEDGEMENT

This is an opportunity to express our sincere gratitude to all. At the very outset, we express our thanks to the almighty God for all the blessings endowed on us. We acknowledge our Sahrdaya College of engineering and technology for allowing us to do our project.

We express my sincere thanks to our Executive Director Rev.Fr. George Pareman, Principal Dr. Nixon Kuruvila for providing us with such a great opportunity. We also convey our gratitude to our Head of the Department Dr. M Rajeswari for having given us constant inspiration and suggestions.

We extend our deep sense of gratitude to our project coordinator Mr. Wilson Joseph, Assistant Professor of Computer Science & Engineering Department for providing enlightening guidance through the project. We can hardly find words to express our deep appreciation for the help and warm encouragement that we have received from our project guide Ms. Deepa Devassy, Assistant Professor of Computer Science& Engineering Department for her wholehearted support. We would also like to extend our appreciation to all other faculty members for their help and advice.

## REFERENCES

[1]. Mariam M. N. Aboelwafa, Karim G. Seddik,Senior Member, IEEE,Mohamed H. Eldefrawy, YasserGadallah,Senior Member, IEEE,and Mikael Gidlund,Senior Member- A Machine Learning-Based Technique for FalseData Injection Attacks Detection in Industrial IoT- 2020 IEEE
[2]. D. Viji, Nikhil Asawa and Tanay burreja -Fake Reviews of Customer Detection Using Machine Learning Models 2019 IEEE
[3]. Nicollas R. de Oliveira, Dianne S. V. Medeiros and Diogo M. F. Mattos,Member, IEEE – A Sensitive Stylistic Approach to IdentifyFake News on Social Networking- 2020 IEEE
[4]. Vectorizer Jayashree M Kudari, Varsha V, Monica BG and Archana R- Fake News Detection using Passive Aggressive and TF-IDF, 2020 IEEE
[5]. S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," Science, vol. 359, no. 6380, pp.1146–1151, 2018 IEEE
[6]. X. Zhou and R. Zafarani, "Fake news: A survey of research, detection methods, and opportunities," arXiv preprint arXiv:1812.00315, 2018 IEEE
[7]. W. Y. Wang, ""Liar, liar pants on fire": A new benchmark dataset for fake news detection," in Annual Meeting of the Association for Computational Linguistics - ACL 2017, 2017
[8]. Kushal Agarwalla, Shubham Nandan, Varun Anil Nair, D. Deva Hema–"Fake News Detection on Machine Learning and Natural Language Process"
[9]. Kai Shu , Amy Sliva , Suhang Wang , Jiliang Tang and Huan Liu-"Fake News Detection using Data Mining Perspective" Rodrigo Barbado, Oscar Araque, Carlos A. Iglesias
[10]. "A framework for fake review detection in online consumer electronics retailers",IEEE 2019.
[11]. Sepideh Paknejad, "Sentiment classification on Amazon reviews using machine learning approaches",2018.
[12]. Shaozhong Zhang and Haidong Zhong "Mining Users Trust from E-Commerce Reviews Based on Sentiment Similarity Analysis", IEEE 2019.
[13]. Muhammad Afzaal, Muhammad Usman, Alvis Fong "Tourism Mobile App with Aspect- Based Sentiment Classification Framework for Tourist Reviews", IEEE 2018.
[14]. Jitendra Kumar Rout, Kim-Kwang, Sambit Bakshi "Revisiting Semi-Supervised Learning for Online Deceptive Review Detection", IEEE 2016.
[15]. NiHaoung and Bin KhanDuo "Detecting spammer groups from product reviews", IEEE 2017

[16]. Jin Hankhao and Liayo Ganqui "A network based spam detection framework for fake reviews in online social media", IEEE 2017
[17]. Xu Yuang, Miingyang Sun, Zhikui Chen, Jing Gao, Peng Li "Semantic Clustering-Based Deep Hypergraph Model for Online Reviews Semantic Classification in Cyber-PhysicalSocial Systems", IEEE 2018
[18]. Ting Bai, Wanye Xin Zhao Member, IEEE, Yulan Jian-Yun Nie Member "Characterizing and Predicting Early Reviewers for Effective Product Marketing on E-Commerce Websites", IEEE 2018
[19]. Cagatay Catal , Suat Guldan "Product review management software based on multiple classifiers", IEEE 2017
[20]. Li Huoung and Miang Luhoui "Spammer Detection and fake user identification using social networks" , IEEE 2019
[21]. Faiza Masood, Ghana Ammad, Ahmad Almogen, Assad Abbas, Hasan Ali Khattak "Spammer Detection and Fake User Identification on Social Networks",IEEE 2019.
[22]. Yuanlin Chen, Yueting Chai , Yi Liu, and Yang Xu "Analysis of Review Helpfulness Based on Consumer Perspective" , Tsinghua Science and Technology, 2015
[23]. Tao Yin, Wenqi Wang, Wenhua Shi "A Study on Fraud Reviews: Incentives to Manipulate and Effect on Sales", China Communications, 2019
[24]. Rodrigo Barbado, Oscar Araque , Carlos A. Iglesias "A framework for fake review detection in online consumer electronics retailers", Information Processing and Managemen, 2017
[25]. Yusheng Zhou and Shuiqing Yang "Roles of Review Numerical and Textual Characteristics on Review Helpfulness Across Three Different Types of Reviews" , IEEE 2019.