IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

FAKE NEWS DETECTION USING MACHINE LEARNING

Binchu mol Abraham
Student,Dept of CSE
Sree Buddha College of
Engineering, Pattoor
Pattoor , India

Dr.Ajesh.F
Asst.Professor ,Dept.of CSE
Sree Buddha College of
Engineering, Pattoor
Pattoor, India

Abstract— Fake news detection from data streams is a challenging problem in today's information age. With the rise of social media and the Internet, false information spreads quickly and easily, leading to potential harm to individuals, societies, and even nations. This problem is particularly relevant during times of crisis, such as the COVID-19 pandemic, where accurate information is critical for public health and safety.In this context, fake news detection from data streams has become a topic of interest in research and industry. The goal of this project is to develop machine learning algorithms that can automatically detect fake news from data streams in real-time. This involves collecting data from various sources, such as social media platforms and news websites, pre-processing the data, selecting and training appropriate machine learning models, and evaluating the performance of the models.Some of the challenges of this project include dealing with noisy and unstructured data, handling a large volume of data in real-time, and addressing the issue of bias in the data. However, the potential benefits of successful fake news detection are significant, including increased trust in information sources, improved decision-making, and protection against malicious actors who spread false information for their own gain.Overall, fake news detection from data streams is a critical research topic with important implications for society. By developing effective detection methods, we can mitigate the spread of false information and promote a more informed and accurate public discourse.

Keywords—**Principle Component Analysis , MLP**

I. INTRODUCTION

Fake news has become a pervasive problem in the modern world, with the potential to mislead individuals and even sway public opinion. The spread of fake news is facilitated by the rapid growth of social media platforms, which provide a means for false information to be disseminated quickly and widely. This has led to growing concerns about the impact of fake news on everything from public health to political elections, and has spurred the development of new approaches to detecting and preventing its spread.

One of the most promising approaches to fake news detection is the use of machine learning algorithms, which can analyze and classify news articles based on their content. Machine learning has emerged as a powerful tool for identifying subtle differences in language, syntax, and other features that may indicate the presence of fake news. By training on large datasets of real and fake news articles, machine learning algorithms can learn to distinguish between the two and make predictions about the authenticity of new articles. There are several challenges associated with fake news detection using

machine learning, however. One of the main challenges is the difficulty of distinguishing fake news articles from real news articles, especially when the fake news is designed to mimic real news in terms of style, tone, and formatting. Another challenge is the need for large and diverse datasets of news articles, in order to train machine learning algorithms effectively. Additionally, machine learning algorithms must be constantly updated to adapt to new types of fake news and to maintain their accuracy over time. Despite these challenges, there has been growing interest in using machine learning for fake news detection, with researchers and practitioners developing a wide range of algorithms and models for this purpose. Some of the most popular machine learning algorithms used for fake news detection include Naive Bayes, Logistic Regression, and Support Vector Machines, among others. Each of these algorithms has its own strengths and weaknesses, and may be better suited to different types of fake news detection tasks. One of the key advantages of machine learning for fake news detection is its ability to learn patterns and make predictions based on large amounts of data. This allows machine learning algorithms to identify even subtle differences in language and other features that may indicate the presence of fake news. For example, some machine learning algorithms can analyze the presence of certain words or phrases that are commonly associated with fake news, while others can assess the overall sentiment of an article and compare it to other articles in order to determine whether it is likely to be fake or real. To train machine learning algorithms for fake news detection, researchers typically use large datasets of news articles that have been manually labeled as fake or real. These datasets may be obtained from a variety of sources, including social media platforms, news websites, and other online sources. Once a dataset has been obtained, it must be preprocessed in order to extract relevant features and prepare it for use in machine learning algorithms. There are several preprocessing techniques that may be used for fake news detection using machine learning, including text cleaning, tokenization, stemming, and stop word removal. Text cleaning involves removing any extraneous characters or symbols from the text, while tokenization involves breaking the text up into individual words or phrases. Stemming involves reducing each word to its base form, while stop word removal involves removing common words that do not carry significant meaning, such as "the" and "and". Once a dataset has been preprocessed, it may be used to train and test machine learning algorithms for fake news detection. Researchers typically use a range of metrics, such as accuracy, precision, and recall, to evaluate the performance of these algorithms. In general, machine learning algorithms have shown promising results for fake news detection, with some studies reporting accuracy rates of up to 95%. Overall, fake news detection using machine learning is a rapidly evolving field, with new algorithms and models. Recently, more websites are being created that are trying to help assess the accuracy of the information, the so called fact-checkers. Unfortunately, it is not possible to check them manually with such a massive amount of new messages. Hence, more and more hope is placed in automatic fake news.The main reason for the rapid increase in the use of disinformation is the ability to use not only traditional mainstream media but also social media, like Twitter or Facebook. It is worth noting that its popularity can rapidly grow according to the rule that false news spreads faster and more comprehensive.Its extensive spread has a severe negative impact on media users and society. The main goal of publishing such information with malicious content is to attract readers, which could increase publisher rank and popularity, which consequently increases revenues form adds. The main contributions of this paper are as follows:Formulating the problem of fake news detection as a data stream classification task. Proposing a novel pattern classification methods based on feature extraction techniques, which address the detection of fake news in streaming data from social media .An extensive experimental analysis backed-up by the statistical tests.

SOCIALTRUTH PLATFORM ARCHITECTURE

The proposed machine learning solutions constitute text verification services, one of the critical elements of the Social Truth platform. From a broader perspective, it is crucial to explain the environment where the proposed solutions will operate and how they will bring benefits for the end-users, which are all kind of actors that need to cope with fake news challenges. The technology stack has been decomposed into the following logical elements physical elements (nodes) and their orchestration, verification services, messaging and event processing.

Physical nodes comprising the system

The first and the most bottom layer in the technology stack constitutes the orchestration framework. It is laid down on top of an infrastructure composed of virtual and hardware machines. This layer is intended to implement automated resource management, and thus it facilitates the entire platform with such capabilities as flexibility, scalability, and fault tolerance

.

Verification services

All the fake news detection mechanism (presented in this paper) are the instances of text verification services. As such, they are the critical building blocks of the system and are deployed as a micro-services. Micro-service is an independently deployable component, which is packed as a Docker container. In the proposed architecture, we heavily use asynchronous event-based communication in favour of synchronous calls. This allows us to avoid tight coupling between the verification services and other components in the platform. In that regard, each verification service subscribes to a dedicated topic and produces results on another one.

Messaging and event processing

From the architectural point of view, Apache Kafka constitutes a flexible and efficient way to integrate all the components, both existing tools as well as the new ones developed during the project or by the community. on top of the Apache Kafka system, we deploy the Complex Event Processing (CEP) engine. We use it to preprocess the data before storing and presenting it to the end-user or the verification service. For example, we use this technology to join data streams produced by verification services belonging to the same type. In that regard, we can present the user analysis results obtained from different classifiers.

II . RELATED WORKS

The paper " Fake News Detection on Socialmedia "[1] briefs that Among the standard solutions present in the research, we may distinguish the analysis of creators and readers of texts,document content, stylometric analysis and verification of positioning the document in social networks by using feature extraction technique. The main goal of publishing such information with malicious content is to attract readers, which could increase publisher rank and popularity, which consequently increases revenues form adds. It is worth mentioning that there is no single definition of what fake news is and what it is not. Interesting are studies analyzing which types of attributes prove to be useful in the context of fake news classification . Among the standard solutions present in the research, we may distinguish the analysis of creators and readers of texts, document content, stylometric analysis and verification of positioning the document in social networks [2]. Image analysis that focuses on false video information is also a promising approach [3]. Equally interesting seems to be the work of Conroy at al. [4] proposing a distinction between approaches to linguistic (semantic, rhetorical, discourse and simple probabilistic recognition models) and social (analysis of the author's behaviour within the social network or analysis of the built context by all of his posts). Castillo et al. [5] bases the construction of recognition models on users' behaviour in the context of posting and forwarding content depending not only on their content but also references to other documents. Ferrara et al. [6] analyze various data representations, and Afroz et al. [7] different variations of stylometric metrics. Sharma et al. [8] discussed several topics related to the problem in question and pointed to the possibility of using the SCAN (Scientific Content Analysis) method to solve it. Jin et al. [9] proposed the compelling approach for the task of automatic news verification, departing from text analysis in favour of image data. Zhang et al. [2] pointed to the dynamic nature of social media messages and proposed analysing them in the context of streaming data. Horne and Adali [10] employed SVM to distinguish between fake, authentic and satire messages. This kind of classifier has also been used by Cheng et al. for users classification, using semantic analysis and behavioural feature descriptors to detect potentially fake online posts [11]. Interesting comparative studies by Gravanis et al. [12] evaluated several linguistic features based classification approaches.They presented the results showing that known classifier models, especially ensembles, may be successfully used as fake news detectors. Bondielli et al. [13] pointed out that while anomaly detection and clustering methods could be used for fake news detection, this problem is usually reduced to the classification task. Atodiresi et al. [14] considered an NLP tools-based approach to tweet analysis. The authors defined this problem as a regression task and thus were able to assign a credibility value to each message.Unfortunately, in most works, the authors consider the problem of fake news detection is a classic problem of data analysis, without taking into account their streaming nature. What is more, it should be taken into account that the profile of messages classified as fake news may change over time,i.e., we are dealing with a phenomenon known as concept drift. This is since, as with other information security problems, such as the detection of unwanted mail, the authors of fake news are aware that publishing them is becoming more difficult because automatic detection systems will detect them. Thus, it can be expected that their profile will change over time to deceive these systems, and therefore requires authors of these types of systems to equip them with mechanisms for adapting to changes in probabilistic characteristics of the fake news detection task. This work will attempt to develop fake news detection algorithms based on a data stream where we will not assume its stationary nature [15]. To the best of the authors' knowledge, there is no work treating fake news detection as a problem of streaming data classification. Although some authors note that social media data are of such nature, only Wang and Terano [16] use techniques adequate to analyze data streams. However, their approach is limited to relatively short streams and does not potentially take into account the nonstationary nature of the data.

III PROPOSED SYSTEM

The proposed solution uses a combination of news checker, as well as Artificial Intelligence algorithms. A thousand attributes of a learning set constitute a problem of very high dimensionality. Many features may show mutualstatistical dependence, and many of them may prove to be utterly unimportant in the context of the classification problemunder consideration, showing no relationship with the actual problem labels

a) PCA: The first considered strategy was the Principal Components Analysis. For the set of observations, the coordinate system is rotated in such a way as to maximize the variance of subsequent attributes. It leads to an increasing percentage of the explained variance. It allows the transformation of data to representations with a lower number of features than the input set by the combination of real attributes of the problem. It is a state-of-art solution to extract features for multidimensional data.

b) COUNT VECTORIZER: The second method used in experiments is based on the base approach of feature extraction– Count Vectorizer. To take into account the same impact of document titles and content, each of the subsets of features was normalized using the standard normalization, followed by the selection of the features represented by the most significant number within the data used to construct the extraction model. Each of the considered methods of reducing the feature space, due to the streaming nature of the processing, was implemented in the form of a model fitted based on the first portion of data supplied to the classification system

c) FEATURE SELECTION: The last method used was a filter-based feature selection. Methods from this group use statistical techniques to assess the relationship between each feature and problem classes [17]. The scores obtained are then used to select the most significant features. In this case, as the correlation measure, the Chi-Squared test was used. Strategies to train the classifier on a data stream: Each of the three proposed dimensionality reduction strategies was analyzed in three different state-of-art methods for constructing classification models in data streams.

a) Streaming Ensemble Algorithm (SEA): Proposed by Street and Kim in [18], SEA constructs a classifier ensemble of a fixed size, by training a new base classifier on each observed data chunk. This approach is separate from the commonly used approaches with updated models [19]. In case of exceeding the fixed pool size, the worst performing model according to a given metric is removed. The final decision of the ensemble is produced according to the sum rule [20].

b) Online bagging (OB): Ensemble learning algorithm proposed by Oza in [21] and based on offline Bagging. It maintains a classifier pool in which, with the arrival of the new sample, each base estimator is trained on it K times, where K comes from the Poisson($\lambda = 1$) distribution

.

c) Single model (SM): In addition to the classifier ensembles, the natural ability of selected classifiers to adapt to partial fitting was also tested, where a single model is constructed. However, each incoming data chunk is used to modify its properties with knowledge acquired based on a new class distribution. This approach, apart from the classifiers that effectively provide the forgetting mechanisms, is not immune to the concept drift phenomenon. Nevertheless, unlike ensemble methods, it is not strongly dependent on the size of a single chunk of data used in processing [22].

C. Base classifiers for data stream processing Each of these processing methods also requires the selection of a base classifier, which – due to the consideration of processing using single models – must meet the requirement to be able to conduct a partial fit of the already built recognition model. Three classification algorithms meeting this condition were selected.

- GNB Gaussian Naive Bayes – without prior probabilities,
- MLP Multi-layer Perceptron – with one hidden layer build

on 100 neurons, using ReLU activation function and stochastic gradient-based optimizer.

- HT Hoeffding Tree – using gini split criterion and Naive

Bayes Adaptive prediction mechanism.

The entire experimental evaluation was implemented using Python libraries, based on the scikit-learn [23] module in the implementation of two base classifiers and all feature reduction methods, on the stream-learn [24] module in data stream processing,calculating evaluation metrics and employed classifier ensembles of stream processing and on the scikit-multiflow [25] module in the implementation of Hoeffding Tree. The implementation of the analyzed processing methods, supplemented with a module of datastream generation prepared following the description of static data included in Section II, together with the analytical script used to generate all tables and illustrations contained in the following section, is publicly available on the GIT repository During the process of methods evaluation, the state-of-art Test-Then-Train methodology was used, which involves alternating testing of algorithms on an incoming portion of data, which has not yet been made available to the classifier for the needs of learning and updating its model after supplementing it with original labels. Two hundred fifty patterns were adopted as the size of a single chunk. Each of the three feature extraction methods has been paired with each of the three stream processing strategies built on each of the three considered base classifiers, assuming 2, 10, 50, 100, 200, 500 or 1000 extracted attributes for the construction of the classification model, which resulted in 189 runs being the basis of the evaluation. Due to the balanced nature of the problem, the results are presented using the accuracy metric, being appropriate for this kind of data. The OB strategy seems to be far less suited for reduction by FS than SEA. The best results are achieved, again by the MLP classifier used as the base, using the PCA method. In this case, for a combination of PCA, OB and MLP with 1000 attributes generated, we achieve the highest average classification value of 81 per cent among the experiments carried out. An interesting difference between the SEA and OB approaches is that GNB rarely goes beyond the level of the random classifier for the latter and PCA reduction. On the other hand, in the case of CV and FS, GNB is characterized by a steady increase in classification ability, directly dependent on the number of problems features. HT properties do not differ from those developed by the SEA strategy. The use of SM in the classification reveals the weakness of the PCA algorithm in tandem with GNB, further reducing the quality of such a solution. However, it can be seen that the same reduction with the MLP algorithm leads to the best results among all SM-base strategies. In this case, the CV extraction does not meet the expectations, in any of the tested instances leading to the best solution, which is evenly distributed between PCA and FS. Summing up the analysis of the results obtained, it can be stated that the most effective of the considered classification algorithms is MLP. One may see a simple linear relationship between its generalization ability and the attributes number of the constructed model, almost regardless of the used extraction method and processing strategy. Obvious observation for all approaches is also quite the

inverse relationship that occurs for HT, whose quality of classification degenerates with the increase in the dimensionality of the problem. GNB and PCA can be considered as the worst combination of streaming approaches, especially for OB and SM. MLP classifier with OB and PCA should be distinguished as the best combination of all analyzed strategies to deal with dimensionality reduction in fake news data stream processing. As we noticed in the introduction to the following work, the overwhelming majority of machine learning research in the field of fake news detection relies on the extraction of linguistic features. The main subject covered in the study presented in this work is, however, the analysis of approaches to feature extraction for the needs of the data stream classification task for the problem above. At the entry point, each of the patterns constructing the stream, representing individual articles, contains a thousand attributes determined by a simple solution of Count Vectorizer – applied to isolate the impact of diverse linguistic analysis methods on the quality of results achieved. The dataset developed for the experiment is based on the Getting Real about Fake news set, containing 13,000 articles marked as fake news by BS Detector Chrome Extension users. In each of them, we have the title, content and timestamp. To develop the classification model, it was supplemented with the same number of articles from sources commonly considered to be verified and reliable, selected in a similar period indicated by timestamps of data from the original set. The dataset developed in this way was then ordered following the publication dates, to develop a data stream enabling to perform the reliable experiments

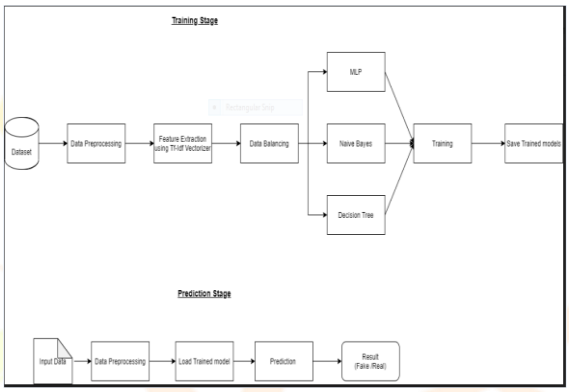

Figure1: Proposed System Architecture

The proposed machine learning solutions constitute text verification services, one of the critical elements of the SocialTruth platform. From a broader perspective, it is crucial to explain the environment where the proposed solutions will operate and how they will bring benefits for the end-users, which are all kind of actors that need to cope with fake news challenges. dedicated crawlers (data connectors) that send data over the binary protocol to the Apache Kafka framework. The Apache Kafka is a distributed streaming platform implementing thepublish-subscribe model. Once the ingested data is published to one of the Kafka topics, it can be simultaneously consumed by various verification services and stream processing applications. Once the services When the services finalize their computations, they make the results available on another Kafka topic, which can be consumed by other services again. Such kind of processing pipeline is called choreography pattern. When the services finalize their computations, they make the results available on another Kafka topic, which can be consumed by other services again. Such kind of processing pipeline is called choreography pattern. It is a contradiction to the orchestration pattern, which introduces a central entity (orchestrator) controlling the execution of each stage in the pipeline. These two approaches have their advantages. We use a mix of both when implementing web service handling the HTTP requests. As we mentioned before, in the described system, we have adapted Apache Kafka. It is a distributed streaming platform, which enables both real-time event processing and event driven communication between various components. From the architectural point of view, Apache Kafka constitutes a flexible and efficient way to integrate all the components, both existing tools as well as the new ones developed during the project orby the community

IV. CONCLUSION

.

It is one of the first work which treats the problem of fake news detection as the stream data classification task and also takes into consideration that the characteristics described the incoming messages could change over time. Studies of this type have not been represented widely in the literature so far, so it is a preliminary analysis of the effectiveness of typical methods of feature reduction and the construction of stream models for an entirely new problem. Extensive experimental research on several algorithms from each of the considered aspects of processing confirmed the possibility of constructing systems of this type in an application for data with a stationary nature of the concept, suggesting extraction using the Principal Components Analysis algorithm in the construction of Online Bagging ensemble encapsulating the Multi-layer Perceptron base classifier. Summing up the analysis of the results obtained, it can be stated that the most effective of the considered classification algorithms is MLP. One may see a simple linear relationship between its generalization ability and the attributes number of the constructed model, almost regardless of the used extraction method and processing strategy. The research presented in work will be continued by considering subsequent analyzes also data dynamics both in prior and posterior probabilities, taking into account different variants.

REFERENCES

[1] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake news detection on social media: A data mining perspective," SIGKDD Explor. Newsl., vol. 19, no. 1, pp. 22–36, Sep. 2017.
[2] X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization, detection, and discussion," Information Processing & Management, 2019.
[3] M. Chora´s, A. Giełczyk, K. Demestichas, D. Puchalski, and R. Kozik, "Pattern recognition solutions for fake news detection," in IFIP International Conference on Computer Information Systems and Industrial Management. Springer, 2018, pp. 130–139.
[4] N. Conroy, V. L. Rubin, and Y. Chen, "Automatic deception detection: Methods for finding fake news," Proceedings of the Association for Information Science and Technology, vol. 52, pp. 1–4, 01 2015.
[5] C. Castillo, M. Mendoza, and B. Poblete, "Information credibility on twitter," in Proceedings of the 20th International Conference on World Wide Web, ser. WWW '11. New York, NY, USA: ACM, 2011, pp. 675–684.
[6] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," Commun. ACM, vol. 59, no. 7, pp. 96–104, Jun. 2016.
[7] S. Afroz, M. Brennan, and R. Greenstadt, "Detecting hoaxes, frauds, and deception in writing style online," in Proceedings of the 2012 IEEE Symposium on Security and Privacy, ser. SP '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 461–475.