Journal of Physics:
Complexity

PAPER • **OPEN ACCESS**

Advancing fake news detection with graph neural network and deep learning

To cite this article: Haji Gul *et al* 2025 *J. Phys. Complex.* **6** 025001

Journal of Physics: Complexity

OPEN ACCESS

RECEIVED
23 December 2023

REVISED
16 April 2024

ACCEPTED FOR PUBLICATION
27 August 2024

PUBLISHED
2 April 2025

PAPER

Advancing fake news detection with graph neural network and deep learning

Haji Gul[1], **Feras Al-Obeidat**[2], **Muhammad Wasim**[3], **Adnan Amin**[1,*] and **Fernando Moreira**[4]

[1] Center for Excellence in Information Technology, Institute of Management Sciences, Peshawar 25000, Pakistan
[2] Zayed University, Abu Dhabi 51133, United Arab Emirates
[3] City University of Science and Information Technology, Peshawar 25000, Pakistan
[4] REMIT, IJP, Universidade Portucalense Porto, Portugal & IEETA, Universidade de Aveiro, Aveiro, Portugal
[*] Author to whom any correspondence should be addressed.

E-mail: adnan.amin@imsciences.edu.pk, hajigul1993@gmail.com, feras.al-obeidat@zu.ac.ae, muhammadwasim443@gmail.com and fmoreira@uportu.pt

Keywords: natural language processing, fake news detection, graph neural network, deep learning

Abstract

In the modern era of digital technology, the rapid distribution of news via social media platforms substantially contributes to the propagation of false information, presenting challenges in upholding the accuracy and reliability of information. This study presents an updated approach that utilizes graph neural networks (GNNs) alongside with advanced deep learning techniques to improve the identification of false information. In contrast to traditional approaches that primarily rely on analyzing text and assessing the credibility of sources, our methodology utilizes the structural information of news propagation networks. This allows for a detailed comprehension of the interconnections and patterns that are indicative of misinformation. By analyzing the intricate, graph-based connections between news items, our approach not only overcomes the constraints of conventional fake news detection methods but also demonstrates significant enhancements in detection accuracy. This paper emphasizes the revolutionary nature of utilizing GNNs in the field of fake news detection. It also examines the potential consequences of our research in reducing the propagation of false information. Our model achieved an impressive accuracy rate of 97%, demonstrating a significant improvement in its ability to identify and classify fake news.The findings highlight the substantial improvement in the ability to detect fake news provided by GNNs in comparison to traditional methods, demonstrating promising growth in the struggle against false information.

1. Introduction

Fake news on social media and various other media is widespread and is a matter of serious concern due to its ability to cause a lot of social destructive impacts [19, 41]. There has been a rapid increase in the spread of fake news in the last decade [17]. Such a spread of sharing articles online that do not comply with facts has led to many problems covering various domains like politics, sports, health, and science [23, 40]. One such area affected by fake news is the financial markets [20], where a rumor can have disastrous consequences and may bring the market to a standstill. Previously, in the field of fake news detection, there were multiple methods to detect fake news. NLP is one of the methods that were previously used for fake news detection [2]. The NLP rating of an algorithmic system enables the combination of speech understanding and speech generation. Additionally, naive bayes uses probabilistic reasoning to determine whether news stories are likely to be authentic or fraudulent based on feature independence assumptions [14]. By combining the predictions of several decision trees, random forest, an ensemble learning technique, improves accuracy and robustness and successfully separates false information from true information [39]. Support vector machines (SVMs) are useful for classifying news articles by extracting pertinent features, since they are good at generating appropriate decisions [3]. By combining the interpretability of logistic regression (LR) with the

feature learning power of neural networks (NNs), LR paired with NN offers a sophisticated method of detecting fake news [31]. Lastly, because recurrent NNs (RNNs) are adept at processing sequential data, they can better detect minor patterns that point to fake news by capturing the temporal dynamics of news stories and user interactions [27]. Conventional approaches to identifying fake news have predominantly relied on NLP and machine learning methods, with a particular focus on analyzing text and assessing the credibility of sources. Although these methods have laid a solid foundation for initial endeavors to eliminating false information, they typically fail to effectively tackle the complex and continually evolving nature of news dissemination on social media. The constraints of current methods emphasize the necessity for inventive solutions that can unwrap the complex network of connections within data, which is crucial for accurately differentiating between authentic and deceptive information [42].

This study introduces an innovative methodology for identifying fake news through the utilization of graph NNs (GNNs), a state-of-the-art deep learning technique known for its proficiency in analyzing data that possesses inherent graph structures. Our contribution encompasses two main aspects. Firstly, we present the utilization of GNNs in the domain of fake news detection, which represents a notable departure from conventional text-based analysis techniques. Additionally, we utilize the relational information pertaining to news items, their paths of dissemination, and the interactions among users in order to improve the process of detection. This methodology not only facilitates a more intricate comprehension of the dissemination of false information but also enhances the precision of identification by capturing patterns that may not be readily apparent exclusively through textual analysis. Our approach overcomes these challenges by employing an advanced feature extraction procedure that encompasses both the substance and the circumstances of news articles. The utilization of GNNs when combined with deep learning principles, allows for the exploitation of graph-based representations to effectively analyze the interconnected inherent in social media data. This novel methodology not only differentiates our research from current approaches but also establishes a fresh standard for the utilization of GNNs in the domains of information verification and fake news detection. The key technical challenge faced in our proposed methodology pertains to the efficient depiction and utilization of graph-based data for the purpose of detecting fake news. Conventional deep learning models lack inherent architectural capabilities to effectively process graph structures, thereby posing a significant obstacle in capturing the intricate interconnections and dynamics inherent in social media networks. In response to this issue, we have created an enhanced GNN structure that can effectively handle graph-structured data. This allows the model to acquire knowledge and recognize the distinct patterns associated with the spread of fake news. The uniqueness of our study lies in the utilization and modification of GNNs to address the particular issue of identifying fake news. The area has traditionally been dominated by text-based analysis and traditional machine learning models. We expand the limits of what can be accomplished in identifying misinformation by providing a strong framework that can adjust to the changing nature of news distribution in digital environments. The findings of our study illustrate the unparalleled effectiveness of our approach compared to conventional methods, presenting a hopeful alternative for future research and practical implementations in the ongoing struggle against false information. The main objectives of our work are highlighted below:

- We Performed a comparison of GNN and traditional classifiers such as decision trees, Naive Bayes, random forest, SVM, LR, NN, and RNN.
- We investigated the ability of GNNs to capture intricate connections among news articles, which are depicted as nodes in a graph.
- We highlighted the potential of GNN to comprehend complex connections within news data, resulting in enhanced precision and forecasting.

2. Literature review

Social media, as an autonomous platform, is the main source of fake news circulation. Users can spread false information by themselves or using bots [15, 16, 22]. Bots are algorithms that use matching input and associated response patterns to carry out particular tasks. Bots distribute bogus news in large quantities to make it seem credible because consumers typically believe everything they read online.5 Because those tales typically garner more attention than other stories, users are also more likely to share them. Additionally, those stories typically have more likes or comments. An additional factor in determining a user's liking to a topic is their emotions and feelings toward it [34]. According to MIT researchers, since people are just as interested in this activity as the bots, fake news spreads more quickly than genuine news [24, 43]. Within the research focusing on enhancing the identification of fake news using GNNs and deep learning, it is crucial to distinguish between 'fake news' and 'biases,' since they both have important functions within the disinformation ecosystem, although in distinct ways [13]. Fake news refers to deliberately invented material

that is spread to deceive or mislead. It is characterized by a total absence of factual accuracy and is generally created to manipulate public opinion or generate financial gain by using sensationalism. Biases, in contrast to fake news, are predispositions or subjective leanings that may impact the perception and spread of news items. Biases, while not intrinsically involving the dissemination of erroneous information, may result in a distorted portrayal of facts, where certain elements are emphasized to support specific perspectives or agendas. The correlation between fake news and biases adds complexity to the misinformation ecosystem. Fake news erodes public discourse and trust by disseminating falsehoods, while biases can distort the public's comprehension of factual information, potentially bolstering the credibility of false narratives or exacerbating societal divisions. Recognizing the complex nature of the situation, the research highlights the need to identify false information by not just confirming its accuracy but also comprehending the biased ways it is presented and the structural patterns through which it spreads. This method emphasizes the complex task of differentiating truth from disinformation, taking into account both the immediate effects of fake news and the gradual effects of biases on public perception [8].

2.1. Combating fake news

Misinformation is a long-existing problem, and its impact spans across technological and political spheres. It's crucial to address this issue because the increasing dependence on social networking sites for daily news is a continuous upward trend due to technological availability, and there's no indication of a decline soon. The tech giant Facebook has already taken steps to combat the circulation of misinformation on its website in some countries, partnering with third-party fact-checkers to review articles and posts and assess their accuracy. Identified fake news content is pushed down in the news feed, and action is taken against repeat offenders [25]. Previous approaches to halting the dissemination of false information have primarily concentrated their investigation on fake news articles spread by automated systems. Social media accounts that publish false material more frequently than real accounts are generally referred to as bots; they have a strong tendency to share unrelated content. Users who exhibit power over others—especially their social media followers—are their main targets. It was noted that the bots used to spread false information to the intended audience were usually active during the initial phases of the spread of fake news, drawing in like-minded individuals who subsequently shared the same content on social media [36]. Similarly, research indicates that social bots often populate the social space to inflict harm and deceive social media users. They have also been employed to induce political disruptions, negatively impact the stock market, engage in personal information theft, and propagate misinformation [11]. The main issue arises with the dynamic nature of the network [16]. Since the network deals with real-time data, it is necessary to control the diffusion of rumors early in the process [45]. One of the approaches to halting the dissemination of rumors was identifying their source [37]. The identification of a proper diffusion model led to an analysis of the pace at which fake news spreads. Then, based on the source, the antirumor—based approach (for a single source) or the approximation-based approach (for multiple sources) was employed to tackle the spread of rumors in the network.

2.2. Machine learning approachs

Several algorithms have been put to the test to see how well they identify false reports from unreliable sources. These algorithms, which have achieved higher accuracy, consist of the following:

2.2.1. Decision tree

A flexible supervised machine learning technique for both regression and classification applications is the decision tree [38]. Starting with the full dataset at the root node, it chooses the optimal feature for partitioning according to factors like Gini impurity or information gain. Recursive splitting continues in this manner until certain conditions are satisfied, like reaching a maximum depth or a minimum number of samples. Final predictions are stored in leaf nodes, and the resulting tree gives understandable if-else rules. Decision trees are useful in ensemble methods like random forests, where they improve robustness and performance even if they are prone to overfitting, which can be reduced via approaches like pruning. The decision tree can be represented as a set of rules

$$\text{Decision at node } n: \begin{cases} \text{If } X \leqslant T, & \text{then go to node } L, \\ \text{If } X > T, & \text{then go to node } R. \end{cases} \tag{1}$$

X_j represents the value of a specific feature in the input vector X, T_j is the threshold for the feature X_j at a particular node and The process continues recursively in the left or right sub-tree until a leaf node is reached. At a leaf node, the predicted output is denoted as y.

2.2.2. Naive Bayes

Naive Bayes is a probabilistic machine learning algorithm commonly used for classification tasks, especially in text-related applications like spam detection [21] or sentiment analysis [1]. Using prior knowledge about relevant conditions [35], the Bayes theorem is utilized to compute the probability of an event. To make the computation of probabilities easier, Naive Bayes posits conditional independence between features given the class label in the context of classification. For a given observation, the algorithm calculates the probability of each class and assigns the class with the highest probability to the observation. Despite its simplicity and the 'naive' assumption, Naive Bayes often performs well, particularly in text classification tasks, making it a popular choice for various applications. The Naive Bayes can be represented as

$$y = \text{argmax}\,(y)\, P\,(Y = y|X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) \tag{2}$$

where $P(Y = y)$ is the prior probability of each class, $P(X_1 = x_1|Y = y)$ is the class conditional probabilities of each feature given the class and argmax(y) is the function used for selecting the class with the highest estimated probability among the possible class labels.

2.2.3. Random forest

Random forest, an ensemble learning technique for classification and regression, constructs numerous decision trees during training, each based on a bootstrap sample of the original dataset [30]. Utilizing random feature selection at each node introduces diversity. These trees, grown to a specified depth or until a stopping criterion is met, collectively form the 'forest.' In prediction, for classification tasks, individual tree predictions are combined through majority voting, while for regression tasks, predictions are averaged. Random forest is well known for its capacity to manage outliers, guarantee high accuracy, and lessen overfitting while providing insights into the significance of individual features. It's become a widely used tool in the field of machine learning, with many different applications, including image classification [5], medical diagnosis [10], and financial prediction [33]. The random forest can be represented as:

$$Y_{\text{ensamble}}\,(X) = \frac{1}{T}\sum_{t=1}^{T} Y_t\,(X) \tag{3}$$

where $Y_t(X)$ is the prediction of D_t and T is the total number of trees.

2.2.4. SVM

The supervised machine learning technique known as SVM was developed to handle tasks related to regression and classification [28]. The principle of operation is determining the best hyperplane and optimizing the margin between classes to create a clear division. Support vectors are crucial to this procedure because they define this ideal boundary by showing which data points are closest to the hyperplane. The kernel trick demonstrates SVM's ability to handle non-linear decision boundaries, allowing implicit operations in higher-dimensional domains. The algorithm's performance is good even in highdimensional areas and it is resistant to overfitting, which makes it useful in a variety of contexts. On the other hand, it can be computationally demanding for big datasets and susceptible to noise in the data. SVM is used in many different fields, including text classification [4], image recognition [29], and bioinformatics [7], because of its capacity to manage challenging classification issues. SVM can be represented as:

$$y_i\,(w \cdot X_i + b) \geqslant 1 \tag{4}$$

where y_i is the class label of the ith data point, X_i is the feature vector of the ith data point.

2.2.5. LR with NN

Using LR as the output layer in a NN intended for binary classification tasks is known as LR with NN [44].. An input layer, hidden layers with activation functions, and an output layer with a single LR unit employing a sigmoid activation function are the three layers of a NN. The output is compressed by the sigmoid function and limited to a range of 0–1, which represents the probability of falling into the positive class. Using binary crossentropy loss and optimization techniques, the network modifies its weights and biases throughout training to reduce the difference between expected probability and actual class labels. For situations involving binary classification, integrating LR—typically a stand-alone algorithm—into a NN works well. It is possible to identify complex patterns in the data thanks to this integration. It can be represented as

$$z = w \cdot X + b \tag{5}$$

$$\sigma(z) = \frac{1}{1 + e^{-z}} \tag{6}$$

where X represents the input features, w is the weight vector, b is the bias vector, z is the weighted sum of inputs, and $\sigma(z)$ is the sigmoid activation function.

2.2.6. GNN

An instance of a unique NN designed specifically for handling graph-structured data is a GNN. In graphs, entities are represented as nodes and their relationships as edges. GNNs aim to obtain embeddings for each node, which capture inherent characteristics as well as relationships with neighboring nodes [18].. Through message-passing protocol, nodes enable the sharing of data with their neighbors and subsequently aggregate those neighbors' representations. Graph convolutional layers are used for these functions in notable architectures such as graph convolutional networks (GCNs). Applications for GNNs can be found in many different fields, including social network analysis [9], recommendation systems [12], and molecular chemistry [6]. Tasks including node classification, graph classification, link prediction, and recommendation demonstrate their efficacy and emphasize how well they can capture complex dependencies in graphstructured data. GNN can be represented as

$$m_i^{(l+1)} = \sum_{j \in N(i)} h_j^{(l)} \cdot W^{(l)} \tag{7}$$

$$h_i^{(l+1)} = \sigma\left(m_i^{(l+1)} + h_i^{(l)} \cdot W_{\text{self}}^{(l)}\right) \tag{8}$$

where $m_i^{(l+1)}$ represents m_i in layer $l+1$, $h_i^{(l+1)}$ represents h_i in layer $l+1$, $W^{(l)}$ represents W for layer l, $W_{\text{self}}^{(l)}$ represents W_{self} for layer l, $N(i)$ denotes the set of neighboring nodes of v_i and $\sigma(\cdot)$ is the placeholder for choose activation function.

3. Material and method

This method uses mathematical formulas to represent the steps that are carried out in the GNNs architecture to systematically detect fake news. The process uses layers of NN and graph-based representation learning to modify node properties such that they match the graph structure and categorize articles as bogus or real. An incremental process is involved in integrating GNN to identify bogus news. The methodology execution diagram is given in figure 1. Node Characteristic X_i is a node feature that represents the content of each article in creation. This could involve using other numerical representations, such as embeddings. then make a graph. G can be described as $G = (V, E)$, where V represents the set of nodes (articles) and E represents the set of edges (relationships between articles). Take the following actions to construct the adjacency matrix: Let A be a matrix, and let A_{ij} represent the connection in the network between articles i and j. This could be ascertained by examining related factors, content similarities, and similar sources. The transformation rule that updates node representations in a GCN is represented by equation (9). Here, $H^{(l)}$ stands for the layer one node characteristics l, $W^{(l)}$ represents the weight matrix applied to these features, $\hat{A}$ refers to the normalized adjacency matrix of the graph, and $\hat{D}^{-1/2}$ denotes the symmetrically normalized degree matrix of $\hat{A}$. The procedure entails combining data from adjacent nodes, denoted as $\hat{A}$, and modifying these characteristics using the weights $W^{(l)}$. The node characteristics $H^{(l+1)}$ obtained from the previous layer $l+1$ are subsequently subjected to a non-linear activation function (such as ReLU or Sigmoid) on an element-wise basis. Updated representations are produced by this process and used in downstream activities or further levels within the GCN,

$$H^{(l+1)} = \sigma\left(\hat{D}^{-1/2}\hat{A}\hat{D}^{-1/2}H^{(l)}W^{(l)}\right). \tag{9}$$

The adjacency matrix A and the identity matrix I are added up in equation (10) to produce $\hat{A}$. Every node in the network has its self-loop connections preserved by the identity matrix I, ensuring that each node carries over its characteristics during message delivery. In addition, $\hat{D}$ represents the degree matrix of $\hat{A}$, containing information on each node's degree (count of connections) in the modified graph. LaTeX format is used to express the equation:

$$\hat{A} = A + I. \tag{10}$$

The input layer of a GNN is in charge of initially designating node features. $H^{(0)} = X$, where X is the initial node feature matrix, represents the process. It depicts the process of setting the initial node representations in

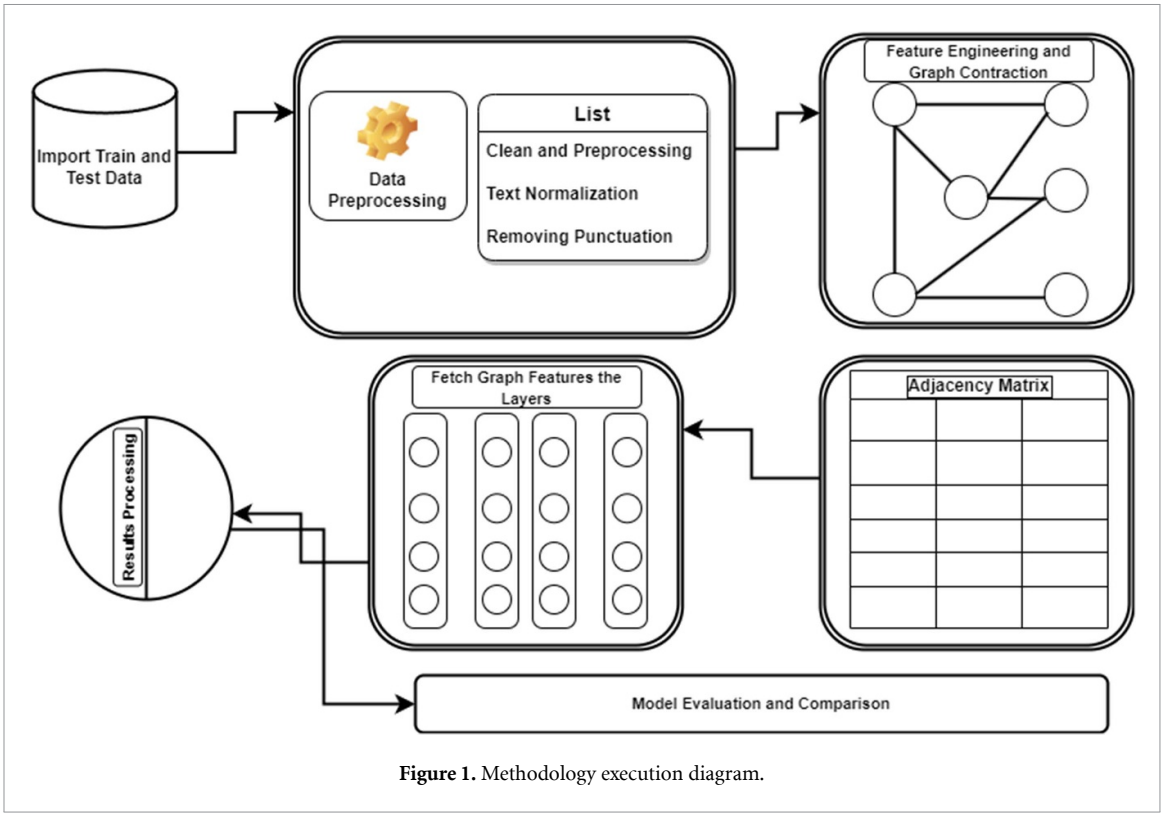

Figure 1. Methodology execution diagram.

the network by allocating the feature matrix X to the first hidden layer $H^{(0)}$. The NN's initial state is represented by this equation, where the input hidden layer receives the initial node features right away. A GNN's hidden layer is computed by applying the graph convolution process, which is typically represented as:

$$H^{(l+1)} = \sigma\left(\hat{D}^{-1/2}\hat{A}\hat{D}^{-1/2}H^{(l)}W^{(l)}\right). \tag{11}$$

The updated node representations in layer $l+1$ are represented in this context by $H^{(l+1)}$. These are obtained by integrating the adjacency matrix A, the node features $H^{(l)}$, and the weights $W^{(l)}$, followed by the application of a non-linear activation function σ. The output layer is denoted by, signifying the complete node representation:

$$Z = H^{(L)}W^{(L)}. \tag{12}$$

The equation defines the variables L and Z. L indicates the number of layers in the network, while Z represents the output node representations obtained by multiplying the final hidden layer $H^{(L)}$ with the weights $W^{(L)}$. During the training process of a GNN, the loss function, typically referred to as the cross-entropy loss L, quantifies the difference between the predicted labels Y_{pred} and the true labels Y_{true}. This function calculates the discrepancy between the predicted and actual labels by evaluating the negative logarithm of the likelihood of the predicted labels. The optimization method aims to minimize the loss function to update the parameters of the model. This update is accomplished by utilizing an optimizer, such as Adam, which modifies the weights $W^{(l)}$ in the network based on the computed gradients of the loss function concerning the weights. The weights are adjusted in the direction that minimizes the loss, as determined by the learning rate α. The mathematical formulation is here:

$$L = -\frac{1}{N}\sum_{i=1}^{N} Y_{\text{true}}(i)\log\left(Y_{\text{pred}}(i)\right) \tag{13}$$

$$W_{\text{new}}^{(l)} = W_{\text{old}}^{(l)} - \alpha\frac{\partial L}{\partial W_{\text{old}}^{(l)}}. \tag{14}$$

Finally, we utilized evaluation indicators to assess the effectiveness of each approach. At the end of the methodology, we also expressed the procedure of GNN in algorithm 1.

Algorithm 1. GNN for fake news detection.

Require: Adjacency matrix A, Feature matrix X, Labels Y
Initialize weights W and biases b
Define GNN architecture:
    Implement message passing function: $h_i^{(l+1)} = \sigma\left(\sum_{j \in N(i)} W^{(l)} \cdot h_j^{(l)}\right)$
    Define graph convolutional layers: $H^{(l+1)} = \sigma\left(A \cdot H^{(l)} \cdot W^{(l)}\right)$
Split dataset into train, validation, and test sets
Initialize optimizer and loss function
Train GNN model:
for each epoch **do**
    Forward pass:
        Compute predictions: $\hat{Y} = \mathrm{GNN}(X, A; W, b)$
    Calculate loss: $L(Y, \hat{Y})$
    Backward pass:
        Update weights using backpropagation: $W \leftarrow W - \alpha \cdot \nabla_W L(Y, \hat{Y})$
end for

Our method based on GNN, is specifically designed to identify fake news. It uses graph-based data structures to accurately represent the extensive network of links between news items, their propagation patterns, and user interactions. This method effectively captures the nuanced and complex relationships using node and edge representation, allowing our GNN model to detect patterns of misinformation propagation that are often disregarded by models that do not use relational data. In addition to content analysis, our approach incorporates sophisticated feature extraction techniques, such as node embeddings, to enhance the detection process by incorporating both content-based and structural insights. We improve this approach by using advanced preprocessing and feature engineering techniques to convert unprocessed news articles into organized graph data that accurately represents the complex relationships present in news stories. The GNN architecture we have developed is designed mainly to address the specific issues associated with detecting false news. It optimizes the layers for processing graphstructured input. In our work, we combine GNN with deep learning techniques to create a hybrid model. This model effectively identifies patterns in textual content and the spread of fake news. Decision Trees and Naive Bayes, which rely on feature independence and statistical analysis, provide a simple approach but face difficulties when dealing with complex misinformation patterns. On the other hand, random forest and SVM aim to enhance predictions by using ensemble learning and handling highdimensional feature spaces. However, they may fail to consider the intricate relational dynamics that exist in news propagation networks. Although LR and NN are powerful in identifying patterns, they mostly concentrate on textual content, potentially disregarding important structural intricacies that are crucial for comprehending the spread of fake news. RNNs excel at handling sequential data and are useful for analyzing the chronological order of news stories. However, they may not fully consider the broader network of connections. On the other hand, the GNN utilizes the structural and relational data of news items and their distribution channels. This allows it to effectively detect complex patterns of false information by examining the relationships between articles, which conventional approaches might ignore. The computational complexity of GNNs is very efficient because they can process nodes (representing news items) and edges (showing connections) in parallel. This efficiency depends on the number of edges and the depth of the network design. The efficiency of the algorithm is denoted by $O(E + D)$, where E represents the number of edges and D represents the network depth. In order to handle the computing requirements of large datasets, graph sampling methods are used, which also enhance the efficiency of processing tasks. However, GNNs successfully handle the space complexity by using sparse matrix representations and message-passing methods to store graph structures such as adjacency matrices and node characteristics. This approach reduces redundant data storage. The space complexity, denoted in Big O notation, is given by the expression $O(V + E)$, where V is the number of vertices or nodes and E is the number of edges. This expression emphasizes the effective use of memory to store the graph data structure that is fundamental to GNNs.

3.1. Datasets

The detection of fake information is a significant and complex effort, especially in the modern era of social media, when users are able to share and flow material without verification occurring. It is possible for the transmission of false information to have substantial repercussions, such as the manipulation of public perceptions, the proliferation of wrong data, and an overall loss of faith in the profession of journalism by the general public. The identification of fake news may be accomplished by the employment of a variety of

approaches, such as the application of NLP, machine learning, and deep learning systems. In general, these methodologies are dependent on a variety of factors, such as the substance of the news story, the news source, the social context, and the temporal dynamics [26] that are involved. The databases come from a wide variety of fields and sources, and they include both fake and genuine news stories.the dataset is collected from www.kaggle.com/code/maxcohen31/nlp-fake-news-detection-for-beginners. Listed below are the columns that they contain:

- Title: The Headline of the News Article
- Content: the main text of the news article
- Subject: The classification of the news article, such as politics, world news, etc.
- Date: The publication date of the news article.
- Target: The classification of the news article as either false or accurate.

In comparison to the real data, which has 21 417 rows, the fake dataset has 23 481 rows overall. The disparity is shown by the datasets, which show that there is a bigger quantity of fake news stories in comparison to real news items. In light of this, some machine learning algorithms would encounter a challenge, as they might acquire the ability to classify the vast majority of news stories as false. This would result in a high degree of accuracy, but a low level of completeness. In addition to including a wide variety of topics, writing styles, and news sources, the databases are heterogeneous. In the process of identifying the semantic and syntactic similarities and differences between fake news sources and real news articles, some NLP approaches, such as word embeddings, may encounter difficulties. Several years' worth of data are included in the dynamic datasets. Certain characteristics, such as the publishing date, the subject matter, and the origin of the news component, may be subject to change over time, which may have an effect on the relevance and accuracy of such characteristics. Please refer to figure 2 for clarification.

3.2. Feature engineering

The procedure initially acquires two separate CSV files, 'fake' and 'true,' into distinct DataFrames named 'datafalse' and 'datatrue.' Before merging into a unified DataFrame called 'data,' each DataFrame is modified by adding a column called 'target.' For the 'datafalse' DataFrame, this column is labeled 'fake', and for the 'data true' DataFrame, 'true'. Then, to guarantee unforeseen circumstances, the data entries are randomized. This leads to the removal of the 'date' and 'title' columns because these characteristics might not significantly affect the classification process. Text preprocessing includes a variety of techniques, such as converting text to lowercase, eliminating punctuation, and eliminating commonly used stop words from the textual data. In the investigation stage, articles are categorized based on their 'subject' to produce a bar chart that efficiently displays the distribution of articles among various subjects. In addition, articles are grouped according to their 'goal' to give an illustration of how fake news is distributed with real ones. Different word clouds are also created for fictitious and real news stories, which help to visually represent the terms that are used the most in each category. A function is implemented to ascertain and graphically depict the terms that are most frequently used throughout the compilation of texts. After that, the dataset is split using the 'train test split' function from the 'sklearn' library into training and testing sets. To train and evaluate the future machine learning model, this is an essential stage. Ultimately, a function for creating and presenting a confusion matrix is developed [32], this aids in assessing how well the model can predict in comparison to the test set's actual labels. To put it simply, the algorithm manages a comprehensive set of steps that include loading data, preprocessing, exploring, and preparing the information needed to build a trustworthy fake news detection model.

4. Results and discussions

Table 1 presents the performance metrics of various classification models, such as Decision Tree, Naive Bayes, Random Forest, SVM, LR with NNM, NN, and the GNN method we incorporated in this paper for fake news detection. These models were evaluated on a specific dataset. Generally, models demonstrate an accuracy range of about 95% to 97%, indicating their overall effectiveness in making predictions. The GNN, which has been utilized as an unusual approach in this study, shows impressive performance with numerous true positive (TP) and true negative (TN) results and significantly reduced false positive (FP) and false negative (FN) predictions. This illustrates GNN's ability to classify data accurately while reducing inaccurate predictions. Given that GNN's performance is on par with or higher than that of traditional classifiers, it appears that GNN holds great promise as a cutting-edge tool for knowledge graph predictive modeling. The noteworthy findings indicate that GNN is a promising method for enhancing prediction accuracy and applying knowledge graph analysis, and that it is worthy of more research and development. In table 1 TTP:

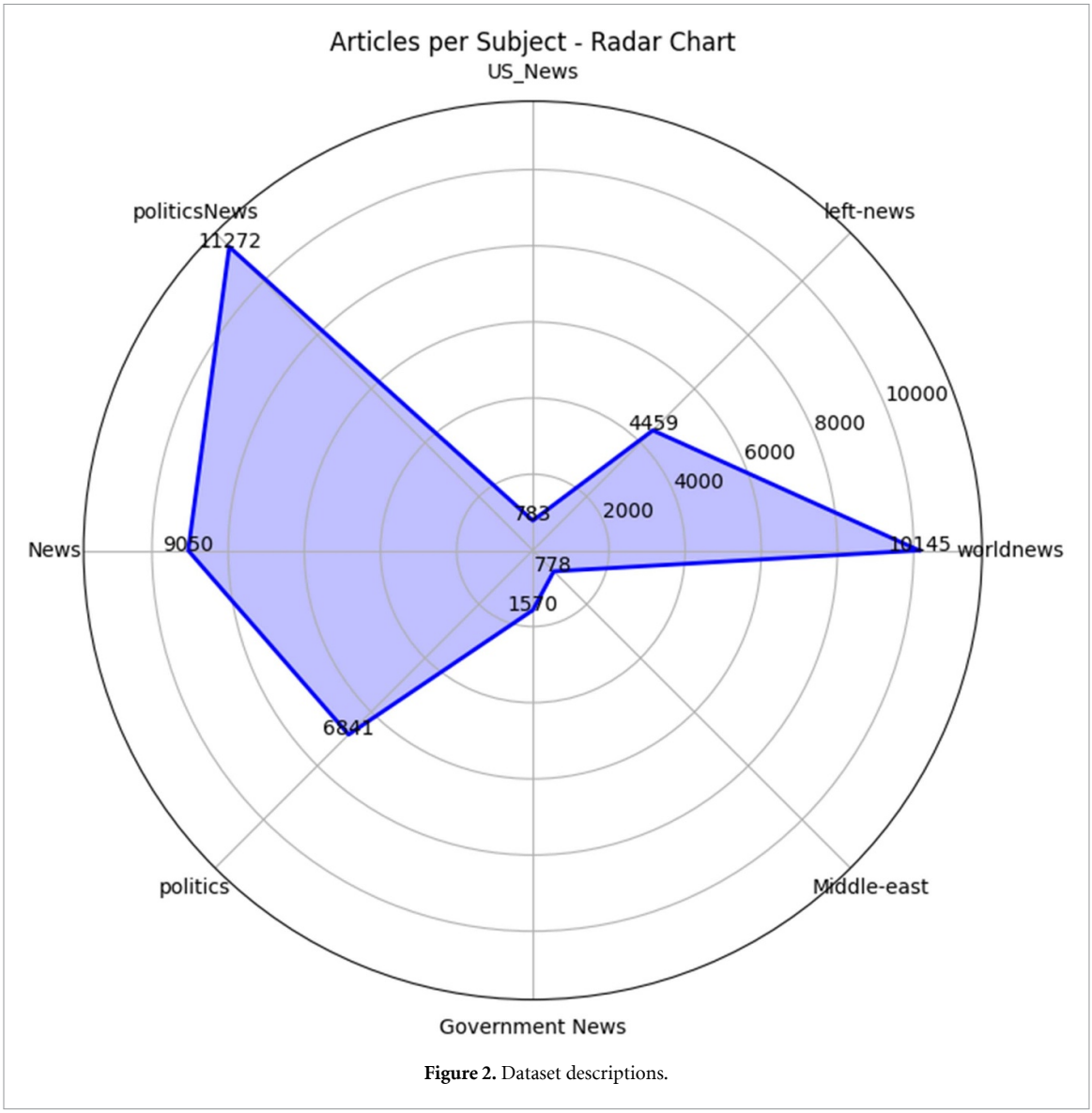

Figure 2. Dataset descriptions.

Table 1. Fake news classification model comparison. The bold values indicate the highest accuracy results.

Methods	TP	TN	FP	FN	TTP	TFP	Accuracy
DTC	4090	4593	155	142	8683	297	0.966 927
NBC	4116	4443	284	137	8559	421	0.953 118
RFC	3900	4676	157	247	8576	404	0.955 011
SVM	4238	4301	226	215	8539	441	0.950 891
LRNNM	4227	4403	224	126	8630	350	0.961 024
NN	4316	4219	331	114	8535	445	0.950 445
RNN	3900	4719	151	220	8619	371	0.958 732
GNN	4316	4419	231	14	8735	245	**0.9727**

total true prediction, TFP: total false prediction, DTC: decision tree classifier, NBC: Naive Bayes classifier, RFC: random forest classifier, SVM: support vector machine, LRNNM: LR with a neural network mindset, NN: neural network, RNN: recurrent neural network, and GNN expressed GNN.

The variation in precision among various methods for identifying false information originates from their basic ability to handle complex relationships in the data. When news stories are represented as nodes in a graph structure, GNN is quite good at understanding the relationships between them, which allows for broad pattern detection. On the other hand, less complex models such as decision trees or naive Bayes might have trouble understanding these complex relationships, which could affect their accuracy. SVMs and LR models perform well in situations with well-defined class borders, but they may struggle with data that is very

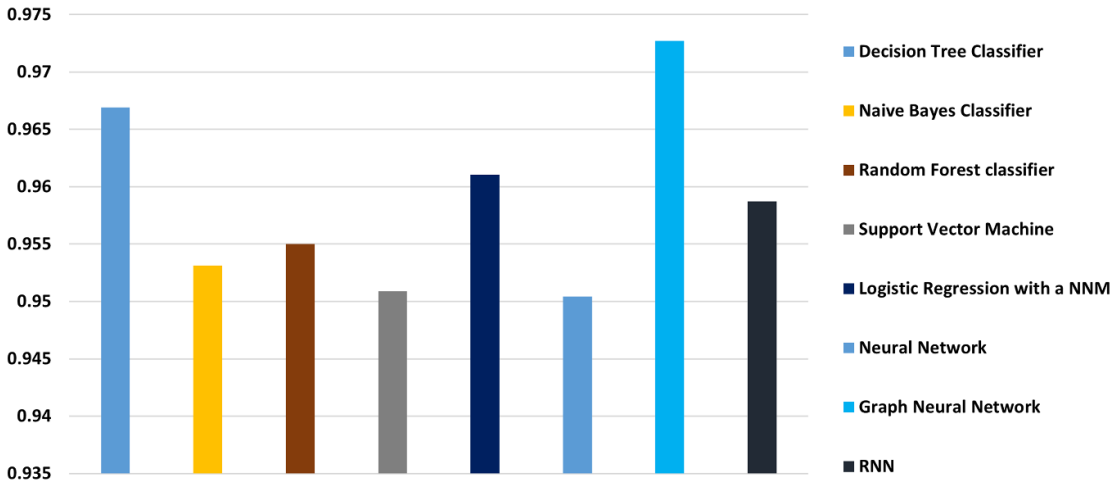

Figure 3. Accuracies of Different Methods.

overlapping or complex, which could have a conflicting impact on their accuracy. Inadequate training or insufficient architectural depth can lead to inferior performance in NN and RNNs. More generally, GNN does exceptionally well in understanding complex graph topologies and intricate interactions, leading to increased accuracy. On the other hand, the effectiveness of other approaches depends on how well they can handle the complexities of the data and the unique features of the dataset. These factors include model complexity, data quality, and hyperparameter tuning accuracy. These factors deserve a careful investigation for more in-depth understanding, see figure 3. The model's ability to correctly categorize situations is measured by the metrics true positives (TP), TN, false positives (FP), and FN. TN are instances that are accurately labelled as negative (e.g. correctly labelling truthful news as true), whereas TP indicate examples that are accurately identified as positive (e.g. correctly detecting fake news as fake). When the model incorrectly classifies a sample as positive—for example, by mislabeling real news as fake—this is known as a FP. On the other hand, FN refer to situations that are mistakenly labeled as bad, such as mistakenly accepting bogus news as true. The 'Total True Predicted' indicator effectively captures both positive and negative occurrences that the system accurately identified, demonstrating the overall prediction accuracy. On the other hand, the Total False Predicted metric combines cases that were wrongly classified and exposes the overall prediction errors of the model. Together, these measures provide a comprehensive insight of the model's performance in differentiating between classes as well as its limitations when it comes to making precise predictions. For more detail, see figures 4 and 5.

4.1. Ablation study

The integration of an ablation study into our research clarifies the importance of certain elements inside our GNN model, therefore enhancing our comprehension of its effectiveness in identifying fake news. This research systematically excludes multiple elements of the model, including graph features, GNN layers, preprocessing approaches, and the classifier head, in order to evaluate how they affect performance measures such as accuracy, precision, recall, and F1 score. Our objective is to identify the fundamental elements for successfully categorizing news items by retraining the model for each modification and comparing the outcomes with the initial configuration. Early projections indicate that this assessment will uncover vital observations, including the essentiality of particular node and edge characteristics in capturing the variations of false information, the ideal depth of GNN layers for efficiently representing the data, and the substantial impact of preprocessing on improving the model's ability to generalize. Furthermore, the research aims to identify the optimal classifier head for the given problem. The results of this ablation study not only confirm the selected components of the original model, but also provide guidance for future research by identifying areas that may be optimized and improved. In the end, comprehending the individual contribution of each component will allow the creation of more efficient and powerful models for preventing the dissemination of false information.

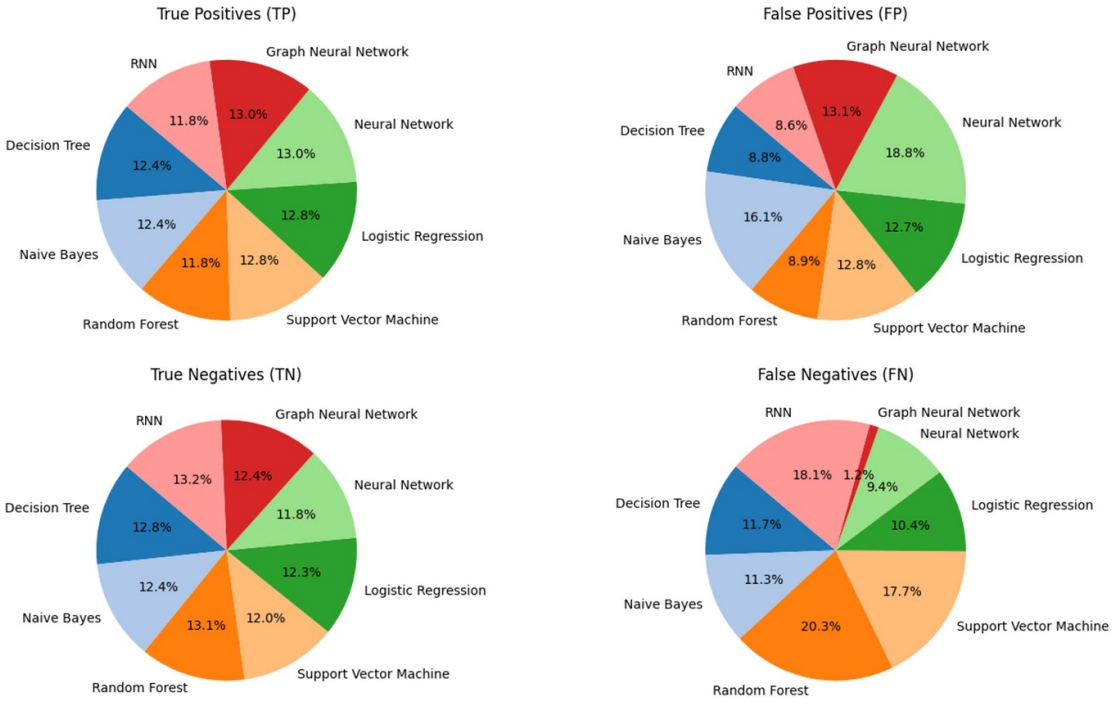

Figure 4. Detail assessment of different method.

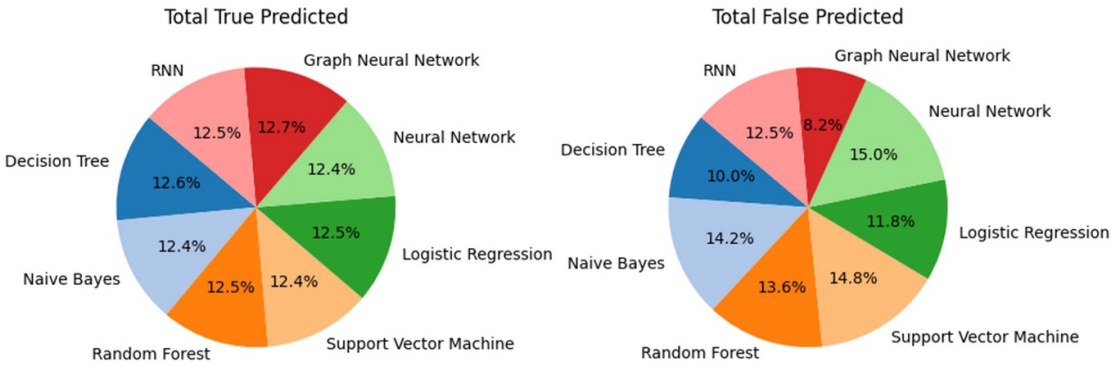

Figure 5. Total positive and negative prediction.

5. Conclusion

Nowadays, with social media making it simple to spread unconfirmed information, spotting fake news gets harder. False information has the power to sway public opinion, spread erroneous information, and damage journalism's reputation. Technologies like deep learning, machine learning, and NLP make it easier to identify fake news. These methods usually depend on elements such as news article content, sources, social context, and temporal dynamics. By analyzing different classification models according to measures such as accuracy, FP, FN, TP, and TN, the GNN has proven to be quite effective in identifying fake news. When compared to previous approaches, the GNN model shows impressive accuracy, demonstrating how well it can differentiate between real and fake news pieces. The precision of the system is derived from its capacity to deftly identify complex connections and trends among data arranged in a graph style. Better TP and TN values are also shown by GNN, demonstrating its dependability in predicting both positive and negative cases. On the other hand, while partially effective, alternative methods show limits in encapsulating the complex relationships present in news data. In summary, GNN proves to be a reliable technique that uses graph-based architectures to distinguish real news stories from fakes. Despite these promising results, our study has limitations. For model training, labelled data availability and quality are constraints. GNNs, like all machine learning methods, depend on the diversity and representativeness of the training dataset. The model's performance may be affected by datasets that do not capture all misinformation tactics, including

fake news's latest strategies. GNNs' computational complexity, especially with large datasets, hinders scalability and real-time processing. Addressing these limitations in future there are many research avenues. Developing more advanced data augmentation techniques for fake news could improve model robustness against emerging misinformation strategies. Second, investigating more efficient GNN architectures or hybrid models that balance accuracy and computational efficiency could enable real-time fake news detection. Finally, integrating user behavioral data and network dynamics into the detection process may reveal fake news propagation patterns, improving countermeasures.

Data availability statement

All data that support the findings of this study are included within the article.

ORCID iDs

Haji Gul https://orcid.org/0000-0002-2227-6564
Adnan Amin https://orcid.org/0000-0002-0852-8833

References

[1] Abbas M, Memon K A, Jamali A A, Memon S and Ahmed A 2019 Multinomial Naive Bayes classification model for sentiment analysis *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **19** 62
[2] Alkhodair S A, Ding S H H, Fung B C M and Liu J 2020 Detecting breaking news rumors of emerging topics in social media *Inf. Process. Manage.* **57** 102018
[3] Baarir N F and Djeffal A 2021 Fake news detection using machine learning *2020 2nd Int. Workshop on Human-Centric Smart Environments for Health and Well-Being (IHSH)* (IEEE) pp 125–30
[4] Basu A, Walters C and Shepherd M 2003 Support vector machines for text categorization *36th Annual Hawaii Int. Conf. on System Sciences* (IEEE) p 7
[5] Bosch A, Zisserman A and Munoz X 2007 Image classification using random forests and ferns *2007 IEEE 11th Int. Conf. on Computer Vision* (IEEE) pp 1–8
[6] Cai H, Zhang H, Zhao D, Wu J and Wang L 2022 FP-GNN: a versatile deep learning architecture for enhanced molecular property prediction *Brief. Bioinform.* **23** bbac408
[7] Chicco D 2012 *Support Vector Machines in Bioinformatics: a Survey* (Politecnico di Milano, Dipartimento di Elettronica e Informazione)
[8] Van der Linden S, Panagopoulos C and Roozenbeek J 2020 You are fake news: political bias in perceptions of fake news *Media Cult. Soc.* **42** 460–70
[9] Dinh X T and Van Pham H 2021 Social network analysis based on combining probabilistic models with graph deep learning *Communication and Intelligent Systems: Proc. ICCIS 2020* (Springer) pp 975–86
[10] Elyan E and Gaber M M 2016 A fine-grained random forests using class decomposition: an application to medical diagnosis *Neural Comput. Appl.* **27** 2279–88
[11] Ferrara E, Varol O, Davis C, Menczer F and Flammini A 2016 The rise of social bots *Commun. ACM* **59** 96–104
[12] Gao C, Wang X, He X and Li Y 2022 Graph neural networks for recommender system *Proc. 15th ACM Int. Conf. on Web Search and Data Mining* pp 1623–5
[13] Gawronski B 2021 Partisan bias in the identification of fake news *Trends Cog. Sci.* **25** 723–4
[14] Granik M and Mesyura V 2017 Fake news detection using Naive Bayes classifier *2017 IEEE First Ukraine Conf. on Electrical and Computer Engineering (UKRCON)* (IEEE) pp 900–3
[15] Gul H, Al-Obeidat F, Amin A, Tahir M and Huang K 2022 Efficient link prediction model for real-world complex networks using matrix-forest metric with local similarity features *J. Complex Netw.* **10** cnac039
[16] Gul H, Al-Obeidat F, Amin A, Tahir M and Moreira F 2022 A systematic analysis of community detection in complex networks *Proc. Comput. Sci.* **201** 343–50
[17] Holan A 2017 The media's definition of fake news vs. Donald Trump's *First Amend. L. Rev.* **16** 121
[18] Hu Z, Dong Y, Wang K, Chang K-W and Sun Y 2020 GPT-GNN: generative pre-training of graph neural networks *Proc. 26th ACM SIGKDD Int. Conf. on Knowledge Discovery & Data Mining* pp 1857–67
[19] Khanam Z, Alwasel B, Sirafi H and Rashid M 2021 Fake news detection using machine learning approaches *IOP Conf. Ser.: Mater. Sci. Eng.* **1099** 012040
[20] Kogan S, Moskowitz T J and Niessner M 2019 Fake news: evidence from financial markets *SSRN Electron. J.* (https://doi.org/10.2139/ssrn.3237763)
[21] Kumar K V and Ramamoorthy M 2022 Naive bayes classifier algorithm for spam detection of email to improve accuracy and in comparison with decision tree algorithm *J. Pharm. Neg. Results* **13** 49–55
[22] Kumar S, Asthana R, Upadhyay S, Upreti N and Akbar M 2020 Fake news detection using deep learning models: a novel approach *Trans. Emerg. Telecommun. Technol.* **31** e3767
[23] Lazer D M J *et al* 2018 The science of fake news *Science* **359** 1094–6
[24] Lohr S 2018 It's true: false news spreads faster and wider. and humans are to blame *New York Times* **8** (available at: https://link.gale.com/apps/doc/A553326916/AONE?u=anon~ad933ee7&sid=sitemap&xid=5a543293)
[25] Lyons T 2018 Hard questions: what's facebook's strategy for stopping false news *Facebook Newsroom* **23** 2018
[26] Misra R 2022 News category dataset (arXiv:2209.11429)
[27] Nasir J A, Khan O S and Varlamis I 2021 Fake news detection: a hybrid CNN-RNN based deep learning approach *Int. J. Inf. Manage. Data Insights* **1** 100007
[28] Noble W S 2006 What is a support vector machine? *Nat. Biotechnol.* **24** 1565–7

[29] Okwuashi O and Ndehedehe C E 2020 Deep support vector machine for hyperspectral image classification *Pattern Recognit.* **103** 107298
[30] Pang H, Lin A, Holford M, Enerson B E, Lu B, Lawton M P, Floyd E and Zhao H 2006 Pathway analysis using random forests classification and regression *Bioinformatics* **22** 2028–36
[31] Poddar K *et al* 2019 Comparison of various machine learning models for accurate detection of fake news *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)* vol 1 (IEEE) pp 1–5
[32] Room C 2019 Confusion matrix *Mach. Learn.* **6** 27
[33] Rustam Z and Saragih G S 2018 Predicting bank financial failures using random forest *2018 Int. Workshop on Big Data and Information Security (IWBIS)* (IEEE) pp 81–86
[34] Dos Santos E F, Silva de Carvalho D and Oliveira J 2021 Pattern identification of bot messages for media literacy *Proc. Brazilian Symp. on Multimedia and the Web* pp 121–8
[35] Saritas M M and Yasar A 2019 Performance analysis of ann and Naive Bayes classification algorithm for data classification *Int. J. Intell. Syst. Appl. Eng.* **7** 88–91
[36] Shao C, Ciampaglia G L, Varol O, Yang K-C, Flammini A and Menczer F 2018 The spread of low-credibility content by social bots *Nat. Commun.* **9** 1–9
[37] Shelke S and Attar V 2019 Source detection of rumor in social network—a review *Online Soc. Netw. Media* **9** 30–42
[38] Song Y-Y and Ying L 2015 Decision tree methods: applications for classification and prediction *Shanghai Arch. Psychiatry* **27** 130
[39] Antony Vijay J, Anwar Basha H and Arun Nehru J 2020 A dynamic approach for detecting the fake news using random forest classifier and nlp *Computational Methods and Data Engineering: Proc. ICMDE 2020* vol 2 (Springer) pp 331–41
[40] Wasim M, Al-Obeidat F, Amin A, Gul H and Moreira F 2023 Enhancing link prediction efficiency with shortest path and structural attributes *Intell. Data Anal.* **2** 467–83
[41] Wasim M, Al-Obeidat F, Moreira F, Gul H and Amin A 2023 Forecasting networks links with laplace characteristic and geographical information in complex networks *Proc. Comput. Sci.* **224** 357–64
[42] Yi J, Nasukawa T, Bunescu R and Niblack W 2003 Sentiment analyzer: extracting sentiments about a given topic using natural language processing techniques *3rd IEEE Int. Conf. on Data Mining* (IEEE) pp 427–34
[43] Zainab Z, Al-Obeidat F, Moreira F, Gul H and Amin A 2023 Comparative analysis of machine learning algorithms for author age and gender identification *Proc. Int. Conf. on Information Technology and Applications: ICITA 2022* pp 123–38
[44] Zekić-Sušac M, Šarlija N, Has A and Bilandžić A 2016 Predicting company growth using logistic regression and neural networks *Croatian Oper. Res. Rev.* **7** 229–48
[45] Zhao Z, Resnick P and Mei Q 2015 Enquiring minds: early detection of rumors in social media from enquiry posts *Proc. 24th Int. Conf. on World Wide Web* pp 1395–405