

Review Article

Fake News Detection Techniques on Social Media: A Survey

Ihsan Ali , **Mohamad Nizam Bin Ayub** , **Palaiahnakote Shivakumara** ,
and **Nurul Fazmidar Binti Mohd Noor** 

Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

Correspondence should be addressed to Ihsan Ali; ihsanalichd@siswa.um.edu.my
and Mohamad Nizam Bin Ayub; nizam_ayub@um.edu.my

Received 25 May 2022; Revised 26 July 2022; Accepted 3 August 2022; Published 22 August 2022

Academic Editor: Kuruva Lakshmanna

Copyright © 2022 Ihsan Ali et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Social media platforms like Twitter have become common tools for disseminating and consuming news because of the ease with which users can get access to and consume it. This paper focuses on the identification of false news and the use of cutting-edge detection methods in the context of news, user, and social levels. Fake news detection taxonomy was proposed in this research. This study examines a variety of cutting-edge methods for spotting false news and discusses their drawbacks. It also explored how to detect and recognize false news, such as credibility-based, time-based, social context-based, and the substance of the news itself. Lastly, the paper examines various datasets used for detecting fake news and proposed an algorithm.

1. Introduction

Several emerging technologies help us comprehend human behavior. Previously, human-machine contact was just a dream. A civilization of living creatures surrounds our globe, a large celestial body, and a connection binds us to the same territory [1, 2]. It connects us to our planet and creates a big civilization to dwell in. A group of persons having the ability to manage a given territory helps build this civilization. Humans, the environment, and many industries all surround society. The government of that state establishes regulations that society must obey to oversee these activities [3]. Various developing technologies might help the government establish security policies. John McCarthy created the term “artificial intelligence” in 1955. It was later revealed that neural networks and machine learning may be used to predict the future [4]. With the new technology, each area has advanced significantly. Therefore, the government has been adopting these technologies into every available program for the people’s benefit [5].

Text categorization is the process of classifying and arranging texts or tags depending on the content of the information. Intent identification is a critical task in natural language processing (NLP), and it has a wide range of appli-

cations that include subject labeling, spam identification, and sentiment analysis [6]. NLP enables text analyzers to automatically detect content, after which a predefined set of labels or classifications are assigned based on their subjects from medical research documents, publications, and other sources from across the globe are identified. [7]. Even though the classifier decides which category of textual content is classified, it is required to assess the degree to which all inputs in the training dataset are comparable. To automatically find and uncover patterns in electronic texts, NLP, machine learning methods, and data mining are applied [8]. The fundamental purpose of the technology is to enable users to extract information from textual tools and deal with activities utilizing text mining. Information extraction (IE) technologies seek to extract precise information from textual materials. This is the first approach, which indicates that the phrases text mining and data extraction may be used interchangeably [9].

The significant improvements in mobile phones and ubiquitous Internet usage have reshaped social connections. Because of their ease of access and quick dissemination of news, Twitter and other social media platforms have become popular ways for people to disseminate and receive news. However, the reliability of the news shared on these platforms

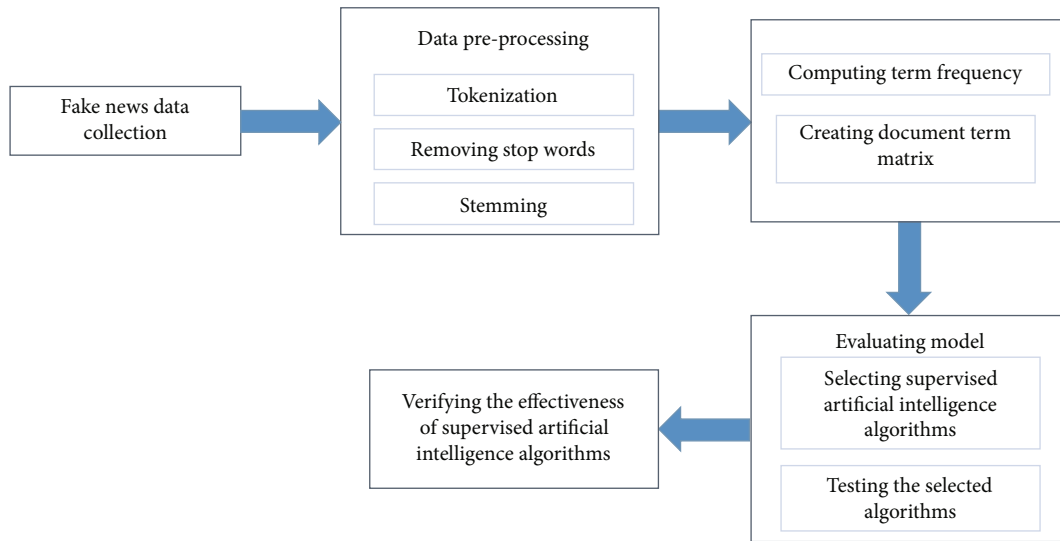


FIGURE 1: General concept of fake news detection (source: [11]).

has become a big concern. Because of the rise of social media, legitimate and fake news are often presented in the same way, making it impossible to discern between the two. In the absence of rigorous verification, well-meaning people may unwittingly support the propagation of fake news. For financial, political, or other reasons, fake news is a material that has been produced to misinform, deceive, or lure readers [10]. Social media usage has skyrocketed in recent years, owing to the advantages of connecting people, sharing material, and keeping up to date with global happenings. The threat of false data and the propagation of fake news have escalated, possibly causing major societal issues.

Fake news may have a harmful influence on society and people, as well as businesses and governments. For example, malicious people may distribute fake information about a business, or spam may do severe harm to the company's reputation. Many scholars have been motivated to run experiments to build a method for detecting fake news as the distribution of false information continues to grow in sophistication and frequency. Figure 1 depicts a high-level overview of the notion of false news identification.

In the context of fake news, any type of news that is purposely misrepresented and broadcast with the express objective of deceiving or causing doubt is defined as follows: The phrase "fake news" is not a new one. Even though its beginnings are obscure, it has proven to be a long-lasting phenomenon. The Battle of Actium, which occurred in 31 BC, is one of the oldest examples [12]. The origins of the phrase may be traced back to World Wars I and II. Others have contended that it predates the advent of "true news" by decades. While there has been some historical imprecision regarding false news, historical reports have shown the prominence of the link between politics and misleading information. Media, particularly political party-affiliated news organizations, have for years spread one-sided ideas and a large lot of material that was lacking in reliability [13].

Furthermore, a thorough overview of news science will be provided in the next part, which will assist us in better understanding the research subject. This research focuses on the identification of false news and the use of cutting-edge detection methods in the context of news. We conduct a comprehensive review of the current literature in the field of identifying false news using a variety of various methodologies. We provide a novel news detection taxonomy based on existing authentication detection approaches in the settings of content, user, and social level, and we discuss how it may be used in various situations. Existing procedures are also evaluated in terms of their difficulties and potential solutions. Fake news may be detected and identified using a novel scenario that is based on textual content, which we present. Thus, Abbreviations provides all abbreviation used in the paper.

The remainder of the paper is as follows. Section 2 discusses the overview of fake news detection. State-of-the-arts fake news detection techniques are provided in Section 3. Section 4 provides the proposed fake news detection taxonomy. Fake news detection mechanisms/techniques and their challenges were explored in Section 5. Section 6 discussed fake news detection based on textual content. Section 7 presents methods for detecting and identifying fake news. Datasets for fake news detection and a proposed fake news detection algorithm were provided in Section 8, while Section 9 concludes the paper.

2. Overview of Fake News Detection

Nowadays, the Internet is propelled by news and advertising. Advertising on websites with hot news and provocative headlines helps capitalize on the site's high traffic. Making money using automated advertising that rewards high visitors to websites has been witnessed. Global inhabitants are stressed and confused by constant information dissemination [14]. Digital disinformation is made intentionally to

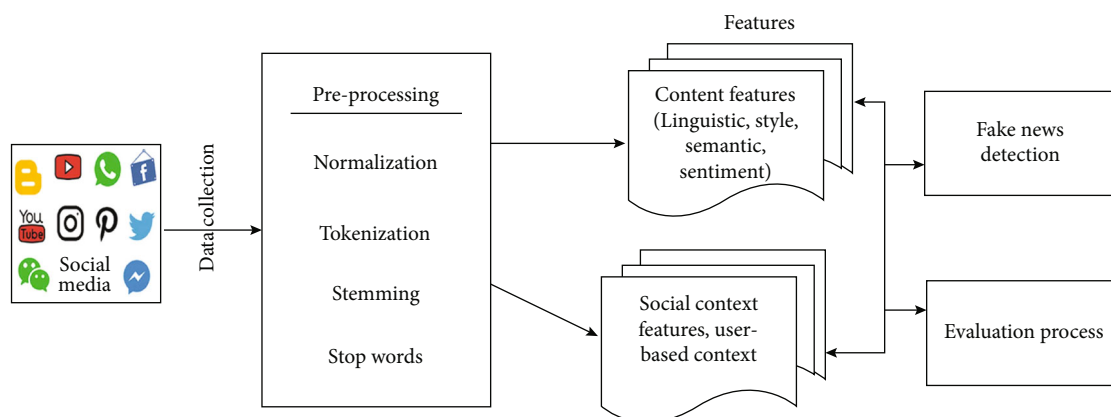


FIGURE 2: An overview of detecting fake news over social media.

harm or mislead the public. A lot of individuals may be harmed by misinformation. Misinformation has been proven to instigate conflict and interrupt voting and most importantly societal animosity. As a consequence of the spread of false news on social media, consumers may become wary of sharing and publishing legitimate material for fear of being misled, since fake news is spread in two key ways: disinformation and misrepresentation.

The reason they spread it is because they witness their friends or other people doing it [15]. For example, when one friend sees something on social media, it will let the user know that their friends have viewed or liked this material if they get the identical offer from a different buddy, which will encourage more consumption. In addition, this recommendation system encourages users to share content even if they are dubious of its legitimacy. People who share the same religious views or who belong to the same political party will distribute and communicate information without doing enough verification checks on the facts. According to cognitive theories [16], humans are susceptible and hence susceptible to bogus news. According to [17], individuals prefer to trust things that support their beliefs (confirmation bias) and would disseminate them without verifying them, while distorting facts that contradict their beliefs. Thus, an overview of detecting fake news over social media is presented in Figure 2.

Fake news has even overtaken the present COVID-19 epidemic scenario. WhatsApp is the latest social media tool to fall victim to the spread of false news. Numerous images pretending to represent situations in China, such as photographs of victims lying on the streets, are spread on WhatsApp to showcase the devastation of the coronavirus. Fact-checking organizations have revealed some of these films as old footage, fake exercises, or even movie scenes. Furthermore, fact-checkers have raised concerns about the government's advice, which suggests using botanicals and homeopathic medicines to avoid COVID-19. This increased the propagation of false news to the point that people began to believe the rumors. There was a case when a man in southern India took his own life after viewing too many documentaries on coronavirus and concluding that he was infected. This emboldened the government's view, and fast action was required in a situation where 3000 individuals were being watched. Follow-

ing this, the central government was forced to take an important step in combating the rise of fake news. To prevent misinformation from mobile phone customers, the federal government has mandated that a caller tuned into an audio recording describing the coronavirus be provided [18]. In addition, a healthcare professional was prosecuted for spreading false information [19].

3. State-of-the-Arts Fake News Detection Techniques

Plenty of other social media platforms, including Facebook, Instagram, YouTube, and Twitter, have grown in prominence as go-to news and entertainment resources for those with mobile devices. While social media and technology have a good influence on society, they are not without flaws or restrictions. Fake news may have a broad variety of consequences, ranging from being just inconvenient to influencing and deceiving whole communities or even entire governments. The linked research demonstrates that false news has a negative influence on society. Methods for recognizing fake news are now accessible in a variety of forms, including knowledge-based, language-based, machine learning-based, hybrid, and topic-agnostic approaches [15].

Examples of two-step methods include the integration of text mining techniques with supervised artificial intelligence algorithms [20], which was suggested to identify false news utilizing accuracy, recall, precision, and *F*-measure to verify the combined algorithms. The structured dataset is created from unstructured datasets via the use of the document term matrix and the TF weighting technique, which are both described in detail below. Concerning all supervised algorithms, KLR has the worst performance across the board in all parameter evaluations and has failed to detect fake news in real-world datasets.

To determine the content characterization, the term frequency-inverse document frequency method is used. The latent Dirichlet allocation (LDA) method was introduced by [1], and it is meant to identify bogus news by employing a random number generator. The similarity of documents between authentic and false news is utilized as a parameter assessment for determining the efficiency of

LDA in a certain situation. The identification of false and true news on social media is carried out successfully by analyzing domain reputation and content comprehension, among other things. The similarity and dissimilarity of the material are only collected for a few key terms in each article, which are then combined. A novel algorithm, called “enhanced graph-based supervised learning algorithm as EGSLA,” was proposed by [21], which used accuracy, precision, sensitivity, specificity, and Mathews’ sensitivity and specificity. The correlation coefficient and the F -measure are used to compare the EGSLA with other algorithms such as decision tree, SVM, and KNN. The “EGSLA algorithm successfully predicts the fake users and news on Twitter by extracting the important features,” which are identified on the weighted graph, and then applying them.

Khan et al. [22] discovered that participants’ perceptions of false news transferred to an adjacent brand advertising when they saw an adjacent brand commercial. The direct impact of behavioral intentions on brands is employed to investigate the consequences of fake news. The discrepancy between the perceived credibility of the news and the actual credibility of the news is investigated and influenced by analyzing changes in the behavior of the audience. User behavioral intentions are strongly influenced by fake news, which has a significant impact on the perceived credibility of news sources. Additionally, Qasim et al. [23] made use of a total of four integrated components, such as an entity extractor, a text extraction unit, a web scraping unit, and a processing unit, which is planned for the FND model. Validation of the usefulness of the new approach is accomplished via the use of accuracy, precision, recall, and F -measure. It is necessary to identify the similarities between extracted entities and page titles for specified keywords to eliminate false positives [24]. These techniques do not have a clear emphasis on the categorization of regional news. In addition, the approach is inadequate for extracting text owing to the existence of picture properties in addition to the text being extracted [24] developed a principled automated technique for distinguishing between these diverse scenarios when rating and categorizing news items and assertions. Accuracy, mean squared error (MSE), and $F1$ score are among the metrics used to assess the effectiveness of this strategy. The aggressive conduct is not taken into consideration for the forecast, nor are the responses to social media, which are used to determine the intentions behind disinformation spread via social media [25]

Ahmed et al. [26] developed a unique approach for identifying harmful social bots in online social networks that were very accurate. The accuracy, precision, recall, and F -score of the suggested method are utilized to compare the results with those of the support vector machine (SVM) approach. The technique examines the time feature of user activity as well as the transaction probability of their click-streams to conclude. The particular intentions of the harmful social bots operating on online social media platforms have not been determined at this time. Furthermore, Figueira and Oliveira [27] devised a content-based analysis method to ensure that the collected tweets contributed to the discussion. To evaluate the performance of the proposed

model, the parameters accuracy, precision, recall, and F -score are employed as parameter metrics. Rumor detection techniques have been developed in recent years [17, 28–30] that have shown success in detecting tumors at an early level, even before refuting or interrogating messages have been placed on social media platforms. The strategy did not intend to design efficient rumor management tactics after detecting a rumor at an early stage in its life. Additionally, Varma et al. [31] discovered fraudulent postings in real-time Facebook data by developing a REST browser, which is a Facebook inspector. Accuracy, reaction time, accuracy, recall, and ROC AUC are all metrics that are used to evaluate the FBI’s overall performance. When a fraudulent post is posted, Facebook inspector identifies it in real-time, without relying on any interaction data linked to the post (likes, comments, or shares). The FBI’s present architecture restricts access to its services to just public Facebook postings [1, 32]. The FBI will be of no use in addressing the zero-attack issue. For the detection of false news, Granskogen and Gulla [30] devised a variety of visual and statistical patterns with distinct characteristics. Accuracy, $F1$ -score, precision, and recall are just a few of the considerations that go into the validation process itself. In news events, statistical features are used to aggregate together images and attribute information, which includes picture statistics and attribute information [29]. Through statistically recording the picture distribution pattern, the verification performance may be increased even more. When models are trained separately on image and nonimage datasets using the described approach, the dependency information is not included in the model.

3.1. Existing Survey on Fake News Detection Techniques. In this section, the existing survey on fake news detection techniques is presented in Table 1.

Table 1 shows the existing survey of fake news detection techniques. It is seen that each of the existing works focused on different areas such as visual, linguistic, temporal, social level, user level, or content level. However, this present research will integrate all these aspects, thus allowing potential researchers and scholars to have deep insights into fake news detection techniques.

4. Fake News Detection Taxonomy

We spend so much time online that individuals choose social media news sources over conventional news sources. In this section, we present the taxonomy for fake news detection. Figure 3 shows the taxonomy for fake news detection.

4.1. Data-Oriented. Various types of data features, including dataset, temporal, and psychological, are being studied in data-driven fake news studies. Researchers in [26, 27, 37] showed that there is no existing benchmark dataset that provides resources for extracting all essential attributes. To facilitate future studies on this topic, we create a comprehensive and large-scale benchmark dataset for false news. This is a possible technique. The spread of fake news on social media follows different temporal patterns that differ from that of legitimate news. The job of early false news identification,

TABLE 1: The existing survey on fake news detection techniques.

Authors/reference	Title	Categories/areas
[7]	"A hybrid model for fake news detection: leveraging news content and user comments in fake news"	Visual
[10]	"Sentiment analysis for fake news detection"	Linguistic
[26]	"Detecting fake news using machine learning: a systematic literature review"	Temporal
[20]	"Can machines learn to detect fake news? A survey focused on social media"	Social level
[13]	"Fake news detection in low-resourced languages "Kurdish language" using machine learning algorithms"	User-level
[3]	"Mapping the scholarship of fake news research: a systematic review"	Content-level
[33]	"Fake news detection tools and methods—a review"	Social level
[34]	"Approaches to identify fake news: a systematic literature review"	Social level
[35]	"Fake news detection in social media: a systematic review"	Content-level
[36]	"Fake news detection: a survey of evaluation datasets"	Content-level
[25]	"Fake news detection on social media: a systematic survey"	Temporal

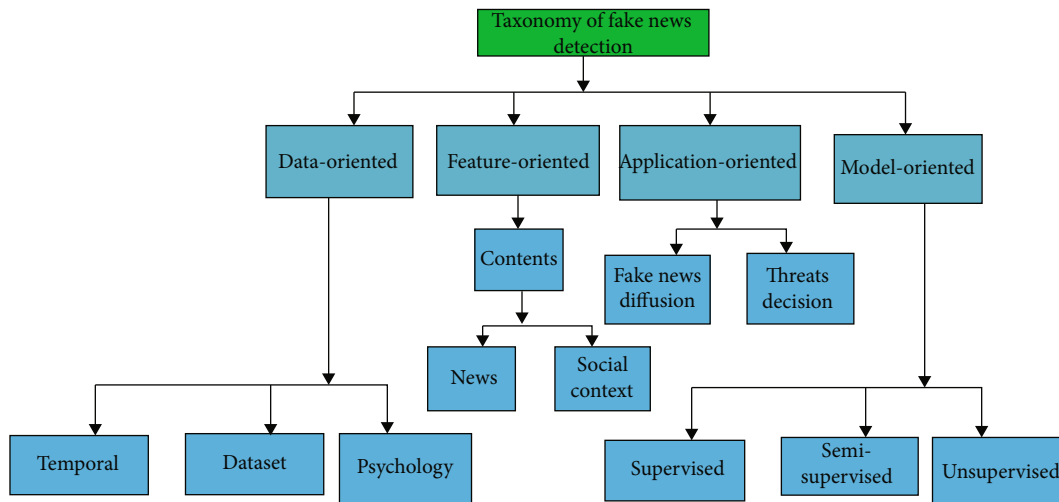


FIGURE 3: Taxonomy for fake news detection.

which attempts to offer fake news warnings early rather than later in the distribution process, is thus fascinating. Using this method to verify news stories, for example, may only look at social media postings that appear within a specified time frame of the original post [38]. It is possible that detecting bogus news early on may assist to prevent it from spreading further on social media platforms. There have been several subjective research into the components of false news published in the social psychology literature [22, 32, 38, 39], but there have been relatively few quantitative investigations to validate these psychological factors. Regarding spreading false information on social media, the echo chamber effect has a tremendous impact, as seen above. Capturing echo chamber effects and utilizing the pattern to identify fake news on social media, for example, may be an interesting experiment. Apart from that, while intent detection from news data is exciting, its application is limited since most current fake news research is focused on determining authenticity while neglecting the intent component of false news. Because the purpose is often publicly accessible, inten-

tion detection is challenging. Therefore, it is interesting to study how data mining tools might be used to analyze and gather psychological objectives.

4.2. Feature-Oriented. False news research with a focus on features is aimed at uncovering valuable characteristics that may be used to distinguish true news from false news from some data sources [1, 35]. News content and the social environment are two significant data sources that have been shown. In terms of news content, researchers created linguistic and visual methodologies for extracting information from text data. However, although linguistic-based qualities have been extensively explored to aid with general NLP tasks such as text classification and grouping, the fundamental characteristics of false news remain unknown [40]. Additionally, "embedding methods such as word embedding and deep neural networks are gaining popularity for textual feature extraction due to their ability to generate better representations and improve feature extraction accuracy" [17, 23, 41]. It has also been shown that visual components taken

from images may serve as key indications of bogus news [37]. However, limited research has been undertaken to utilize important visual characteristics for the false news detection challenge, including classic local and global features and recently generated deep network-based features [42]. Several sophisticated approaches have recently been shown, including the ability to edit video recordings of renowned persons [22], create high-quality films [43], and other skills. As a consequence, distinguishing true from false visual information becomes much more difficult and critical, and more complex visual-based criteria are required for this study to be successful [44]. We added user-based, postbased, and network-based components to the system from the perspective of the social context. Existing user-based features are mostly focused on broad user profiles rather than distinguishing across numerous account types and obtaining user-specific attributes from each of them. Others, such as convolutional neural networks (CNN) [45], might be used to represent postbased attributes to better capture people's thoughts and reactions to bogus news. According to the authors, photos in social media postings may also be used to better comprehend people's reactions to news events [20, 31]. Network-based characteristics are retrieved and utilized to demonstrate the different processes by which various kinds of networks are built. It is critical to advance this basic work to investigate how additional networks can be created in terms of other characteristics of interactions among relevant individuals and posts and more important network modeling approaches, such as network embedding that can be used to describe connections [46].

4.3. Model-Oriented. Modeling-based fake news research provides the door for the creation of more effective and practical techniques for detecting and preventing false news from spreading [47]. It has been detailed in the previous sections how different characteristics may be extracted and included in classification models such as naïve Bayes, decision trees, logistic regression, and support vector machines (SVM) and then recommended the correct classifiers from all these frameworks [13, 48]. Developing more complex models and making greater use of the retrieved characteristics will need additional investigation. The creation of the aggregation approach, the probabilistic method, ensemble method, and projection method are some examples of this study [15, 19]. The following are areas where we feel there is the promise for further research: Algorithms that integrate many feature representations into a weighted form and maximize the weights of each feature are called aggregation algorithms in the beginning. Because fake news usually contains both genuine and incorrect assertions, probabilistic models may be a better choice for predicting the possibility of it being fake news than just providing a binary value. Class labels (such as false vs. genuine news) may be predicted by using the same distribution of features that were used to store them in the first place [49]. Each factor, such as the reliability of the source, the nature of the news, or the response of the public, has unique limits in terms of accurately anticipating false news on its own, making it very difficult to detect false news [50]. Combining several weak

classifiers into a single strong classifier is the goal of ensemble approaches, which have been widely used in the machine learning literature for a wide range of applications [26]. An ensemble model may be useful since both news content and the social environment may provide additional information that can increase false news detection accuracy [51]. Finally, "incorrect news content and social context information may introduce noise into the raw feature space; projection techniques use projection functions to map between original feature spaces (e.g., news content and social context characteristics) and unique physical and behavioral spaces that may be more helpful for classification" [51].

The bulk of the existing solutions is also supervised, necessitating the usage of a fake new ground truth dataset that has already been annotated before training a model. It takes time and effort to build a trustworthy fake news dataset on the other hand, since the process often involves the involvement of skilled annotators who conduct a rigorous assessment of claims and extra evidence, context, and reporting from respectable sources [52]. Therefore, it is equally important to investigate scenarios in which there are few or no labeled fake news articles, and semisupervised or unsupervised models may be employed to detect false news. Unsupervised models are more practical since unlabeled datasets are more easily accessible, even if supervised models are more accurate when using a well-curated ground truth dataset [52].

4.4. Application-Oriented. The term "application-oriented fake news" refers to a study that extends beyond the identification of fake news. Along these lines, we suggest two key approaches: false news dissemination and fake news intervention [23]. Regarding fake news distribution on social media networks, false news diffusion outlines the pathways and patterns of false news dissemination. In the early stages of the study, it was discovered that authentic information and misinformation spread in very different ways on online social networks [39]. Similarly, the dissemination of bogus news on social media has particular features that require more examination, such as sociodemographic characteristics, life cycles, and transmitter detection. Among different social groups, social dimensions are defined as the variety and weak reliance on social ties within each grouping [11]. Because their friends on social media who have the same views as they do influence consumers' impressions of fake news (i.e., echo chambers), users' perceptions of false news vary across different social dimensions [53]. Because of this, it is interesting to explore why and how diverse societal aspects contribute to the dissemination of incorrect information across a variety of areas such as politics, education, athletics, and other fields of interest. People's attention and emotions are drawn to the fake news broadcast process at various stages along the process, which culminates in a unique life cycle. Breaking news and more in-depth news have different life cycles, according to social media studies [54]. An in-depth understanding of the life cycle of fake news will result from the investigation of how specific tales "go viral" from ordinary public discourse. It is necessary to capture the crucial "trajectories of fake news transmission

in general” [55] as well as additional insights into the process for particular fake news pieces, such as graph-based and evolution-based models [13], to track the life cycle of false news on social media. It is also vital to identify the main spreaders of fake news on social media to restrict the breadth of the propagation” [13]. Consider that key spreaders may be divided into two categories: those who project a confident demeanor and those who project a genuine demeanor. They may either give alternative and critical viewpoints on misleading news and endeavor to explain it or can encourage other people to accept the information they are disseminating by transmitting it together with supporting opinions. This means that study into the identification and application of clarifiers and persuasion techniques is critical to preventing the spread of misinformation [13, 29]. In terms of legitimacy, spreaders might be humans, bots, or cyborgs. More research is needed to better identify and recognize fraudulent accounts formed for propaganda purposes on social media since social bots have been used to actively spread fake news on social media platforms [56]. Moreover, to conclude, we recommend further studies into how to deal with fake news and how to intervene before it spreads, as well as how to intervene after it has gone viral, to lessen the consequences of false news [57]. Users who have already been influenced by fake news should be immunized with factual information to modify their beliefs. Removing harmful accounts that spread misleading information or fake news is a primary goal of proactive intervention tactics for combating fake news. Several recent studies [17, 19, 58] are using content-based and network-based immunization strategies to combat disinformation. To anticipate both legitimate and fraudulent news and to prevent the spread of fake news in real-time, one solution relies on a multivariate Hawkes process [33]. With the use of aforesaid identification techniques, operators may be targeted to halt disseminating bogus news, or filtering can be targeted to improve the distribution of legitimate news.

5. Fake News Detection Mechanisms/Techniques and their Challenges

In some estimations, fake news has existed for almost as long since the printing press was invented in 1439 as real news has been widely disseminated. In this part, we will cover different false news detecting mechanisms/techniques, as well as the difficulties associated with using them. The naïve Bayes classifier, SVM, and semantic analysis are three approaches that should be investigated further in the context of false news identification on social media, according to the researchers.

5.1. Naïve Bayes Classifier. According to the Bayes’ theorem, “conditional probability” is the “probability that something will happen given that something else has already occurred.” Naïve Bayes refers to this kind of calculation [5]. Since we already know how likely it is for something to happen, we can estimate the likelihood of it. A supervised learning method, naïve Bayes, is a sort of classifier [47]. For each class, it predicts “membership probability” and hence

belongs to the machine language class. Among other things, it estimates the chance that a given piece of evidence or record belongs to a certain class [59]. If one is looking to identify the “most likely class,” they must first identify the class with the highest probability. MAP categorization is another name for this technique [60]. Alternative interpretation is as follows: The “naïve” premise that all features are unrelated underlies the naïve Bayes classifier. There is no evidence to support this claim of independence in most cases. Take a look at this scenario: During a scan of an article, the naïve Bayes classifier finds the term “Barack.” It is not uncommon for the same story to also mention Barack Obama. This strategy will overestimate “the possibility that an object belongs to a certain class,” as previously mentioned, despite the fact that these two attributes are interrelated [34]. The research supports the idea that the naïve Bayes classifier is unsuited for text classification because it overestimates the likelihood of dependency. “Strong feature dependencies” are no problem for the naïve Bayes classifier since the dependencies will almost always cancel each other out [39]. The popularity of the naïve Bayes classifier may be attributed in part to the fact that it is both quick and readily accessible. For “text classification issues,” it is a superb option because of its adaptability. It may be used for binary or multiclass classifications [10]. Because the naïve Bayes classifier is so straightforward to use, it does not need a big amount of counts to provide its findings. Therefore, as the name says, it is easy to train on a little dataset [24].

Although this technique has its advantages, the most notable downside is that it considers all features as though they are separate, which may not always be the case. Consequently, there is no linkage between the features and their learning.

The naïve Bayes classifier has some challenges, like the following:

- (i) All predictors (or qualities) are presumed to be independent in naïve Bayes, which is seldom the case in real life. Consequently, the use of this technology is restricted
- (ii) This strategy overcomes the “zero-frequency problem” by assigning a restricted contribution to a categorical variable whose category was not available in the training dataset. For this issue, you need to use a smoothing technique [24]. Do not put a lot of trust in the probability it produces, since there is a potential that its forecasts are incorrect

5.2. Support Vector Machine (SVM). One of the most used supervised learning algorithms is the SVM, which may be used interchangeably with the support vector network (SVN). SVMs are trained using data that has previously been divided into two groups. As a result, the model is built only after it has been trained before. Furthermore, the SVM method’s purpose is to identify which group fresh data fit into, as well as to optimize the margin between the two classes [12]. The SVM’s ideal objective is to discover a hyperplane that splits the dataset into two distinct groups. “The

data points closest to the hyperplane” are “support vectors,” and removing them would change the placement of their dividing hyperplane [55]. This is why the support vectors are so important. A hyperplane may be described as “a line that linearly divides and classifies a group of data” and “the farther from the hyperplane our data points reside, the greater the possibility that our data points have been properly categorized” [61]. Because of this, it is a good idea to use the SVM approach because it is incredibly accurate and does well on datasets that are tiny and succinct. Classification and even quantity determination may be accomplished using this method’s wide range of applicability. Support vector machines, on the other hand, can deal with large, multidimensional spaces, and use less memory [62].

Using SVMs, on the other hand, has the drawback of being less successful on noisy (meaningless) datasets with overlapping classes because “the training time with SVMs might be substantial” [63]. In addition, “directly providing probability estimates” is not what the SVM algorithm does [63].

Additionally, SVM faces several additional challenges, such as the following:

- (i) The SVM technique does not work well with large data sets
- (ii) When the data set includes more noise, such as when the target classes overlap, SVM performance suffers
- (iii) In many cases, the number of characteristics for each data point exceeds the number of training data samples, which is common
- (iv) There can be no probability-based explanation for support vector classification since it works by placing data points on each side of a classifying hyperplane

5.3. Semantic Analysis. Natural language processing (NLP) is a discipline of computer science that is descended from the field of semantics. The technique of semantic analysis, as previously described, investigates signs of truthfulness by defining the “degree of compatibility between a personal experience,” which may be equated to a “content “profile “formed from a collection of comparable facts,” as equated to a “personal experience” [64]. The conceit is that the creator of the false news is unfamiliar with the particular event or thing being discussed. If, for example, a person has never gone to the region in question, they may overlook information that has already been included in “profiles on related themes” or may contain ambiguities that semantic analysis may identify [65]. One of the most persuasive reasons in support of semantic analysis is that it is capable of properly categorizing a text via the use of association and collocation, which are two of the most powerful tools available [66]. When dealing with languages that have terms with several meanings and near-synonyms, such as the English language, where there are many words with multiple meanings and

synonyms, this is very advantageous to the speaker. For example, if one selects to use a simple algorithm that is incapable of discriminating between several word meanings, the result may be ambiguous and incorrect. The consequence is that semantic analysis operates similarly to how the human brain analyzes information while looking through text by taking into account rules and connections. It should be noted that there are two potential limitations to the use of semantic analysis, which can be seen in the context of the scenario of comparing profiles as well as the “description of the writer’s personal experience” mentioned above [67]. The first and most important need is that a sufficient volume of previously discovered content for profiles should be accessible to even “assess the alignment between traits and descriptions” [68]. In addition, there is the problem of appropriately associating “descriptors with retrieved properties,” which is a difficult task [26].

As a result of these difficulties, “comparative and objective sentences, classification accuracy, and sarcasm are all considered problems in sentiment analysis.” Most sentiment analysis models [15, 22, 32] wrongly classify a considerable portion of opinionated data as neutral, although it is not.

- (i) Because much of the research on sentiment analysis and opinion mining has been conducted on English language texts, sentiment corpora and lexicons have only been developed in English. When attempting to use these resources and discoveries in other languages, it is usually difficult and inaccurate. Moreover, the question of domain adaptation is raised as a result of this. Studying opinionated data and information in other languages should be promoted since opinionated data and information are not just available in English [3, 32]
- (ii) Classifying sentiments from a small amount of labeled opinionated data is a difficult and expensive operation [23, 26]. On the other hand, unlabeled opinion data is quite simple to get and is extremely inexpensive. In the absence of opinionated data, most researchers begin using unsupervised or semi-supervised ways to gather information. Because these algorithms may use unlabeled data, they require less effort than supervised learning models
- (iii) Sent WordNet [29, 39, 58], ANEW [17, 53], LWIC [11, 32], and Sentinel [1, 22] are all useful resources for determining sentiment words and their intensity. These lexical resources have been used to detect user reviews [17], sentiment strength [29], big emotional oscillations of social media users [23], key circumstances in online marketplaces [28], and patient opinion on health services [12]. The knowledge/lexicon-based solutions, on the other hand, are often limited to the scope of words and their definitions. If the words are not provided in the lexicon (as is often the case in domain-specific applications), these solutions may fail [1, 23, 45, 58]

6. Fake News Detection Based on Textual Content

This section will examine the identification of “fake news” using textual content. We examine the most critical features at the content, user, and social levels [26]. Detailed explanations of each level are provided in the following subsections.

6.1. Content-Level. Fake news and true news may be studied using news content. Essentially, the most valuable elements retrieved from news articles are linguistic and visual. Numerous sorts of linguistic characteristics may develop the following:

- (i) Lexical characteristics, such as the total number of words, the number of characters in each word, the frequency of big words, and the number of unique terms
- (ii) Functional phrases, n -grams, and other syntactic properties such as a bag of words techniques [31], or punctuation and part of speech (POS) tagging. Additionally, visual signals are a critical modulator in the propagation of misleading news [29]. As previously mentioned, misleading news exploits people’s inherent vulnerabilities and hence often relies on sensation-alist or even fabricated pictures (or fake films) to elicit fury and maybe other emotive reactions from clients

In the news ecosystem, the component takes content. A news article consists of the news body (content) and supplementary material. As a general rule, the way an author writes a news story shows how they think about the subject. We incorporate the following news-related ancillary information:

- (i) *Links*: primary sources for news (e.g., CNN, BBC).
- (ii) *Title*: the major subject of the article is described in the title text. Typically, headings are written to attract the interest of viewers
- (iii) *Authors*: the newspaper article’s author
- (iv) *Date of publication*: the moment at which news is released and indicates the freshness or delay of the item
- (v) *Political news*: in this case, we know how much a news source is for a certain party. A news source, for example, with numerous stories favoring the right-wing, demonstrates the source’s and writers’ bias

6.2. User-Level. People that engage in news-related activities on social media have unique user characteristics. Various characteristics of user demographics, including age at registration, number of followers and followers, and number of tweets published [1], are used to extract these user-level variables to infer the trustworthiness and dependability of each user. Furthermore, user participation in the news distribution process extends from responding to a post to distributing news articles. Several studies have shown that there are important perceptual and behavioral elements that significantly promote user participation in the propagation of fake news:

6.2.1. Naive Objectivity. Consumers feel that their version of reality is the only correct one, and those who disagree are considered uneducated, illogical, or prejudiced [46].

6.2.2. Cognitive Dissonance. Consumers favor information that validates their preexisting beliefs [23].

People make decisions based on the relative advantages and drawbacks of alternative situations depending on their existing circumstances, according to prospect theory. Economic game theory may be used to represent the news generating and consumption cycle as a two-player strategic game. Ref [31] may be applied to this desire to maximize the reward of a decision while still achieving positive social outcomes. When it comes down to it, the information ecosystem is comprised of two sorts of important players: publishers and consumers. The publisher’s usefulness originates from two perceptions:

- (i) *Immediate utility*: the profit earned by the publisher is strongly connected with the number of customers contacted
- (ii) *Long-term utility*: the newspaper’s credibility for news credibility

The utility for customers is divided into two parts:

- (i) *Information utility*: the ability to receive accurate and impartial information
- (ii) *Psychological utility*: getting information that meets their previous beliefs and social demands, e.g., confirmation bias and prospect theory

In the strategic game of news consumption, both the publisher and the reader want to increase their overall utility.

6.3. Social Level. When we talk about social dimensions, social ties between different social groups might be rather variable, with little correlation between them, and this is what we are referring to. Social media connections may have a big impact on how people perceive misleading news items, albeit the extent to which this is true varies across various social dimensions [69]. As a result, it is worthwhile to investigate why and how various social elements contribute to the propagation of false news. User information on Facebook tends to be selected in ways that are consistent with their system of ideas, leading to the establishment of polarized groups, sometimes known as echo chambers, according to recent results [3]. Users on social media sites such as Facebook, for example, always follow others who share their interests and, as a result, get news that supports their preferred established narratives [49]. Many psychological variables contribute to the process by which individuals consume and trust bogus news that contributes to the echo chamber effect.

When individuals believe that a source is credible, they are more likely to believe that the source is credible if they believe that other people believe that the source is trustworthy. This is particularly true when there is insufficient evidence available to determine the honesty of the source. Consumers may select the information that they hear often, even if it is false

news, according to the frequency heuristic, which is defined by [41] who demonstrates that social homogeneity is the primary driver of material diffusion, with one of the most prevalent results being the development of homogeneous communities, polarized clusters of people. In most cases, a buddy with the same profile (polarization), that is, belonging to the same echo chamber, is the one to get the information.

The fact that false news's style, platform, and themes are always changing presents a general difficulty with content-based techniques. Models that have been trained on a single dataset may underperform on new datasets that include content, style, or language that differs significantly from the original. In addition, the target variables of fake news change over time, with some labels becoming obsolete and others requiring relabeling to capture the most current changes. To accommodate these changes, most content-based approaches must be reextracted from news stories, and data must be relabeled to reflect the new characteristics that have emerged. Additionally, these algorithms need a large amount of training data to detect false news. Fake news has already spread much too far by the time these techniques have collected enough evidence to verify it. Given that the majority of the linguistic aspects utilized in content-based techniques are language-specific, their usefulness beyond the framework of a given language is limited [56].

7. Methods for Detecting and Identifying Fake News

The rising global adoption and use of social media platforms has created an environment that is conducive to the spread of online false news in a more efficient manner. There is a flood of information on social media platforms that is large, diversified, and heterogeneous (it includes both genuine and incorrect information), and this information travels fast, having a tremendous influence on the whole community [38]. The outcome has been the collaboration of a large number of academics and technology behemoths in the identification of false news on the internet. Because of the advent of big data and the availability of a large number of user-generated data, deep-level features have started to take the role of feature extractors in traditional automated rumor detection systems. This is due to the availability of vast amounts of user-generated data. This section presents several cutting-edge research on fake news detection, all of which come under the larger umbrella of the content and social context of the news item under investigation [70].

Figure 4 shows the detail of fake news detection techniques.

7.1. Content-Based. Using the content of the article [11], the content-based fake news recognition approach attempts to identify fake news by examining either the text or the images inside the news piece or all of these elements. To automatically identify false news, researchers often depend on either latent [3, 15, 22, 32, 39] or hand-crafted [28] aspects of the material.

7.1.1. Knowledge-Based. To validate the authenticity of a given claim, knowledge-based systems use the fact-checking method, in which the supplied claim is checked

against information obtained from external sources. Manual fact-checking approaches (using experts or crowdsourcing) and automated fact-checking techniques (using artificial intelligence) are already available.

(1) Manual Fact-Checking. There are two types of manual fact-checking: (a) expert-based and (b) crowdsourced. Expert-based methods are methods based on experts use an expert-oriented strategy and rely on human professionals who are educated in certain fields to make judgments to be effective. To combat misinformation, "fact-checking websites such as Snopes and PolitiFact use an approach known as fact-checking. Their reliability is certain, but they require a significant amount of time and do not scale well with the tremendous amount of information available on social media." The benchmark datasets LIAR [71] and FakeNewsNet [15], as well as other datasets provided on this page, are used by many academics to generate their research datasets. Crowdsourced is as follows: When using crowdsourced methodologies, the "wisdom of the crowd" may be used to verify the veracity of news items. Fiskkit, which gives a place for individuals to debate key news items and determine their veracity, uses a similar strategy to get their message out. Crowdsourced fact-checking is less reliable than fact-checking conducted by experts, more difficult to administer, and biased and includes inconsistent annotations [22, 28]. In exchange for these time savings, it provides more scalability. CRED BANK [38] is a widely accessible large-scale benchmark fake news dataset that has been annotated by fact-checkers and is intended for use by anybody. Users who are not trustworthy must be screened out of datasets prepared using this method, and conflicting annotations must be addressed before the datasets may be used. The creation of comparable datasets and the annotation of those datasets may also be accomplished via the use of crowdsourcing platforms such as Amazon Mechanical Turk (AMT).

(2) Automatic Fact-Checking. Consequently, automated fact-checking methods have been developed to solve the problem of manual fact-checking not scaling well with a large amount of data, particularly those created via the usage of social media. These techniques depend heavily on natural language processing (NLP), data mining, machine learning (ML), network/graph theory approaches, and many others, rather than on human brains. In general, there are two stages to the automatic fact-checking process: (1) fact extraction, which is concerned with the collection of facts and the creation of a knowledge base, and (2) fact-checking, which is concerned with determining the authenticity of news articles by comparing them to the information contained in the knowledge base. It checks if a given claim is genuine or untrue using open web sources and a knowledge base/graph. Regarding false news identification, real-world datasets are often insufficiently organized, unlabeled, and noisy [29], making automated detection a challenging task.

7.1.2. Style-Based. False news may be identified using a style-based technique, which is similar to the approach used for

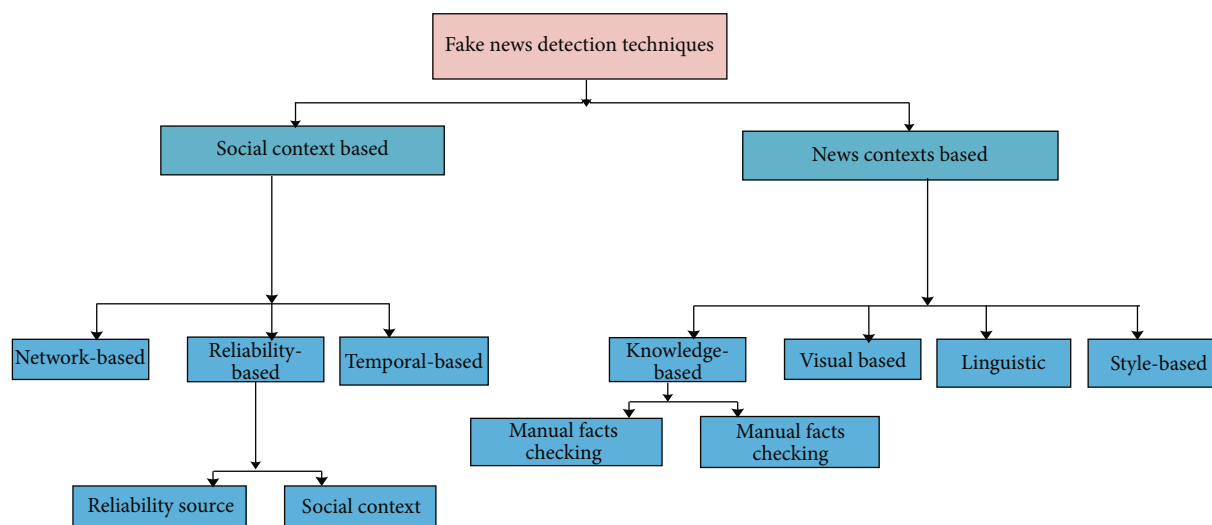


FIGURE 4: Fake news detection techniques.

knowledge-based false news identification. The aim of the writer to deceive the audience is assessed using this method [48], rather than the legitimacy of the news material itself. In most cases, fake news providers are motivated by a desire to exert influence over large groups of people by disseminating inaccurate and misleading information. The names are usually all capitalized to make them catchy, and there are substantially more proper nouns and fewer stop words [27] to make them catchy. To detect fake news, style-based techniques capture the qualities of writing styles that separate genuine users from anomalous ones. As part of the investigation into fake news, Hoy and Koulouri [1] examine the writing style of hyperpartisan news [14]. The most significant contribution of [1] is the detection of stylistic deceit in written materials [61].

7.1.3. Linguistic-Based. Varma et al. [31] presented a total of twenty-six lexicon textual characteristics for consideration. Several researchers provided an improved collection of linguistic criteria to distinguish between bogus and legitimate news [58]. A model for social article fusion (SAF) was developed by [51] that includes social engagement factors in addition to linguistic elements. Preston et al. [52] offer a model that incorporates network account features in addition to linguistic features. To discriminate between true and fraudulent news information, the authors [14] have employed linguistic characteristics, as well as syntactic and semantic elements, to make their determination. Azad et al. [13] provide a model for detecting false news with varying durations of news claims by using several versions of word embedding techniques. Guimarães et al. [29] examine a particular news item's lexicon, syntax, semantics, and discourse levels, as well as its grammatical structure. By conducting dependency parsing at the sentence level, the hierarchical structure learning method proposed by [7] develops a hierarchical structure for a given text. Even though this strategy is effective in a variety of settings, it encounters difficulties in identifying disinformation on popular social media platforms, where messages are brief and, as a result, the linguistic elements collected from

them are frequently insufficient for machine learning algorithms to make accurate predictions [38]. These algorithms are also unable to distinguish between fake news that consists only of images or videos, rather than written content and legitimate news that does not include textual content

7.1.4. Visual-Based. Due to the widespread belief that visual material may increase the credibility of a news article [29], fake news producers routinely use contentious graphic imagery to attract and mislead visitors. Orabi et al. [48] collect a large number of visual and statistical picture features for news credibility from a range of photographs using a statistical modeling approach. The verifying multimedia use task [27] of the MediaEval-16 benchmark is concerned with the difficulty of distinguishing between images that have been digitally altered and those that have not (tampered with).

7.2. Social Context-Based. Three important features of the social environment have been identified, namely, user profiles, user posting and replies, and network architecture [1]. It is a visual representation of how news spreads over time and gives valuable information for determining the validity and political position of news stories. Numerous context-based techniques for false news identification have been investigated recently [23, 32].

7.2.1. Network-Based. To identify false news, network-based fake news detection examines various social networks such as relationships, tweet-retweet, and comment relationships. It is capable of identifying who is spreading false news, the connections between the spreaders, and how fake news spreads on social media. As a result of their mutual interests and similarities, users prefer to develop diverse networks of online media platforms, which act as conduits for the dissemination of information. Studying diverse networks on social media [15, 22, 29] provides useful insights into the people who share news and how they interact [1]. In this case, a tree is used to describe the pattern of message

TABLE 2: Methods for detecting and identifying fake news.

Features	Knowledge-based			Content-based		Linguistic-based	Visual-based	Social context-based		Temporal-based	Credibility-based
	Knowledge-based	Style-based		Style-based				Network-based			
DeClarE [72]	✓	✓		✓		✓		✓		✓	✓
MVAE [64]				✓			✓				✓
EANN [73]	✓							✓		✓	
SAFE (Zhang & Su, 2021)	✓	✓						✓		✓	
FNND-SCTI [74]	✓					✓	✓				✓
TOLA [13]	✓	✓					✓	✓		✓	
FANG [62]		✓				✓		✓			✓
SAME [13]						✓	✓				
Att-RNN [75]	✓	✓				✓		✓			✓

TABLE 3: Datasets for detecting fake news based on news domain.

Item/entity	No. of datasets	List of datasets
Technology	6	"Yelp, EMERGENCY, Burfoot satire blog, FNC-1, CNN/daily news summary dataset, tam et al."
Politics	17	"PHEME, BuzzFeed, LIAR, fact-checking, FakeNewsNet, Benjamin political news, Burfoot satirical news, BuzzFeed news, FNC-1 Spanish disinformation, is the news real or fake? TW info, TSHP-17, Qprop, NELA-GT-2018, NELA-GT-2018, CNN/daily mail summarization dataset, tam et al. dataset"
Economy	3	CNN/daily news summary dataset, Burfoot satire news, Spanish fake news
Society	16	"PHEME, CREDBANK, BuzzFeed, fact-checking, FEVER, EMERGENCY, FakeNewsNet, Burfoot satire news, MisInfoText, FNC-1, Spanish false news, FCV-2018, verification corpus datasets from CNN/daily mail summary and Zheng et al."
Science	3	"Tam et al.'s datasets, FacebookHoax, Spanish false news"
Security	1	Spanish fake news
Health	2	"Spanish fake news, CNN/daily mail summarization dataset"
Tourism	1	Ott et al.'s
Sport	2	"Spanish fake news, CNN/daily mail summarization dataset"
Education	1	"Spanish fake news"

TABLE 4: Datasets for detecting fake news based on application purpose.

Item/entity	No. of datasets	List of datasets
Fake detection	15	"Yelp, LIAR, FakeNewsNet, Benjamin political news, Burfoot satire news, BuzzFeed news, Ott, et al. 's FNC-1, Spanish disinformation, fake or real news, NELA-GT-2018, TW info, FCV-2018, CNN/daily mail datasets for a summary"
Fact-checking	5	"Fact-checking, FEVER, MisInfoText, TSHP-17, Qprop"
Reliability grouping	3	"CREDBANK, BuzzFeed, verification corpus"
Rumor detection	3	"EMERGENT, PHEME, tam, et al.'s dataset"

propagation, which, together with the relationship between posts, provides extra information about the temporal behavior and mood of the postings.

7.3. Temporal-Based. According to studies, news articles on the Internet are not static but are continually developing as new material is added or the original claim is twisted. This is especially noticeable in instances when rumors resurface many times after the original news piece is published. The lifecycle study of rumors aids in the comprehension of this phenomenon, and Varma et al. [31] analyze the repeating rumors at the message level throughout various periods. Zhang and Ghorbani [58] give an in-depth knowledge of the patterns of rumor dissemination across time.

7.4. Credibility-Based. According to several sources, the news quality and trustworthiness/credibility of a claim, publisher, or spreader are indicators of their credibility. Utilizing the idea of credibility, Pilkevych et al. [51] detect users who are spreading misinformation. Preston et al. [52] are concerned with determining the veracity of a particular assertion. Bhavani and Santhosh Kumar [14] suggest a credibility analysis method for analyzing the reliability of a Tweet, which inhibits the spread of false or harmful information on the social media network. Using a web-based system, TweetCred assesses the trustworthiness of a tweet on a real-time basis.

In summary, Table 2 provides the literature that utilized these approaches.

8. Fake News Detection Datasets

A large number of different fake news datasets are accessible because of the many academics working on this subject; however, only a few benchmark fake news datasets are published in the media. The authors of [15] have underlined the fundamental prerequisites for establishing a viable fake news detection dataset, such as uniformity in length, news genres, themes, and so on, as well as a collection of both genuine and fake news pieces to validate the ground truth for each element in the dataset. Among the most important aspects, according to the authors, are the following: The following section contains a collection of publicly accessible datasets, as well as a comparative study of those datasets. In the following table, we provide a high-level summary of several false news datasets that are currently accessible.

8.1. Surveyed Datasets Comparative Analysis. Many datasets exist, as revealed by the literature review study, and are useful for assessing fake news detection techniques. Scholars must do a comparative analysis of various datasets to choose which one to employ for their research, taking into consideration the goal of their study. To offer this analysis, we must first identify the factors that will be used to compare the

TABLE 5: Datasets for detecting fake news based on media platform.

Item/entity	No. of datasets	List of datasets
Mainstream media	13	"Fact-checking, yelp data, FEVER, Benjamin political news, Burfoot satire news, MisInfoText, FNC-1, and Spanish false news fake or real news, Qprop, TSHP-17, NELA-GT-2018, CNN/daily mail collection of summaries"
Online social media	10	"PHEME, CREDBank, BuzzFace, FacebookHoax, BuzzFeed news, Ott and colleagues' dataset, TW info, FCV-2018, verification corpus, tam, et al.'s dataset"
Mainstream + online social media	4	"LIAR, EMERGENT, FakeNewsNet, Zheng, et al.'s dataset"

```

1. Begin
2. Initialize check = 0, valid = 1; //the check is binary for
   Every session
3. If(count == IP)
4. While IP. Changes("DNS hijack#"); //DNS attack
5. Detect("IP"). Tag("session")
6. Else(tag_IP);
7. Mark IP_valid++;
8. End if

```

ALGORITHM 1: Verifying IP address for fake news.

properties of the datasets. The primary goal of this section is to present a set of dataset criteria that may be used to compare dataset features, as well as to demonstrate how each of the surveyed datasets performs concerning these needs. To do this, we must first determine which types of needs are addressed by each dataset. Thus, different datasets for fake news detection used in various applications/domains are provided in Tables 3–5.

8.2. Fake News Detection Algorithm. In the framework of this study, the creation of algorithms focuses on the logic behind cross-layer detection optimization principles. An enhanced detection strategy is suggested in some levels of the model. The identification is being done to create a flag that would warn consumers of the potential of reading bogus news online. The purpose of this research is to offer four different algorithms: an algorithm for confirming a node(s)/source(s) identification, an algorithm for identifying the degree to which news information is false or not from the source, and finally, an algorithm for determining whether or not news content is phony, an algorithm for filtering false news and other news.

It is critical to have an algorithm for recognizing the source of internet fake news. This algorithm examines the article's website, title, content, and author's name. If all of these conditions are satisfied, the news is confirmed. The algorithm checks the database to ensure the website's legitimacy. If the relevant result is discovered or not found, it will be returned.

9. Conclusion

It is not an easy undertaking to develop high-quality fake news datasets because of the need of having data readily available for training and evaluating the algorithms that identify false news. To find a solution to this issue, several scholars have made contributions to the effort of automati-

cally recognizing false news and establishing accurate benchmark datasets of fake and legitimate news derived from social media sites. The number of individuals who get their news from social media platforms rather than through conventional news media channels is expected to continue growing as the popularity of social media continues to rise. Individual individuals as well as society as a whole have suffered substantial effects as a result of incorrect information being spread via social media, according to the research. In this work, we examined the issue of fake news by doing a literature review that was divided into two phases: characterization and detection and then discussing our findings. This study focuses on the detection of fake news and the use of cutting-edge detection techniques in the context of news, user, and social levels. This study offered a taxonomy for detecting fake news. This research investigated several cutting-edge fake news detecting systems and associated problems. Methods for detecting and identifying false news, such as credibility-based, temporal-based, social context-based, and content-based, were also thoroughly examined. Finally, the research investigates several datasets used to identify false news and proposes an algorithm. During the period in which we were tasked with detecting false news, we investigated the many methods currently in use to do so from the point of view of data mining. These methods included feature extraction and model creation, and we made recommendations based on what we discovered. We also addressed the datasets, assessment criteria, and prospective future strategies in fake news detection research. Throughout the discussion, we went into great depth about how to broaden the scope of the area to serve additional uses in addition to news monitoring.

Abbreviations

NLP: Natural language processing
 IE: Information extraction (IE)
 LDA: Latent Dirichlet allocation (LDA)
 MSE: Mean squared error (MSE)
 SVM: Support vector machine (SVM)
 CNN: Convolutional neural networks (CNN)
 POS: Part of speech (POS)
 AMT: Amazon Mechanical Turk (AMT)
 SAF: Social article fusion

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors of this work received partial support from the Faculty Grant (GPF096A-2020, GPF096B-2020, and GPF096C-2020), University of Malaya, Malaysia.

References

- [1] N. Hoy and T. Koulouri, "A systematic review on the detection of fake news articles," 2021, <http://arxiv.org/abs/2110.11240>.
- [2] R. D. Abdiansyah, D. Mutiara, S. P. Sumedha, and N. Hanafiah, "Effective methods for fake news detection: a systematic literature review," in *2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI)*, vol. 1, pp. 278–283, Jakarta, Indonesia, 2021.
- [3] O. Abu Arqoub, A. Abdulateef Elegu, B. Efe Özad, H. Dwikat, and F. Adedamola Oloyede, "Mapping the scholarship of fake news research: a systematic review," *Journalism Practice*, vol. 16, no. 1, pp. 56–86, 2022.
- [4] V. Agarwal, H. P. Sultana, S. Malhotra, and A. Sarkar, "Analysis of classifiers for fake news detection," *Procedia Computer Science*, vol. 165, no. 2019, pp. 377–383, 2019.
- [5] I. Ahmad, M. A. Alqarni, A. A. Almazroi, and A. Tariq, "Experimental evaluation of clickbait detection using machine learning models," *IASC-Intelligent Automation & Soft Computing*, vol. 26, no. 4, pp. 1335–1344, 2020.
- [6] M. O. Ahmad, J. Markkula, and M. Oivo, "Factors affecting e-government adoption in Pakistan: a citizen's perspective," *Transforming Government: People, Process and Policy*, vol. 7, no. 2, pp. 225–239, 2013.
- [7] M. Albahar, "A hybrid model for fake news detection: leveraging news content and user comments in fake news," *IET Information Security*, vol. 15, no. 2, pp. 169–177, 2021.
- [8] M. Albahar and J. Almallki, "Deepfakes: threats and countermeasures systematic review," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 22, pp. 3242–3250, 2019.
- [9] A. Asif, D. Alfraraj, and M. A. Alshamari, "A comprehensive approach of exploring usability problems in enterprise resource planning systems," *Applied Sciences*, vol. 12, no. 5, p. 2293, 2022.
- [10] M. A. Alonso, D. Vilares, C. Gómez-Rodríguez, and J. Vilares, "Sentiment analysis for fake news detection," *Electron*, vol. 10, no. 11, 2021.
- [11] J. Revez and L. Corujo, "Librarians against fake news: a systematic literature review of library practices (Jan. 2018–Sept. 2020)," *The journal of academic librarianship*, vol. 47, no. 2, article 102304, 2021.
- [12] K. Anoop, M. P. Gangan, and V. L. Lajish, "Leveraging heterogeneous data for fake news detection," in *Linking and mining heterogeneous and multi-view data*, pp. 229–264, Springer, Cham, 2019.
- [13] R. Azad, B. Mohammed, R. Mahmud, L. Zrar, and S. Sidiq, "Fake news detection in low-resourced languages 'Kurdish language' using machine learning algorithms," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 6, pp. 4219–4225, 2021.
- [14] A. Bhavani and B. Santhosh Kumar, "A review of state art of text classification algorithms," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1484–1490, Erode, India, 2021.
- [15] R. Oshikawa, J. Qian, and W. Y. Wang, "A survey on natural language processing for fake news detection," 2020, <https://arxiv.org/abs/1811.00770>.
- [16] R. Biswas, N. Vyas, and M. Baskar, "Sentiment Analysis on National Education Policy Change 2020," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 1480–1488, 2021.
- [17] M. Celliers and M. Hattingh, *A Systematic Review on Fake News Themes Reported in Literature*, vol. 12067, Springer International Publishing, LNCS, 2020.
- [18] T. Chauhan and H. Palivela, "Optimization and improvement of fake news detection using deep learning approaches for societal benefit," *International Journal of Information Management Data Insights*, vol. 1, no. 2, article 100051, 2021.
- [19] B. Collins, D. T. Hoang, N. T. Nguyen, and D. Hwang, "Trends in combating fake news on social media – a survey," *Journal of Information and Telecommunication*, vol. 5, no. 2, pp. 247–266, 2021.
- [20] F. C. D. da Silva, R. V. da Costa Alves, and A. C. B. Garcia, "Can machines learn to detect fake news? A survey focused on social media," in *Hawaii International Conference on System Sciences (HICSS)*, vol. 2019, pp. 2763–2770, Grand Wailea, Hawaii, 2019.
- [21] S. Deepak and B. Chitturi, "Deep neural approach to fake-news identification," *Procedia Computer Science*, vol. 167, no. 2019, pp. 2236–2243, 2020.
- [22] S. Khan, S. Hakak, N. Deepa, B. Prabadevi, K. Dev, and S. Trelova, "Detecting COVID-19-related fake news using feature extraction," *Frontiers in Public Health*, vol. 9, no. January, pp. 1–9, 2021.
- [23] R. Qasim, W. H. Bangyal, M. A. Alqarni, and A. Ali Almazroi, "A fine-tuned BERT-based transfer learning approach for text classification," *Journal of healthcare engineering*, vol. 2022, Article ID 3498123, 17 pages, 2022.
- [24] A. Drif and S. Giordano, "Fake news detection method based on text-features," in *International Academy, Research, and Industry Association (IARIA)*, vol. 23no. 3, pp. 26–31, France, 2019.
- [25] M. K. Elhadad, K. Fun Li, and F. Gebali, "Fake news detection on social media: a systematic survey," in *2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, Victoria, BC, Canada, 2019.
- [26] A. A. A. Ahmed, A. Aljarboub, P. K. Donepudi, and M. S. Choi, "Detecting fake news using machine learning: a systematic literature review," *Journal of Educational Psychology*, vol. 58, no. 1, pp. 1932–1939, 2021.
- [27] Á. Figueira and L. Oliveira, "The current state of fake news: challenges and opportunities," *Procedia Computer Science*, vol. 121, pp. 817–825, 2017.
- [28] O. D. Apuke and B. Omar, "Fake news and COVID-19: modelling the predictors of fake news sharing among social media users," *Telematics and Informatics*, vol. 56, article 101475, 2021.
- [29] N. Guimarães, Á. Figueira, and L. Torgo, "Can fake news detection models maintain the performance through time? A longitudinal evaluation of twitter publications," *Mathematics*, vol. 9, no. 22, 2021.

- [30] T. Granskogen and J. A. Gulla, "Fake news detection: network data from social media used to predict fakes," *CEUR Workshop Proceedings*, vol. 2041, no. 1, pp. 59–66, 2017.
- [31] R. Varma, Y. Verma, P. Vijayvargiya, and P. P. Churi, "A systematic survey on deep learning and machine learning approaches of fake news detection in the pre- and post-COVID-19 pandemic," *International Journal of Intelligent Computing and Cybernetics*, vol. 14, no. 4, pp. 617–646, 2021.
- [32] M. Bhogade, B. Deore, A. Sharma, O. Sonawane, and M. Singh, "A review paper on fake news detection," *International Journal of Advance Scientific Research and Engineering Trends*, vol. 6, no. 5, pp. 94–96, 2021.
- [33] S. Hangloo and B. Arora, "Fake news detection tools and methods—a review," *Communications in Computer and Information Science*, vol. 1, no. August, pp. 1–12, 2016.
- [34] D. de Beer and M. Matthee, *Approaches to Identify Fake News: A Systematic Literature Review*, vol. 136, no. Macaulay 2018, 2021Springer International Publishing, 2021.
- [35] F. D. C. Medeiros and R. B. Braga, "Fake news detection in social media: a systematic review," *The ACM International Conference Proceeding Series*, vol. 3, no. 5, pp. 2–7, 2020.
- [36] A. D'Ulizia, M. C. Caschera, F. Ferri, and P. Grifoni, "Fake news detection: a survey of evaluation datasets," *Computer Science - PeerJ*, vol. 7, no. 2, pp. e518–e534, 2021.
- [37] R. Katarya and M. Massoudi, "Recognizing fake news in social media with deep learning: a systematic review," in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2020.
- [38] N. Guimarães, Á. Figueira, and L. Torgo, "An organized review of key factors for fake news detection," 2021, <http://arxiv.org/abs/2102.13433>.
- [39] S. Raza and C. Ding, "Fake news detection based on news content and social contexts: a transformer-based approach," *International Journal of Data Science and Analytics*, vol. 13, no. 4, pp. 335–362, 2022.
- [40] N. Islam, A. Shaikh, A. Kaiser et al., "Ternion: an autonomous model for fake news detection," *Applied Sciences*, vol. 11, no. 19, pp. 9292–9315, 2021.
- [41] S. Jan, O. B. Tauqeer, F. Q. Khan et al., "A framework for systematic classification of assets for security testing," *Computers, Materials and Continua*, vol. 66, no. 1, pp. 631–645, 2021.
- [42] P. Kaur, R. S. Boparai, and D. Singh, "Hybrid text classification method for fake news detection," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 5, pp. 2388–2392, 2019.
- [43] T. Khan, A. Michalas, and A. Akhunzada, "Fake news outbreak 2021: can we stop the viral spread?," *Journal of Network and Computer Applications*, vol. 190, article 103112, 2021.
- [44] B. Kim, A. Xiong, D. Lee, and K. Han, "A systematic review on fake news research through the lens of news creation and consumption: research efforts, challenges, and future directions," *PLoS One*, vol. 16, no. 12, pp. 1–28, 2021.
- [45] P. Machete and M. Turpin, *The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review*, vol. 12067, Springer International Publishing, LNCS, 2020.
- [46] C. Melchior and M. Oliveira, "Health-related fake news on social media platforms: a systematic literature review," *New Media & Society*, vol. 1, no. 23, 2021.
- [47] C. V. Meneses Silva, R. Silva Fontes, and M. Colaço Júnior, "Intelligent fake news detection: a systematic mapping," *Journal of Applied Security Research*, vol. 16, no. 2, pp. 168–189, 2021.
- [48] M. Orabi, D. Mouheb, Z. Al Aghbari, and I. Kamel, "Detection of bots in social media: a systematic review," *Information Processing & Management*, vol. 57, no. 4, 2020.
- [49] I. Segura-Bedmar and S. Alonso-Bartolome, "Multimodal fake news detection," *Information*, vol. 13, no. 6, p. 284, 2022.
- [50] W. S. Paka, R. Bansal, A. Kaushik, S. Sengupta, and T. Chakraborty, "Cross-SEAN: A cross-stitch semi-supervised neural attention model for COVID-19 fake news detection," *Applied Soft Computing*, vol. 107, article 107393, 2021.
- [51] I. Pilkevych, D. Fedorchuk, O. Naumchak, and M. Romanchuk, "Fake news detection in the framework of decision-making system through graph neural network," in *2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT)*, pp. 153–157, Lviv, Ukraine, 2021.
- [52] S. Preston, A. Anderson, D. J. Robertson, M. P. Shephard, and N. Huhe, "Detecting fake news on Facebook: the role of emotional intelligence," *PLoS One*, vol. 16, no. 3, pp. 1–13, 2021.
- [53] A. Reyes-Menendez, J. R. Saura, and F. Filipe, "The importance of behavioral data to identify online fake reviews for tourism businesses: a systematic review," *PeerJ Computer Science*, vol. 5, no. 9, pp. 1–21, 2019.
- [54] S. Shahin, B. Ang, and N. D. Anwar, *Disinformation and fake news*, Journal Mass Commun, 2022.
- [55] S. Shah Nawaz and P. Astya, "Sentiment analysis: approaches and open issues," in *2017 International Conference on computing, Communication and automation (ICCCA)*, vol. 2017-Janua, pp. 154–158, Greater Noida, India, 2017.
- [56] K. Shu, H. R. Bernard, and H. Liu, "Studying fake news via network analysis: detection and mitigation," *Summer Tutor*, vol. 3, no. 5, pp. 43–65, 2019.
- [57] K. Stahl, "Fake news detector in online social media," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1S4, pp. 58–60, 2019.
- [58] X. Zhang and A. A. Ghorbani, "An overview of online fake news: characterization, detection, and discussion," *Information Processing and Management*, vol. 57, no. 2, article 102025, 2020.
- [59] C. J. Hutto and E. Gilbert, "Vader: a parsimonious rule-based model for sentiment analysis of social media text," in *Proceedings of the international AAAI conference on web and social media*, vol. 4no. 3, pp. 216–225, Ann Arbor, Michigan USA, 2014.
- [60] G. Xu and H. Jin, "Using artificial intelligence technology to solve the electronic health service by processing the online case information," *Journal of Healthcare Engineering*, vol. 2021, Article ID 9637018, 12 pages, 2021.
- [61] D. Berrar, "'Bayes' theorem and naive Bayes classifier," *Encyclopedia of Bioinformatics and Computational Biology*, vol. 1–3, no. January 2018, pp. 403–412, 2019.
- [62] S. L. Ting, W. H. Ip, and A. H. C. Tsang, "Is Naïve bayes a good classifier for document classification?," *International Journal of Software Engineering and Its Applications*, vol. 5, no. 3, pp. 37–46, 2021.
- [63] H. Zhang and J. Su, "Naive Bayesian Classifiers for Ranking," in *Machine Learning: ECML 2004*, J. F. Boulicaut, F. Esposito, F. Giannotti, and D. Pedreschi, Eds., vol. 3201 of ECML 2004. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2004.

- [64] K. P. Murphy, "Naive Bayes classifiers generative classifiers," *Bernoulli*, vol. 4701, no. October, pp. 1–8, 2007.
- [65] S. Karthika and N. Sairam, "A Naïve Bayesian classifier for educational qualification," *indian journal of science and technology*, vol. 8, no. 16, 2021.
- [66] W. Dai, G. R. Xue, Q. Yang, and Y. Yu, "Transferring naive Bayes classifiers for text classification," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 1, pp. 540–545, 2022.
- [67] C. Lin, "Support vector machine solvers," *Large scale kernel machines*, vol. 3, no. 1, pp. 301–320, 2007.
- [68] L. Zhang, W. Zhou, and L. Jiao, "Wavelet support vector machine," *IEEE Transactions on Systems, Man, and Cybernetics—Part B*, vol. 34, no. 1, pp. 34–39, 2004.
- [69] I. Sánchez-Torné, J. C. Morán-Álvarez, and J. A. Pérez-López, "The importance of corporate social responsibility in achieving high corporate reputation," *Corporate Social Responsibility and Environmental Management*, vol. 27, no. 6, pp. 2692–2700, 2020.
- [70] X. Zhou, A. Jain, V. V. Phoha, and R. Zafarani, "Fake news early detection: an interdisciplinary study," pp. 3207–3208, 2019, <http://arxiv.org/abs/1904.11679>.
- [71] Y. Wang and J. Y. Xu, "An autonomous semantic learning methodology for fake news recognition," in *2021 IEEE International Conference on Autonomous Systems (ICAS)*, pp. 1–6, Montreal, QC, Canada, 2021.
- [72] K. M. Leung, *Naive bayesian classifier*, vol. 2007, Polytechnic University Department of Computer Science/Finance and Risk Engineering, 2007.
- [73] Z. Liang, J. Liu, A. Ou, H. Zhang, Z. Li, and J. X. Huang, "Deep generative learning for automated EHR diagnosis of traditional Chinese medicine," *Computer Methods and Programs in Biomedicine*, vol. 174, pp. 17–23, 2019.
- [74] M. Basaldella, F. Liu, E. Shareghi, and N. Collier, "COMETA: a corpus for medical entity linking in the social media," in *EMNLP 2020. 2020 Conference on Empirical Methods in Natural Language Processing*, vol. 2no. 1, pp. 3122–3137, 2020.
- [75] H. H. Deyab and R. B. Atan, "Orchestration framework for automated Ajax-based web application testing," in *2015 9th Malaysian Software Engineering Conference (MySEC)*, pp. 1–6, Kuala Lumpur, Malaysia, 2015.