Machine learning for False Information Detection in Social Internet of Things

Mahmoud M. Ismail[1], Nihal N. Mostafa[2], Esmeralda Kazia[3], Ibrahim Elhenawy[4]

[1]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt

[2]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt

[3]Department of Applied and Computer Sciences, Barleti University, Albania

[4]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt

Emails: mmsabe@zu.edu.eg; nihal.nabil@fci.zu.edu.eg; ict.co@umb.edu.al; ielhenawy@zu.edu.eg

Abstract

By capitalizing on object relationships and local navigability, the social internet of things (SIoT) is one of the burgeoning paradigms that could solve the technical challenges of conventional IoT. Because of this paradigm's capacity to combine conventional IoT with social media, it is possible to create smart objects and services with greater utility than those created using conventional IoT infrastructures. In recent years, scholars have become interested in SIoT, leading to a plethora of works examining various mechanisms for providing services and technologies within this context. In this vein, we present a comprehensive review of recent research covering important aspects of SIoT. In this research, we give a detailed justification for the function of several machine learning paradigms and provide a practical application of it to unexamined concerns relating to erroneous data and other social IoT. First, we give a classification of false news detection approaches and an analysis of these techniques. Second, the potential uses for detecting fake news are examined at length, including how it might be applied to the areas of fake profile detection, traffic management, bullying detection, etc . We also suggested a detailed review of the possibilities of machine learning algorithms for detecting bogus news and intervening in social networks. In our paper, we introduce categories of fake news detection methods providing a comparison between these methods. After that, the promising applications for false news detection are extensively discussed in terms of fake account detection, bot detection, bullying detection, and the security and privacy of SIoT. After all, A thorough discussion of the potential of machine learning approaches for fake news detection and interventions in SIoT networks along with the state-of-the-art challenges, opportunities, and future search prospects. This article seeks for aiding the readers and researchers in explaining the motive and role of the different machine learning paradigms to offer them a comprehensive realization of so far unexplored issues related to false information and other scenarios of SIoT networks.

Keywords: Social Internet of Things; Machine learning; False Information; Data Fusion

1. Introduction

The Internet of Things (IoT) is a leading concept that connects numerous diverse smart objects (e.g., sensors, cellphones, computers, and actuators) with varying degrees of computational and networking functionality [1, 2]. Using a variety of procedures, these intelligent objects are able to exchange information, collaborate, and ultimately achieve a common goal. These Internet of Things devices have already proven their worth in a variety of contexts.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

[3]. As time goes on, more and more industries will use IoT to enhance their services and the lives of their customers. In Figure 1, we showcase the development of the Internet of Things field over the course of two decades. Consistent with these tendencies, people all over the world have witnessed the arrival of the era of smart connected vehicles, which has changed the conventional vehicle Ad-hoc networks into Internet-of-Vehicle (IoV) [4, 5]. In this new paradigm (for instance, Internet of Things to Internet of Vehicles), smart objects are used to establish a structured hierarchy between automobiles. IoV has benefited greatly from emerging IoT technology. On the other hand, sizable IoT acceptance in any new application domain is hampered by heterogeneity and scalability issues [6]–[8]. The social internet of things (SIoT) is a recent innovation that uses human interrelationship-making capacity as a basic tenet to overcome the difficulties of diversity and expandability that plague traditional IoT [9]. To build a system wherein items can define social connections and could undertake required responses, the IoT and social networking frameworks have converged [10, 12]. Objects in the SIoT environment can communicate with one another and act in a socially intelligent manner. The services in the network are available for both request and supply [1]–[13]. Fisk's theory, which described the ties that bind people together, served as inspiration for the SIoT's adoption of a social framework [14]. By incorporating social artifacts into the IoV, a new approach called the Social Internet of Vehicles (SIoV) emerged in the fourth stage [15], [16] to improve upon the services provided by the IoV. Because of this awareness, connected gadgets can interact with one another based on commonalities in their environments and their hobbies [17]. The newest development in SIoT is the Social Collaborative Internet of Things (SCIoT), wherein social items work together by communicating and sending knowledge to complete a task [18], [19]. Instead of depending on server-oriented design, these frameworks make widespread use of social connections to allocate the services needed. As a result, it is crucial to discuss the most recent advancements in the SIoT domain from a variety of vantage points. From the point of view of device and social interaction, Figure 1 shows how the SIoT has developed over time [20]. Figure 1 shows the development of social existence along the horizontal plane and the enhancements in decision-making utilizing living person and entity information together along the vertical axis [21]. As can be seen in Figure 1, the SIoT has greater potential in terms of both public interactions and smart decision-making [22]. Consequently, studies in this area have blossomed in the latest days [23], [24], and [25].

Fake news is all the rage these days, which refers to the intentional or unintentional expansion of misleading information through public and **SIoT** platforms. Fake news is defined as "any form of false, inaccurate, or misleading information designed, presented, and promoted with the intent of causing public harm or profit" [1]. Since most of our lives are particularly associated online through public platforms, increasingly people are seeking out and consuming news from SIoT platforms rather than traditional news organizations like newspapers or television which fake news on SIoTcan be less expensive and able to discuss the news with friends or readers and takes less time compared to traditional organizations. Also, users of online media are panicking about the increasing digitization, with the possibility that the news may become fake, and the majority of people do not question the veracity of information before passing it on, thus becoming a member of the influential group that creates and spreads fake news. It should be indicated that fake news is a global problem that affects people all over the world. People and communities alike may

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

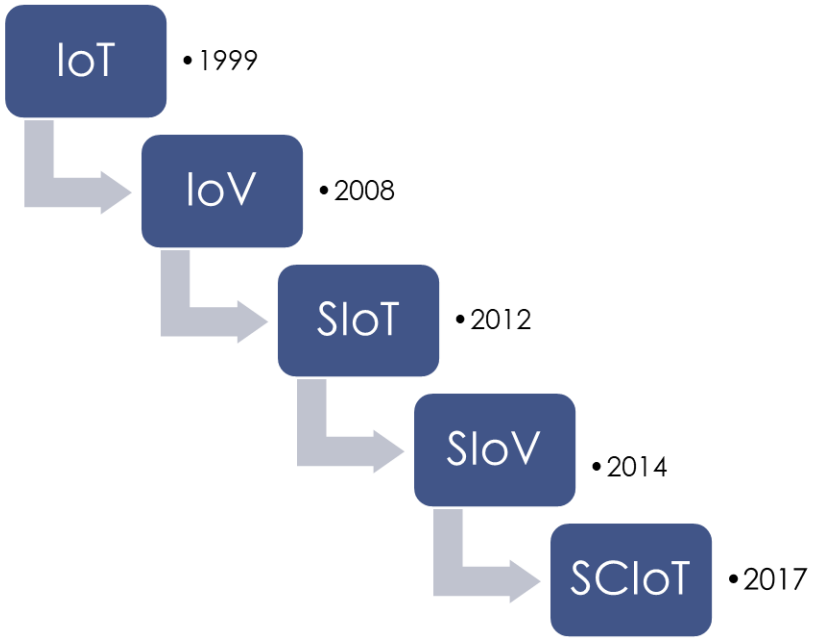

Figure 1.: Illustration of the evolution of IoT in social integration

suffer as a result of the widespread circulation of false information. To begin, the prevalence of fake news threatens to upset the credibility equilibrium of the news industry. During the 2016 US presidential election, it is evident that the most famous false information was actually more broadly accepted on Facebook compared to the most prevalent truthful national media [2]. Users' information is sold to Cambridge Analytica, the firm held to account for Trump's election campaign. Because of this, inaccurate information about the opposing candidate was disseminated. Second, the goal of fake news is to get people to believe things that aren't true or are biased. False news is frequently used by propagandists to impart key propaganda or to appear knowledgeable. Some news outlets claim that Russia is spreading false information by using fake social media profiles and automated software for social media platforms (SIoT bots) [3]. In addition, many people believed and spread false information about vaccines during 2020 COVID-19 pandemic [4]. The effectiveness of vaccines is harmed as a result of this. According to Francesco Rocca, president of the International Federation of Red Cross and Red Crescent Communities, disinformation is the second global health crisis in recent memory.

Nowadays, determining whether a news clip is fake or real is very simple, feasible, and worthwhile. In today's information age, the Internet of Things (IoT) and Artificial Intelligence (AI), there may be much better and multiple options to do the task if it were just simple matching and comparing, but this job needs a much wider insight of Literature, **SIoT** interactions, human speech, logics, possibilities, and so on. The ability to detect fake news on online media raises a number of research problems challenging, where there are several aspects of this issue that make it particularly complicated for detection and recognition such as true evidence may be cited in a false context to support a false claim in fake news for misleading readers and making it non-trivial and difficult to detect [5]. Nowadays, researchers are doing their efforts for making fake news detection that is not only efficient but also explainable [6]–[9].

1.1. Related Surveys

Recent years have seen the introduction of a variety of survey-based approaches to the problems of false information detection in SIoT, classification, and avoidance. Each research has a unique focus, whether it is on textual data, visual data, audio data, or a combination of these. Some others conduct comprehensive research on all the facets of fake news in that language. Therefore, the most contemporary and extensive research works in this area are explored and discussed below, followed by a discussion of the key differences between those studies and the one under investigation. For example, the work [15] presented the research in an effort to thoughtfully explore cutting-edge methods for detecting fake news in **SIoT** platforms. Initial emphasis is placed on the negative effects of disseminating

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

false information. Next, we discuss the dataset and NLP methods employed in earlier studies. An in-depth survey of deep learning-based methods has been presented, allowing for the systematic classification of illustrative approaches. the work [16] provided an in-depth analysis of the various methods currently in use to spot fake news, then trained a variety of Machine Learning (ML) models on the self-aggregated dataset in an effort to identify false news items. Success in correctness and other assessment metrics followed the implementation of these models via hyper-tuning of parameters. More, the work [17] surveyed the existing research on the topic of rumor position characterization in highly interconnected social media platforms (OSNs). In particular, it provided a detailed explanation of various methods and evaluate their relative merits. Also, it provided many datasets that can be used for this purpose and discuss the limits of each. Finally, it concluded with a discussion of challenges and potential future directions that can help to motivate even more pertinent research. Using current detection techniques and approaches, the study [18] presented a complete survey on fighting false news and examines the problems associated with its detection. Fake news has been met with solutions that take into account the many different factors involved in the fight against it, including the technological, the economic, and the psychological. Further, it investigated stakeholder responses to the propagation of fake news by using the fake news combat spectrum. Finally, some technological strategies for addressing the problems of fake news and the potential they bring have been discussed. In [19], a new taxonomy is proposed for traits that can be used to identify malevolent individuals and bots, and we have provided a thorough overview of the state-of-the-art ways of doing so. The study also tried to steer clear of the critical issue of fake news identification by highlighting some major issues and prospective future subject areas for the benefit of academics who are just getting started in this domain. In [20], the authors reviewed the current state of the art for trust prediction models in SIoT networks, categorized them according to various criteria, and provide some suggestions for future research. Table 1 summarises the previous survey articles as well as our own research findings. This survey-style study on fake news detection tries to fill in the gaps and build on the successes of earlier studies in the field.

Table 1: Analytical comparison between related survey according to different criteria they cover.

Study	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**
[21]	Yes	No	No	Yes	No	Yes	No	Yes	No	No	No
[16]	No	No	No	No	Yes	No	No	No	No	No	No
[20]	No	No	Yes	No	No	Yes	No	No	Yes	No	No
[17]	No	No	Yes	Yes	No	No	Yes	No	No	No	Yes
[18]	No	Yes	No	No	Yes	No	Yes	No	No	No	No
[22]	No	No	Yes	No	No	Yes	No	Yes	Yes	No	No
[19]	No	No	No	Yes	No	No	No	Yes	No	No	No
[23]	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No
[24]	Yes	Yes	Yes	No	No	No	No	No	No	No	Yes
[29]	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No
[27]	Yes	No	No	No	No	Yes	No	No	Yes	Yes	No
[25]	Yes	No	Yes	Yes	No	No	Yes	No	No	No	Yes
[26]	Yes	No	No	No	No	Yes	No	Yes	No	Yes	No
[28]	Yes	Yes	No	No	No	No	Yes	No	Yes	No	No
[15]	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes
This	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

C1=Taxonomy, C2=Dataset, C3=Metrics, C4=Preprocessing, C5= Experiment, C6=Applications, C7=Open issues, C8=ML, C9=CNN, C10=RNN, C11= Language model

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

1.2. Motivation and Research Gaps

In today's hyper-connected world, where millions, if not billions, of people, are exchanging information and exchanging data in real-time across a wide range of online services, SIoT networks are in a constant state of data creation and transmission. The veracity of content circulating on SIoT networks is unclear in contrast to traditional news sources due to the liberation of free expression.

Over the past several years, we have seen a dramatic increase in the number of people actively engaging in informational research and dissemination via SIoT networks. Users' tastes are being heavily influenced by the publicly available content of SIoT media. In this respect, the notion of "Fake news" has been all-pervasive in the wake of the "2016 US presidential campaigns," where it was speculated that the widespread dissemination of false themes during the elections had a significant impact on the final tally. n light of this, the works in this collection review and analyze different MLapproaches employed to deal with the problems caused by fake news, taking into account the current condition of information falsification in terms of ecosystem, various platforms for data exchange, and creation, insightful commentary, and real instruments. This study focuses on identifying fake news in SIoT networks thru the various research achievements pertaining to ML viewpoints, discussing the architecture, improvements, challenges, and opportunities of machine learning for reliable SIoT networks in order to provide a comprehensive and structured explanation. This effort was launched to aid in the accurate assessment of the connection between machine learning and trustworthy SIoT networks, specifically concerning the effective detection of rumors and fake news. Moreover, the authors of this study hope that it will serve as a valuable resource for future investigators, the AI community, machine learning engineers, and novices alike.

False information detection is a difficult problem that is still in its beginning stages, necessitating further research. As a result, it is critical to pursue additional research avenues to improve current fake information detection approaches [23]. One of the intriguing difficulties is slightly earlier fake information detection, which aims to supply early warnings of fake information throughout the spreading process. Because early detection of fake information reduces the spread of fake information on various **SIoT** media networks [24]. Manual fact-checking, which includes the need for experts and also crowdsourced judgment, has produced some results in determining the veracity of certain news content. However, manual fact-checking still has several limitations, such as labor and the amount of time needed, especially when dealing with big amounts of data. On the other hand, the automatic fact-checking approaches can handle huge amounts of data in a short period of time, but it has many limitations because most automatic ML algorithms trained to identify fake news are related to specific linguistic and text-based contents, and also style [25] Which most of earlier researches designed to detect fake information using ML approaches in which features was obtained in a manual process, which is a time-consuming and labor-intensive task, as well as the solution is through using deep learning, where DNN approaches can effectively capture hidden representations, resulting in superior performance in comparison to ML models [26]. Rumor detection research should begin by putting state-of-the-art activity detection methods to the test in the context of rumors. A rumor detection system must determine whether or not a detected event is a rumor in addition to what event detection systems do. Determining whether a single **SIoT** media post reports a rumor or not is challenging if only its content is used, and also the lack of publicly existing datasets has been a significant barrier to the implementation of rumor classification systems [12]. We encourage researchers to make their datasets available for further research across different datasets, allowing the research community to compare their methodologies.

Another attractive issue that everybody needs to face is the prospect of a news snippet being fake nowadays and turning out to be true in the near or distant future, which makes the fake news future a hilly road. There should be a few accurate sources of sheer actual news from which to check facts and compare the authenticity of their news stories, and the methodology or approach should be capable of delivering the resulting tagging promptly [13]. Aggregation techniques improve feature weights by combining various feature representations into a weighted manner, and each feature like source credibility, news content style, or social response, has a few issues in terms of explicitly predicting false news [11]. Because fake news frequently combines true and fake statements, this could make much more sense to estimate the possibility of fake news rather than generating a binary value, and probabilistic models estimate probability distributions of class labels (false/real news). In the raw feature space, false information content or social contextual information might well be noisy, so projection approaches are helpful for classification [11].

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

Fake news is aimed to allow it challenging for individuals to recognize false news by taking advantage of our cognitive abilities, feelings, and intellectual biases. Furthermore, it is hard for computational approaches to identify false information because of the manner fake news is shown like real news and uses some true evidence with the fake information [22]. The majority of the existing system is performed through supervised learning models, Because of the large amount of unlabeled data from **SIoT** media, unsupervised models must be developed. Also, a lot of the work is concerned with linguistic features in English language text, and other common and provincial languages are just not being considered at this time [16]. Supporting explainability has a strong interest in ML and AI domain, in which the fake news detection models need to be more interpretable and understandable for users (i.e., decision trees, and rule-based models). But now the research is heading toward deep learning models which these models are black box models, so the researchers need these models more explainable. Traditional approaches in fake news detection provide the prediction without explanation (why this news is fake), so more challenging to add the explainability to fake news detection models [8], [9].

1.3. Contributions

Instead of relying on existing survey research [56-60], this work provides comprehensive coverage to discuss the function of deep learning in the identification of information pollution, rumors, and fake news via SIoT networks.

- First, the paper asserts, categorizes, and characterizes the false information ideas in SIoT networks, making it easier to grasp the basic notion of false information and its essential qualities. This is the first attempt the authors are aware of to tackle these ideas head-on, to provide readers with a holistic understanding of tainted data and the risks it poses.
- Second, this survey provides a synopsis of the current research on the use of ml algorithms and deep learning techniques to identify and counteract online misinformation, such as fake news, rumors, and other fabrications. Various facets of these methods are dissected throughout the debate, such as data modalities, learning strategies, input representations, and recognition levels. The impact of fake news on the survey is also taken into account from a machine-learning perspective.
- Third, this study provides and examines the application areas connected to the detection and intervention of fake news, such as the detection of fraudulent accounts, bots, bullying, and the security and privacy of SIoT media.
- Finally, the current state-of-the-art and research gaps concerning identifying and detecting various types of information pollution are discussed. As a result, the reliability of SIoT networks can be enhanced by using these insights to identify areas where machine learning could be applied to combat the difficult problem of false information spread via SIoT media.

2. DEFINITIONS AND FOUNDATIONS OF FAKE NEWS

2.1. Definitions

The research of false facts covers a set of concepts that frequently overlaps but have different meanings like fake news, rumors, or hoaxes, among others. We differentiate between such concepts by providing community-accepted definitions:

- Misinformation [27] is defined as any piece of data whose text conflicts with the epistemic consensus obtained through the systematic application of a methodology. For example, Misinformation can be found in clauses made by the team like anti-vaccine activists, who fail to admit scientific evidence [28].
- Disinformation is a form of misinformation that is intended to influence and misdirect public perception [17]. Disinformation encompasses all types of information dissemination whose goal is to come back fame or wealth to the creator, whereas disinformation manifests itself in the shape of misleading news and hoaxes.
- Fake news is information that has been posted in the news media that is untrue. The term "false news" refers to any form of news that contains one or several untrue facts. Fake news contains both misleading news, or news that is designed to control and manipulate, and unplanned fake news stories, or the documentation of unauthenticated false information. All these forms of news have distinct origins. While misleading news is intended to spread propaganda, non - intentional fake news is motivated by the desire to obtain an audience through the use of untrustworthy sources.
- Rumor Zubiaga et al. [12] classify a rumor as " an item of circulating information whose veracity status is yet to be verified at the time of posting". Rumors usually being created within a **SIoT** media network. There are several kinds of rumors that have been used in automatic detection and widely used

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

datasets in this classification: true rumor "rumor which has been proved", false rumor "rumor that has been rejected with real evidence", and unproven rumor "rumor which has not been proven or rejected yet".

- Satires and parodies contain rumor content, such as irony and sarcasm. It is possible to identify its deceptive nature.
- Conspiracy theories that are difficult to prove true or untrue.
- Spams are any advertisement that takes to reach audiences through the use of **SIoT** media without their permission. Spams are generally viewed as unwanted messages, primarily e-mails.
- Scams and hoaxes are motivated solely for entertainment or to deceive persons.
- Click baits utilize miniaturized pictures or sensationalist headlines to persuade persons to view and share questionable content. Clickbait is mostly akin to misleading advertising.
- Stance is the attitude of people toward a specific objective or claim. Stances forward into objectives like legal abortion include both for and against attitudes. There are several types of stances: supporting, asking questions, trying to deny, and providing feedback.

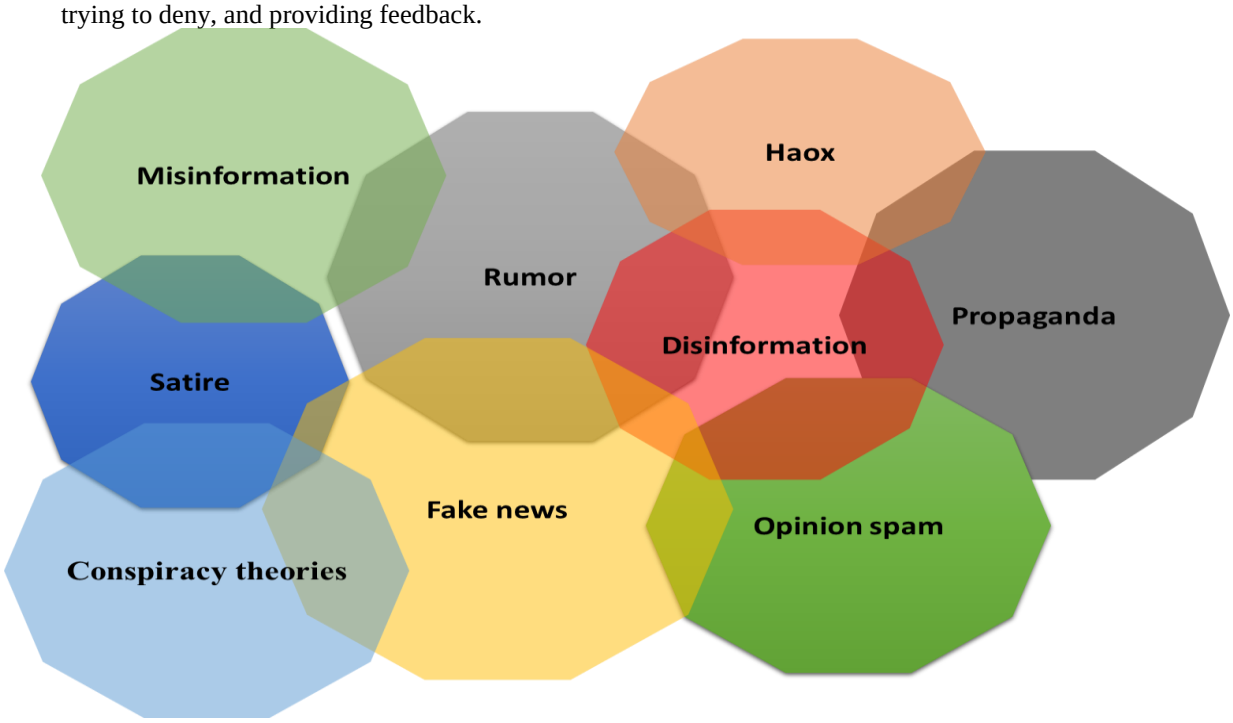

Figure 2: Venn diagram indicating different categories of false information over social networks

- A bot is an application program that manages a **SIoT** media profile and performs routine tasks like posting or reposting other users' messages [29]. These **SIoT** bots evolve, integrating sophisticated rules and behavior patterns for mimicking people within networks and being extremely challenging to identify. In current years, the relationship between bots and political campaigns has received a lot of attention, and their capability to aid in the propagation of fake information on **SIoT** media [30].

See Figure 2 for a Venn diagram depicting the intersection and union of various information pollution setups. While it's true that different forms of disinformation have their own unique quirks, the authors of this paper use the names of various subfields interchangeably in several places to provide a holistic look at disinformation in IoT networks. This new taxonomy classifies and compares various types of disinformation based on the following five criteria: first, A breakdown of what each class entails. Second, veracity, which means nothing untrue is included. Third, intent, or if the data is meant to deceive or entertain the world. Fourth, the public's reaction to each classification. Fifth, the freshness of the data.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

2.2. Fake News Categorization

False data can take the form of tweets, postings, blogs, photos, discussions, tales, or defiant news and propagate rapidly over SIoT networks. Information pollution takes several forms, none of which are inherently inconsistent but all of which have a certain degree of heterogeneity that allows us to classify them with precision. [31].

A. Components of Fake News

Some key components for characterizing fake news should be known in order to better comprehend the extent and diversity of online fake information [15].

- **The Originators:** The originators or the spreader of online false information could be both real people and non-people. Real people, and fake news originators include both innocuous writers and viewers who share false information unwittingly and harmful users who intentionally make misleading information. **SIoT** bots and cyborgs are the most common types of non-people originators.
- **Victims:** Target Victims are the primary targets of online fake news. They could be online **SIoT** media consumers or consumers of other online media portals. The targets of the news can be teenagers, electors, family members, elderly citizens, and so on, depending on the objective of the news.
- **News Content:** The body of the news is referred to as news content. It includes tangible substance such as author, headline, message body, and image or video and intangible content such as objectives, feelings, and subjects.
- **SIoT Context:** describes how news is disseminated on the Web, social context analysis includes two types: (i) User network analysis: how online users are involved in the news, (ii) broadcast pattern analysis: the temporal pattern of the dissemination.

B. Fake News Detection Approaches:

SIoT science studies have recognized fake news from various aspects and presented a broad classification of various forms of fake news. The methodologies for detecting fake news primarily focus on news content, **SIoT** context, and structure. To extract discriminatory features of fake news, various types of feature representations can be developed (see Figure 3).

- **News Content:** news content-based approaches extract distinguishing characteristics of fake news through linguistic-based and visual-based features.
  - **Linguistic-based:** linguistic characteristics produce specific writing styles, sensational feelings, and headlines that are frequently used to detect fake news [32], in which linguistic characteristics are extracted from textual information at various levels of document structure: lexical characteristics (characters, token levels), (ii) syntactic characteristics (phrases, and documents levels) To encapsulate the numerous characteristics of fake news [33].
  - **Visual-based:** visual-based type of fake news relies heavily on visual analysis as content and visual-based characteristics are retrieved from visual components, which contain the use of images, video, and/or a combination of both [34].
- **SIoT Context:** the key components of social context-based techniques are user-based, post-based, and network-based.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

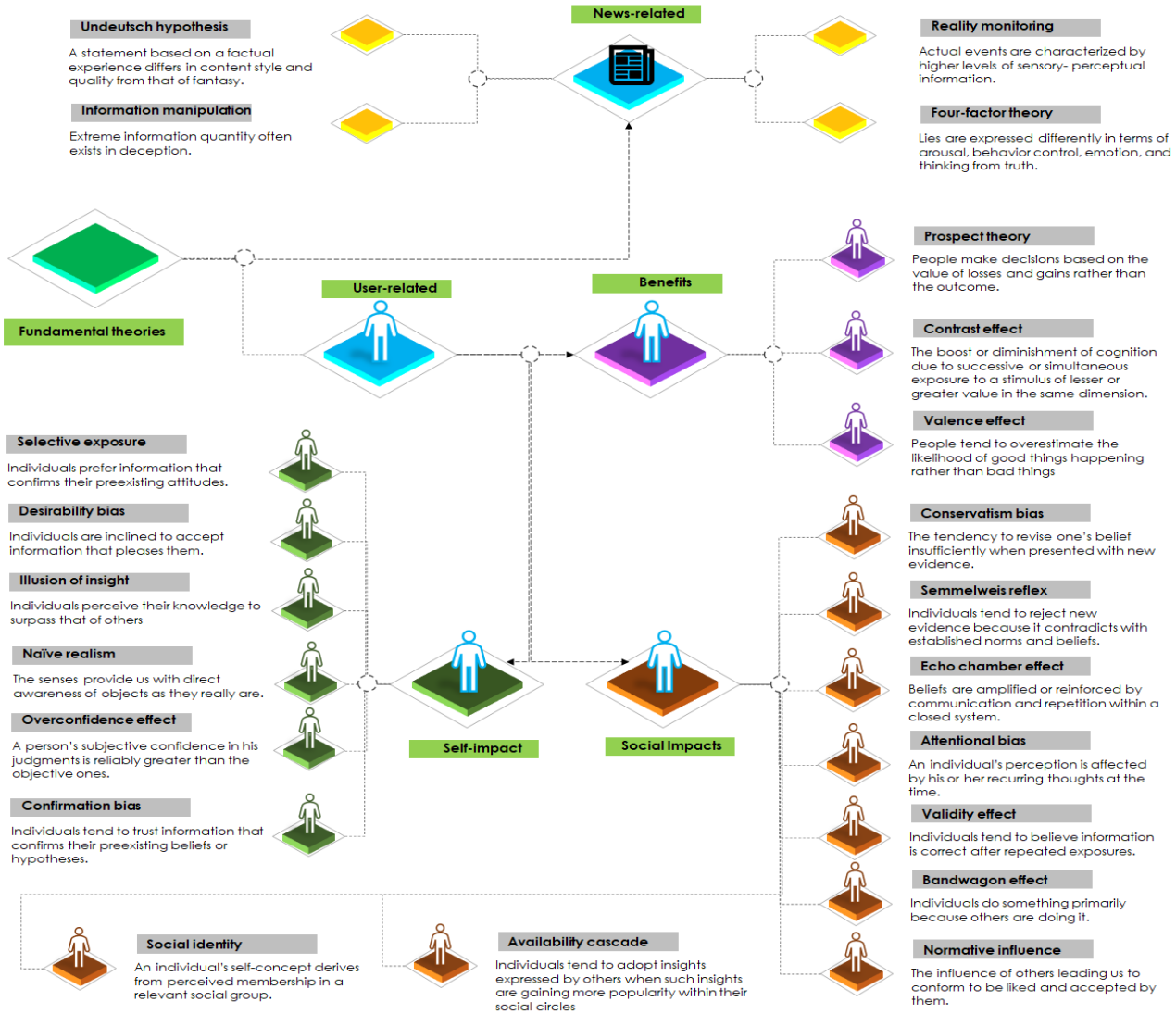

Figure 3:Basic Theories in Societal Sciences as well as Finances

1) **User-based:** user-based types are focused on a specific audience for fake profiles with their age ranges, sex, culture, and so on, user-based features are obtained from their profiles to capture both global and local changes for user profile features across propagation pathways to identify fake news [36].
2) **Post-based:** post-based fake news is primarily focused on **SIoT** networking sites to aid in the detection of possible fake news based on broad public interactions outlined on posts. Posts have the following characteristics: stance (users' perspectives on the news) [34], topic [37], and credibility (degree of reliability) [38]. A post can be a Facebook post with an image or video and caption, a tweet, a meme, or something else.
3) **Network-based:** Network-based news is geared toward specific members of a specific organization who are associated in some way; this ideology is also applied to groups of friends on Facebook and groups of mutually connected individuals on LinkedIn. Network-based features are obtained by building certain networks: diffusion network [39], interaction network [40], and propagation models [41].

Finally, hybrid methodologies take into account and combine multi-modal background information about the source tweets [45].

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

2.3. Basic Principles

The field of machine learning known as natural language processing (NLP) focuses on teaching computers how to interpret, analyze, and even create written and spoken language. Word embedding and data pre-processing make up the NLP technology. Significant progress in NLP has been made recently thanks in large part to the application of ML methods [41]. To give computers an understanding of human language, the human language should be converted into a mathematical formalism.

2.3.1. Pre-processing

Attribute-based data representation, attribute binarization, attribute transformation, attribute persistence, and attribute management in the face of data loss and obfuscation all necessitate preprocessing. There are a variety of visualization methods that can be useful during the preliminary processing of data. Since social media information sources are disjointed, unstructured, and noisy, a careful pre-processing method is necessary to absorb the information in a neural net for fake news identification. It is well known that data pre-processing can reduce computing time and storage needs during the learning phase. Moreover, text pre-processing prevents every ingests of noisy data, reducing the influence of artifacts on the learning process. After appropriate text pre-processing, the data acquire a rational structure. The most evocative adjectives were also included. When scholars tried to detect fake news using only the characteristics, without any data cleaning or pre-processing, they were only 78% accurate. The accuracy jumps to 93.0% when the pre-processing procedures are taken and irrelevant data is discarded. Numerous research employs pre-processing techniques such as data quality evaluation, dimensionality reduction, and dataset splitting to improve data accuracy and efficiency [20-25]**.**

Information is typically culled from a wide variety of normally trustworthy but format-variant sources. More time is spent on handling data quality issues when working on a machine learning challenge. The expectation of flawless data is unrealistic. There could be inaccuracies because of human error, problems with the data collection procedure, or the limitations of available measuring tools. The ineffectiveness of many fake news detection programs can be traced back to the quality of the datasets they use. In light of this, it should come as no surprise that the success of a machine learning project is highly dependent on the quality of the data used in said project. However, few research guarantees the accuracy of the data they employ. To improve their fake news identification accuracy, S and Chitturi [41] downloaded the George McIntire dataset from GitHub and removed rows that lacked labels as part of the clarification procedure. Duplicate and low-quality photos were eliminated by Wang et al. [44] to improve the overall quality of the collection. Removal of URLs, lowercase and hashtag characters (#), mention characters (@), and numbers were added to the data cleaning method by [45].

Train, test, and validation sets can be created from the dataset. The term "training set" describes the data set used for fine-tuning the parameters. It is common to practise to fine-tune a model's settings by comparing its predictions against a validation set of data. The term "test set" is used to describe a collection of data used exclusively for the purpose of evaluating the effectiveness of a fully described model. Despite the fact that many studies on fake news identification split their dataset into training, validation, and test sets [15-20], very few studies have employed only the training and test sets. Statistics show that 70:30, 80:20, and 60:20 splits work well for detecting bogus news. The 80:20 rule is often referred to as the Pareto principle (for many results, around 80% of consequences arise from 20% of the causes). Using the ratio that was used by every study is usually a solid bet.

Tokenization is the process of separating a text into its individual words. That works for any sort of persona. The most popular method of tokenization involves the use of the space character. Stemming refers to the practice of removing a terminal letter to reveal a word's root. Stemming typically involves the elimination of affixes of derivation. When one term is formed by adding another, this is called an inflectional affix. Most often, the derivative term belongs to a different group of words than the one from which it was derived.

Lemmatization is a text normalization process that aims to eliminate inflectional endings [43]. It does this by analyzing words semantically, producing the root version of bloated terms, and removing them. A derivational termination is a string of letters added to the end of a word to change its connotation. S, bat, and bats are all derivational ends.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

2.3.2. Metrics

Evaluating the results produced by a machine learning model is an essential part of any predictive modeling workflow. Once a model is built, it may have a superior classification result, but it still needs to be tested to see if it can solve the original problem. However, it is typically not possible to make this call based solely on classification accuracy. Alternative evaluation criteria are required for accurate assessment. It is simple to develop a model, but much more difficult to develop a strategy that shows promise and can be evaluated by the inspection metric. Many different indicators are used to determine the model's effectiveness. A crucial tool for setting up and organizing an assessment is the evaluation matrix. A summary of the model's effectiveness on the test set in comparison to the true values is displayed in the confusion matrix. It discusses the good and bad outcomes of the model and how successful it has been. Metrics including accuracy (A), precision (P), and recall (R) were evaluated by scholars [40, 54, 58] to evaluate the efficacy of their models. Metric selection is totally dependent on model structure and method of execution. We present various measures for assessment that have been utilized extensively in prior research [30-14].

3. FALSE INFORMATION ANALYSIS

Machine learning algorithms have increasingly been the subject of extensive study and application in the detection of fraudulent information, and they have shown promising results compared to more conventional methods of spotting such data. The purpose of this part is to provide a comprehensive overview of the current state of the art in the ML and DL literature pertaining to the identification of fake news. Figure 4 provides a taxonomy of machine learning methods based on five distinguishing characteristics. This encompasses the approach to learning, the mode of operation, the input format, the kinds of data, and the level of detection. Below, we compare and contrast much research from various methodological traditions in greater detail.

3.1. Type of Data in News

We describe the various kinds of data that make up media articles; there are four main formats that utilize their news [31].

1) **Text:** Text linguistics is a part of linguistics that concentrates on text as a communication process. It has more than just a phrase and tokens; it has tonality, grammatical structures, and semantics that enable dialogue analysis.
2) **Multimedia:** It is, as the name implies, an amalgamation of various forms of media. Images, video, audio, and graphics are all included. That's very visual and immediately grabs the attention of the audience.
3) **Hyperlinks or Embedded Content:** Hyperlinks allow authors to attach to diverse sources and acquire viewers' confidence by asserting the news story's hypotheses. With the rise of online media, authors tend to instill a screenshot of a related **SIoT** networking post like a Facebook post, a tweet, a YouTube video, a sound cloud clip, and an Ingram post.
4) **Audio:** Although audio is aspect of the multimedia type, it is a separate medium that can be used as a source of news. This component comprises podcasts, broadcast networks, and radio services, and this medium attains a larger number of people to share the news.

3.2. Input Representation:

Words are a good place to start when studying representation strategies in fake news because they are the smallest units in natural languages. So, there are diverse ways to represent fake news inputs.

1) One-hot vector is the simplest way to represent a word in a computer-readable manner (e.g., using a vector), which has the same dimension as the vocabulary size and assigns 1 to the word's corresponding position and 0 to others, and hardly comprises any semantic information about words other than the ability to distinguish them from one another.
2) n-gram models are one of the earliest ideas in word representation learning. It's simple: when we need to guess the next token in a sequence, we typically look at some prior statements. These probabilities are suitable for determining tokens in sequences and also for forming vector representations of words because they reflect word meanings. It became the foundation among several NLP models, ranging from word2vec to BERT.
3) Bag-Of-Words (BOW) models consider a manuscript to be a bag of its words, ignoring the order in which these words appear in the manuscript. As a result, the manuscript can be represented as a vocabulary-size vector, with

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

each word in the manuscript corresponding to a unique and nonzero dimension. Then, for each word, a score (e.g., the number of occurrences) can be computed to indicate the weights of these words in the document.

4) Many methods based on Neural Probabilistic Language Model (NPLM) have emerged, which embed words into distributed representations and use the language modeling objective to optimize them as model parameters. Word2vec, GloVe, and fastText are some well-known examples. Despite differences in detail, all of these methods are very efficient to train, make use of large-scale corpora, and have been widely used as word embeddings in many NLP models.
5) In addition to using larger corpora, more parameters, and more computing resources than word2vec, they also take into account complex contexts in text. Instead of assigning a fixed vector to each word, ELMo and BERT use multilayer neural networks to calculate dynamic representations for the words based on their context, which is especially useful for words with multiple meanings. Furthermore, BERT initiates (though does not originate) a new fashion of the pretrained fine-tuning pipeline. Previously, word embeddings were simply used to represent the input. However, after BERT, this is becoming a widespread procedure to continue using the same neural network structure, such as BERT, in both pretraining and fine-tuning, which is taking BERT parameters for initialization and fine-tuning the model on downstream tasks. This takes us to Pre-trained Language Models (PLM) which implicitly encapsulate a wide range of linguistic features and styles within the parameters of their multilayer network.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

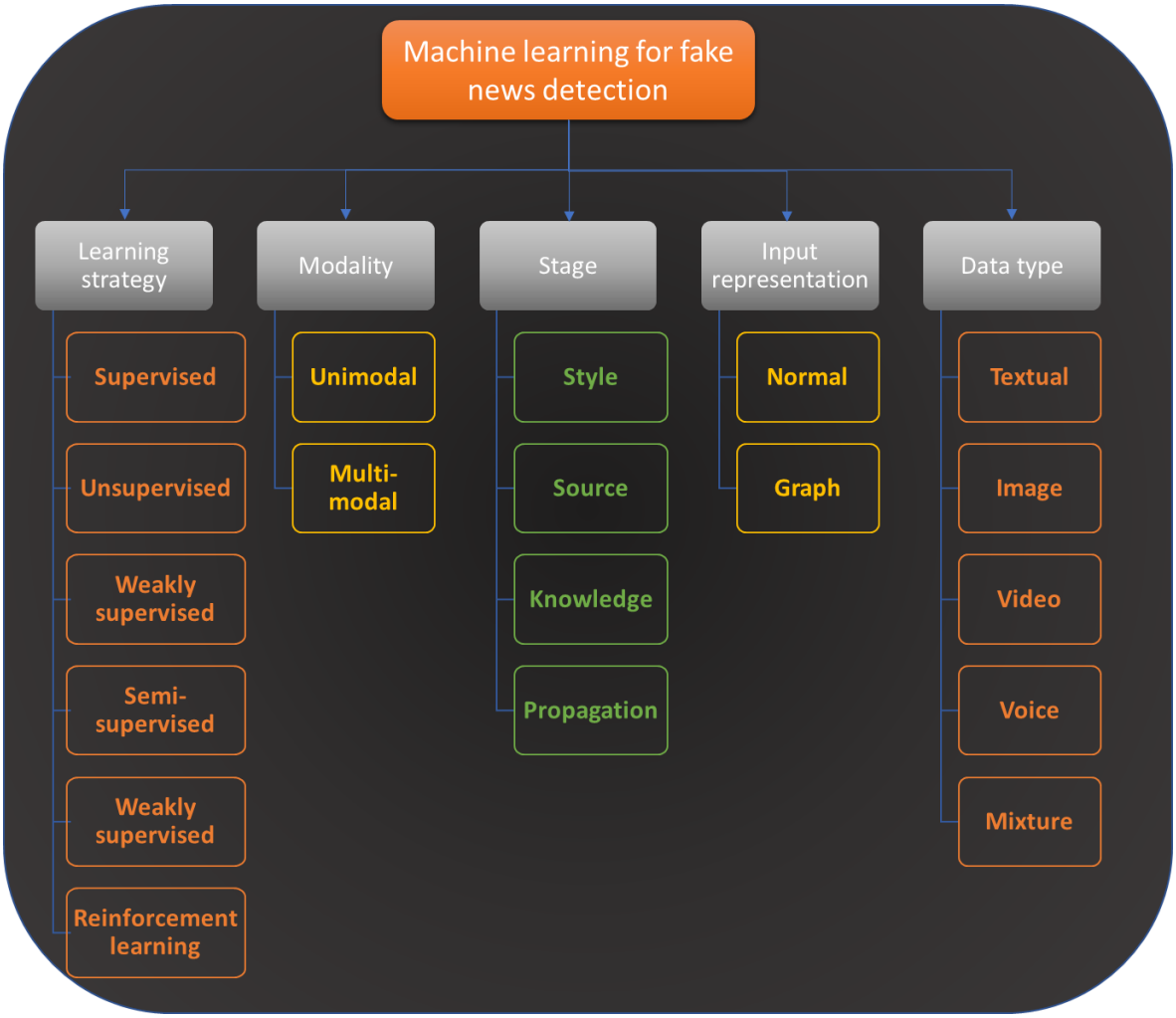

Figure 4: taxonomy of machine learning approaches for fake news detection in social networks.

6) Furthermore, another type of input representation is graph embedding. The goal of graph representation learning is to map each node to a vector while preserving the distance characteristics between nodes. The pairwise proximity between vertices in a network is referred to as first-order proximity. In weighted networks, for example, the weights of the edges are the first-order proximity between vertices. If no edge is observed between two vertices, their first-order proximity is 0. If two vertices are connected by a high-weighted edge, they should be close to each other in the embedding space. The distance between the joint probability distribution in vector space and the empirical probability distribution of the graph can be minimized to achieve this goal. The two-step relationship between two vertices is captured using second-order proximity. Although there is no direct edge between two second-order proximity vertices, their representation vectors should be close in the embedded space if they have similar neighborhood structures. Graph sampling is a technique for simplifying graphs. Even if the entire graph is known, we may want to use sampling to gain a smaller graph. If the graph is unknown, sampling is regarded as a method of exploring the graph (Negative Sampling or Edge Sampling). This forward Graph embedding method take a graph as input, which can be a homogeneous graph, a heterogeneous graph, a graph with/without auxiliary information, or a constructed graph. Graph embedding strategies that transform input graphs into a low-dimensional vector representation while conserving inherent graph characteristics like DeepWalk, Line, and Node2Vec.

3.3. Stage

We classify fake news primarily based on news content features and existing factual sources. Current approaches can be divided into two types: knowledge-based and style-based.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

3.3.1. **Knowledge-based:** knowledge-based approaches seek to use outside sources to verify suggested claims in news content. The objective of fact-checking is to allocate a truth value to a claim in a specific context [35]. Current techniques for fact-checking can be classified as expert-oriented, crowdsourcing-oriented, or computational-oriented [11].

3.3.2. **Style-based:** style-based approaches attempt to identify fake news by obtaining tricksters in news content writing style, which focuses on how it presents information to its audience, fake news is written by a number of users who are not journalists [31]. There are two major types of style-based methods: deception-oriented methodologies and objectivity-oriented methodologies [11]. In the analysis, social context models include relevant user social engagements, capturing this ancillary information from various viewpoints. Current techniques for social context modeling can be classified into two parts: Stance-based and Propagation-based.

3.3.3. **Stance-based:** Stance-based type is similar to any such style-based, but it differs in that it concentrates on how declarations are produced in a news piece. True news stories are designed in such a manner that they provide enough information about a particular topic, but it is up to the viewers to interpret the meaning of the story [42]. Stance-based articles are written to provide very few details about a particular topic while making a lot of statements (fake arguments) [31].

3.3.4. **Propagation-based:** also called structure-based features that recognize fake news by examining similarities in the spread of information via information cascades using the **SIoT** network's propagation structure, and consider the interrelationships of relating posts on **SIoT** media to forecast news truthfulness [43], [44]. Which can build a propagation process through both homogeneous and heterogeneous credibility networks [34].

3.4. Supervised Learning:

supervised Learning is classified as a machine learning research area, with the goal of developing techniques and algorithms that can use labeled training samples to make decisions over unseen examples. Supervised classification algorithms can predict the class of new objects based on a representative sample of the problem classes. Among the supervised ML methods are ANN, boosting classifiers, naive Bayes, decision trees, KNN, SVM, and RF.

3.5. Semi-supervised Learning:

Semi-supervised learning attempts to characterize some data given a set of labeled and unlabeled examples. The following are the major categories of semi-supervised methods: The SVM approach, which is an extension of the traditional SVM algorithm, and the graph-based approach, which uses identified labels as vertices and edges and unlabeled data as edges. As a result, the semi-supervised method trains a genetic algorithm, such as a fuzzy SVM or DNN, using a mix of labeled and pseudo-labeled data.

3.6. Unsupervised Learning:

Cluster analysis methods such as (1) K-means, (2) K-medoids, and (3) fuzzy C-means models are examples of unsupervised machine learning algorithms. DNN can also be used for unsupervised learning. There have been only a few unsupervised attempts to detect fake news. One of the primary reasons for developing an unsupervised method is that fake news varies across domains – for example, political fake news may differ from health-related fake news. As a result, a model that is solely based on the content of the news which only analyses the text may not generalize well across all domains.

3.7. Weakly Supervised Learning:

Weakly Supervised Learning is a form of machine learning in which noisy, limited, or imprecise sources are used to provide supervision signals for labeling large-scale training data in a supervised learning setting. This method relieves the load of acquiring hand-labeled datasets, which can be costly or impractical. Instead, inexpensive weak labels are used with the understanding that they are imperfect but can still be used to create a strong predictive model. This might consider introducing false positives (because untrustworthy sources typically propagate a combination of true and false news) as well as false negatives (fake news propagation by trusted sources, e.g., by accident).

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

4. Application On Fake News Detection

4.1. Cyberbullying detection

Bullying through social media has become a big problem with the increase the social media platforms. Cyberbullying is more spread and quickly which can cause harm to other people. The manual removal of cyberbullying content may be considered a loss of time and effort. So, it is essential to implement automatic bullying detection models. In this section, we provide the most studies that aim to detect cyberbullying in social media. Rosa et al. **[40]** compared the abilities of Fuzzy Fingerprints (FFP) with LR, NB, and SVM to identify cyberbullying using unbalanced datasets. The result shows better performance than SVM. Escalante et al. **[41]** identify the aggressive and non-aggressive profiles by using class term-occurrence information to achieve a non-sparse, discriminative model for documents. So, profiles can be classified as sub-profiles such as sexual predators, or aggressive text. The results show superior sub-profile-based than profile-based representations. Cheng et al. **[42]** introduced a comparison between SVN, KNN, RF, and LR on crowded data on the Twitter streaming API. Also, provided a PI-Bully model to detect the users' idiosyncrasies to enhance the prediction of cyberbullying actions. The results show recall with 80%. An expanding study for the same author who introduces multimodal analysis (XBully) on datasets involves image, video, user profile, time, and location information. The results show better performance than other studies **[43]**. Another contribution to the Turkish balanced Turkish dataset uses Chi-square to find a relation between feature and cyberbullying. Apply the AdaBoost algorithm to detect bullying. A study using the genetic algorithm by Kumari and Singh **[44]** extracted features using VGG and CNN algorithms. Then optimize the features using a genetic algorithm (GA). A contribution to the Arabic language which can detect cyberbullying using ML and NLP methods over-collected tweets from Arab countries [45].

4.2. Security and data privacy

Security issues in social media platforms can cause problems like fake accounts, malicious bots, network congestion, etc. According to web 2.0 which defines the application of a network, the SIoT network is the connection between users and mobile internet technology. The recent problem in social media related to trustworthiness, and confidentiality is to implement security control mechanisms to provide more security and privacy [47]. For example, Ma and Yan [48] provide security control using pervasive SIoT networking for unwanted content. Another contribution provided a DeepScan that detects malicious accounts using LSTM on-location analysis on the NN platform [49]. A study by Zhou et al. [50] introduced an approach that aims to detect the many laundering accounts by identifying spatial-temporal features. The results show a high detection rate and low false positive value. Further study by Campos et al. [51] uses many classifiers to identify malicious bots. This approach utilizes discrete wavelength transformation to find writing patterns. COLOR+ is introduced by Zhang et al. [52] to detect fake account fog computing-based depending on the interaction between users and neighbors. This approach is a rapid response method and is suitable for mobile devices. Moreover, Liu et al. introduced a crowd retweet approach that analysis the tweets to detect spam tweets and retweet the behavior of users [53]. Security and privacy are not only related to security issues in the network but also to the awareness and behavior of users. So, users must be suspicious of any links or spam messages send to them. Moreover, many users do not read security notices. Also not share any medical or political information from an unauthorized source. Most of the users that founded to be victims of theft or cyberbullying founded to have another viewpoint on social media security and privacy [54].

4.3. Traffic Control

The SIoV [17] is a trendy new phrase that has recently gained popularity. Standard car ad-hoc networking has been changed into IoV systems as a result of the new field of smart tethered automobiles, which is in accordance with current tendencies [40]. As a result, the SIoV can be thought of as an updated version of the IoV. In SIoV, the things interact socially and can communicate with one another and share information such as the state of the roadways, the climate, open parking spots, toll gates, and other traffic-related details. During the production process, the SIoV system will be put in the car. These sensors are capable of communicating with the production unit to supply it with a variety of information. During the time that the vehicle is traveling along the road, for instance, it will keep a list of social relationships. By doing so, it can communicate with the owner as well as other vehicles that are utilizing the On-Board Unit (OBU). Providing and receiving data, including navigational data, is one of the OBU's primary functions.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

Utilizing the Road Side Units (RSUs) while the car travels along the road allows for the possibility of it communicating with other vehicles on the road.

4.4. Tourism Services and Applications

One of the fascinating uses of the SIoT paradigm is in the administration of tourism services and the preservation of cultural assets [38], [39]. Let us imagine that David had no idea what he was doing and just showed up in Seoul for the first time. Finding a hotel or a place to stay is not a simple endeavor. He began using a social mobility program in order to discover the greatest possible site for his business (SMA). In order to accomplish this goal, his cell phone has already formed a new social connection using an application geared toward tourists. He could get to taxi booths and bus terminals by using that program. The social mobility app makes use of co-location and personal contacts in order to transmit a query that gathers information on the many transportation networks that are accessible. Additionally, a search is conducted in order to locate reasonable costs and expected schedules from various goods that are either directly or indirectly linked to David's cell phone. Inquiries and responses are processed hop-by-hop within the social object network and are finally saved on David's smartphone. He takes a quick look at the outputs that have already been established, such as the bus service, and bases this on his choices. The buying demand for a ticket is started via the social mobility function of the app. The mobile ticketing service is contacted by the bus terminal to receive the application. David will be able to access the e-ticket that he purchased on his smartphone in this manner [33].

4.5. Smart Healthcare

The discipline of "smart health care" [41] is quickly becoming one of the most exciting new areas in hospitals. It is possible to save a patient's life by utilizing a sensor. For the purpose of diagnosing potentially life-threatening disorders, for instance, the heartbeat sensor is linked to the cellphone and the server. Even individuals who reside more than a hundred kilometers distant can be cared for and followed up on thanks to this technology [41]. In a similar manner, a smart sensor installed on highways and roads can notify a smart ambulance when there has been an accident. As a result, the smart ambulance will be able to verify that it has all of the necessary supplies and will be at the scene as quickly as is practically possible.

5. Supervised Datasets in SIoT

An even more important factor is the dataset that was being used. According to the study, the major challenge for researchers in developing new approaches for fake news detection is the lack of available data. The reliability of the dataset is an essential aspect of developing a successful supervised learning model. In this Section, we introduce some critical evaluation metrics for evaluating the quality of fake news datasets, as well as compare the existing datasets for fake news detection. **Table 2** displays the most popularly applied datasets. Some dataset is required to verify whether an approach is performing as expected or not when trying to analyze its operation for the purpose of getting the job done. Similarly, obtaining a dataset containing both real and fake news is required in order to evaluate the accuracy of its results.

Table 2: Fake news datasets available.

No.	Dataset	YEAR	Source & Platform	Extraction Time	Language	Size	Labels	Purpose	Type of disinformation	Content-Type
1	Buzzface [46]	2018	Facebook	September 2016	English	2,263	Four-Grade	Veracity classification	Fake news articles	Text
2	FAKENEWSNET [47]	2018	Twitter	*	English	422	Two-Grade	Fake Detection	Fake news articles	Text, image

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

3	Fake.Br Corpus [48]	2018	Mainstream	January of 2016 To January of 2018	Brazilian Portuguese	7200	Two-Grade	Fake Detection	Fake news articles	Text
4	LIAR [49]	2017	POLITIFACT.COM Facebook Twitter	2007 to 2016	English	12,800	Six-Grade	Fake Detection	Fake news articles	Text
5	Emergent [50]	2016	Twitter snopes.com	*	English	300	Three-Grade	Rumor detection	Rumors	Text
6	FEVER [51]	2018	Wikipedia	June 2017	English	185,445	Three-Grade	Fact-Checking	Fake news articles	Text
7	CREDBANK [52]	2015	Twitter	October 2014 to February 2015	English	60 million	Five-Grade	Veracity Classification	Rumors	Text
8	Buzzfeed news [53]	2017	Facebook	2016 to 2017	English	2,283	Four-Grade	Fake Detection	Fake news articles	Text
9	BuzzFeed-Web is [54]	2018	Facebook	September 19 to 23, 26, and 27 September 2016	English	1627	Four-Grade	Fact-checking	Fake news articles	Text
10	PHEME [55]	2016	Twitter	August 2014	English and German	330	Three-Grade	Rumor detection	Rumor	Text
11	BS Detector	*	BS Detector	*	English	28,665	Six-Grade	veracity checking	Fake news articles	Text
12	George McIntire	2017	Mainstream	2016	English	10,558	Two-Grade	Fake Detection	Fake news articles	Text
13	FNC-1 [56]	2017	Twitter snopes.com	June 2017	English	6,337	Two-Grade	Fake Detection	Fake news articles	Text
14	Spanish FakeNewsCorpus [57]	2019	TripAdvisor	January 2018 To July 2018	Spanish	800	Two-Grade	Fake Detection	Fake news articles	Text

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

15	FakevsSatire	2018	Twitter Facebook	January 2016 to October 2017	English	486	Two-Grade	Fake Detection	Fake news Satire	Text
16	BuzzFeed Political [53]	2017	Facebook	2016 to 2017	English	120	Two-Grade	Fake Detection	Fake new Articles	Text
17	SOME-LIKE-IT-HOAX [58]	2017	Facebook	July 2016 to December 2016	English	15,500	Two-Grade	Fake Detection	Hoaxes	Text
18	Fact Checking [59]	2014	Mainstream	April 2013	English	221	Five-Grade	Fake Detection	Fake news article	Text
19	Benjamin Political News [53]	2017	Mainstream	2014 to 2015	English	225	Three-Grade	Fake Detection	Fake news articles	Text
20	Burfoot Satire News [60]	2009	English Gigaword Corpus	*	English	4,233	Two-Grade	Fake Detection	Satire	Text
21	MisInfoText [61]	2019	Snopes Facebook	2016	English	1,692	Four-Grade	Fake Detection	Fake news articles	Text
22	Gold Standard Deceptive Opinion Spam [62]	2011	TripAdvisor	*	English	800 reviews (400 truthful and 400 gold-standard deceptive reviews)	Two labels (truthful and deceptive)	Fake Detection	Fake reviews	Text
23	Twitter [63]	2016	Twitter	March 2015 to December 2015	English	992	Two-Grade	Rumor detection	Rumor	Text
24	Twitter15 [64]	2015	Twitter	2015	English	1490	Four-Grade	Rumor detection	Rumors	Text
25	Twitter16 [64]	2016	Twitter	2016	English	818	Four-Grade	Rumor detection	Rumors	Text

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

26	NELA-GT-2018 [65]	2019	Mainstream	February 2018 to November 2018	English	713,000	Two-Grade	Fake Detection	Fake news articles	Text
27	TW_Info [66]	2019	Twitter	January 2015 To April 2019	English	3,472	Two-Grade	Fake Detection	Fake news articles	Text
28	FCV-2018 [67]	2019	Twitter Facebook YouTube	April 2017 To July 2017	Multi	380 videos and 77258 tweets	Two-Grade	Fake Detection	Fake news articles	Text, Video
29	Verification Corpus [68]–[70]	2019	Twitter	2012 to 2015	English, Spanish, Dutch, French	15,629	Two-Grade	Veracity Classification	Hoaxes	Text Image Video
30	NELA-GT-2020	2021	Mainstream	January 2020 to December 2020	English	1.8 million	Two-Grade	Fake Detection	Fake news articles	Text

- **BuzzFace:** This dataset was presented by Santina and Williams [46] and was produced by combining a collection of media articles that were shared on Facebook in September 2016 by 9 different news sources. These articles were then annotated by BuzzFeed using mainstream sources such as ABC News Politics, Addicting Info, CNN Politics, Eagle Rising, Freedom Daily, Occupy Democrats, Politico, Right Wing News, and the 2016 Presidential Election. The samples consisted of approximately 2,263 Facebook news posts from 9 Facebook news pages (73.18% mostly true) with four classifications (mostly true, mostly false, a mixture of true and false, and no factual content).

- **FAKENEWSNET:** Using fact-checking websites like PolitiFact (political news) and GossipCop (popular culture), Shu et al. [47] developed two comprehensive datasets with a wide range of elements in news content, social context, and spatiotemporal data (entertainment news). There are a total of 422 news articles in this dataset, 211 of which are false and 211 of which are true (fake and real). For each news sample, it also provides essential details like the publisher, the specifics of the item itself, and the number of shares and likes it received.

- **Fake Br. Corpus:** A. Santos et al. [48] sourced authentic news from Brazil's three most prominent news outlets (G1, Folha de So Paulo, and Estado) and our false news from four sources (Di'ario do Brasil, A Folha do Brasil, The Jornal Brasil, and Top Five TV) in the same amount of time. Its reach extends to 4,180 Portuguese language samples pertaining to politics, 1,544 samples pertaining to television and celebrities, 1,276 samples pertaining to society and daily news, 112 samples pertaining to science and technology, 44 samples pertaining to the economy, and 44 samples pertaining to religion.

- **LIAR:** This information is proposed and published by Wang et al. [49] as a means of identifying internet hoaxes. Includes 12,800 brief assertions from PolitiFact.com that were manually marked. True, largely true, half true, barely true, false, and pants-faire are the possible labels for each data point. It can also be used in studies of political rumor detection, topic modelling, topic mining, and stance classification.
- **Emergent:** The Emergent dataset, developed by Ferreira and Vlachos [50], is a credible resource for a variety of NLP tasks related to verification. There are around 300 assertions in it, and 2,595 headlines from articles falling

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

into three broad categories (true, false or unverified). To the extent that it has the potential to be improved for stance categorization.

- **FEVER:** Using modified lines from Wikipedia and supporting evidence from those articles, Thorne et al. [51] introduced a publicly available dataset they named FEVER for extracting and confirming facts from textual sources. This dataset contains approximately 185,445 claims collected from Wikipedia and tagged with one of three possible categories (supported, refuted, and notenoughinfo).

- **CREDBANK:** More than 60 million tweets covering 1049 facts are included in the dataset presented by Mitra and Gilbert [52], and the authenticity of the tweets is evaluated by 30 annotators and annotated with credibility scores. They give ratings of certainty for each of five categories (Very Inaccurate, Somewhat Inaccurate, Possibly Inaccurate, Uncertain (Dubtful), and Highly Accurate).

- **Buzzfeed news:** Buzzfeed's list of fake election events on Facebook is based on an examination of the nine months leading up to the 2016 US Presidential Election, broken down into three three-month segments, during which time various methods were used to determine which stories generated the most interest among Facebook users. In addition to the URL of the news article, the number of shares, reactions, and comments is included. There are roughly 2,283 news samples spanning 4 categories on Facebook. [53].

- **BuzzFeed-Webis:** Potthast et al. [54] present a sample that includes the work of nine publishers in the week prior to the 2016 US midterm elections. There are six prolific hyperpartisan authors. A Facebook blue checkmark, signifying credibility and prominence within the network, was awarded to all contributors. BuzzFeed's professional journalists spent seven workdays checking the veracity of every post and linked news articles from the nine publishers. A total of 1,627 publications were examined, with 826 falling into the "mainstream" category, 256 leaning to the "left," and 545 leaning to the "right." The data set was divided into four categories.

- **PHEME:** Collection of tweets made during the 2014 unrest in Ferguson, Missouri, USA. Samples of 330 rumors (159 true, 68 false, and 103 unverified) were presented and analyzed in Zubiaga et al., along with the results of the annotation task. 297 of the rumors were in English, and 33 were in German. [55].

- **BS Detector:** This data was collected from the BS detector browser extension, which was developed to determine whether or not news reports were accurate. When comparing a website to a manually compiled list of domains, it examines all of the website's links for indications of potentially unreliable information sources. There are no human annotators involved in the labeling process, as the BS detector does for us.
- **McIntire:** The New York Times, the Wall Street Journal, Bloomberg, National Public Radio, The Guardian, and other publications were used to compile this information. The labels in this dataset are True and Fake, making it a binary one. As for the numbers, there are 10,558 samples across 4 different fields. It includes legitimate news from both the left and the right, and a model was constructed to determine if an item was fake or real based on tokens and sentences by compiling a dataset of fake and real news and using a Naive Bayes classifier.

- **FNC-1:** The FNC-I challenge used the emergent dataset, which included the text of news articles, their accompanying headlines, and a label indicating the stance (relevance) of the content and title. Approximately 6,337 articles are randomly sampled, with 50% being genuine and 50% being bogus, and both classifications being present (true and false).

- **Spanish Fake News Corpus:** Using a corpus of Spanish-language news articles gathered from multiple sources and annotated with two labels (genuine and fake) for automatic fake news detection, Posadas-Durán et al. [57] describe a style-based approach to this problem. Science, sports, economy, education, entertainment, politics, health, and security are all included in the wide-ranging topic covering. With two labels, the data samples roughly 800 reviews (400 honest and 400 gold-standard misleading TripAdvisor reviews).

- **FakevsSatire:** To aid the study of fake news, Golbeck et al. [71] compiled a database of news articles and parodies. Article abstracts, complete texts, links to real stories, articles debunking false news, and thematic codes

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

are all included in the publicly available dataset. This anthology contains 283 fabricated news pieces and 203 humorous works. The articles span from January 2016 to October 2017, are all written in English and are focused on American politics. The dataset comprises two labels for each article, together with the title, a link to the article, and its complete content (Fake, and, Satire).

- **Some Like It Hoax:** Tacchini et al. [58] demonstrate that on a dataset of 15,500 Posts on Facebook from 32 pages (14 conspiracy and 18 scientific), and greater than 2,300,00 likes by 909,236 consumers, Facebook posts can be classified as hoaxes or non-hoaxes (8,923 (57.6%) are hoaxes and 6,577 (42.4%) non-hoaxes) with high accuracy based on who "liked" them.

- **Fact-Checking:** Vlachos and Riedel [35] presented the activity of fact-checking and described the development of a dataset based on statements fact-checked by journalists and put online. Data samples about 221 samples, and Labels on a five-point scale: TRUE, MOSTLYTRUE, HALFTRUE, MOSTLYFALSE, and FALSE. This dataset was collected from different mainstream sources such as Channel 4 and the Truth-O-Meter from PolitiFact.

- **Benjamin Political News:** There are a total of 225 news pieces covering various aspects of politics from various news websites, with 75 articles covering each of the three types of news (actual, fake, and satire) included in the data collection. In order to compile this data, it first gathered definitions of authentic, fraudulent, and satirical new sources. The websites that spread incorrect information were culled from Zimdars' database of bogus and misleading news sources (Zimdars, 2016), all of which have had at least one of their stories debunked by a third-party fact-checking service like snopes.com. All of the authentic resources are from reputable news outlets included on Business Insider's "Most Trusted" list (Engel, 2014). When looking for satire, look for websites that make it clear right away that they are parodying something else [53]. This information was compiled from a wide variety of well-known publications, including The Wall Street Journal. Resolving the Fed Crisis, The Economist/Washington Post Inerrant Pundit Infowars References such as "The Onion," "Borowitz Report Satire Wire," "English Gigaword Corpus," etc.
- **Burfoot Satire News:** Burfoot and Baldwin introduced This dataset which is a set of 233 satirical news stories and 4000 true news stories that were used in a classification problem between these 2 kinds of media articles using lexical and semantic features. The authors assemble real-world news stories from newswire documents drawn from the English Gigaword Corpus. They handpick satire stories that are tightly linked in subject to the actual news gathered to choose the satire documents.
- **MisInfoText:** Torabi and Taboada [61] zero in on datasets that feature articles that have been manually checked for accuracy by experts in the field. Articles were collected from fact-checking sites, cleaned up, and organized, and then labeled as true, false, or similar for use in text classification activities. With 1,380 articles from the BuzzFeed dataset and 312 from the Snopes dataset, and four and five labels, respectively, there are 1,692 data points to analyze.

- **NELA-GT-2018:** Norregaard et al. [65] present a dataset consisting of 713,000 items with two labels, true and false, collected between February 2nd and November 11th, 2018. Using ground truth scores from eight different evaluation sites to wrap additional aspects of veracity like reliability, bias, transparency, adherence to journalistic standards, and consumer trust, this collection of news stories was compiled from 194 different news and media outlets, including mainstream, hyper-partisan, and conspiracy sources.
- **NELA-GT-2020:** This dataset [72] is an updated version of the NELA-GT-2019 [73] and NELA-GT-2018 [65] datasets, and it contains a significant number of English news stories annotated with source-level reliability labels. To begin, it uses a scraper that is more reliable and less likely to experience unexpected data loss. About 1.8 million media pieces, retrieved from 519 sources between January 1, 2020, and December 31, 2020, make up NELA-GT-2020. These sources come from both major and alternative news outlets, and the tweets included in the media reports offer another layer of context to the data.
- **TW_Info:** Jang et al. [66] collected information from Twitter, a highly influential social media platform. Estimated total number of tweets sampled: 3472 (1 387 fake (16453 tweets) and 20 85 real (5 6651).
- **FCV-2018:** The dataset was created using a method given by Papadopoulou et al. [67] that combines text search with near-duplicate video retrieval, and it was then manually annotated according to a set of journalistic principles. After the dataset was built, machine learning was utilized to conduct automatic verification using a predetermined

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

set of features. English, Russian, Spanish, Arabic, German, Catalan, Japanese, and Portuguese are just a few of the languages that are spoken around the world. Quantity of data: 380 movies and 77258 tweets, categorized in two ways.

- **Verification Corpus:** the goal is to investigate the obstacles of using a computational verification structure to automatically classify Twitter posts with untrustworthy media content as fake or real [68]. Which created a data corpus of Twitter posts related to major events, focusing on those that linked to images (fake or real), the veracity of which could be validated by individual online sources [69], [70].

6. Challenges, Opportunities, And Future Directions

The previous sections have detailed different aspects related to the detection of rumors and fake news, and also provide a taxonomy for categorizing the techniques of fake news detection. It is worth noting that forecasting fake news cooperatively from manifold perspectives is recommended, wherever one can syndicate their strengths. Moreover, there is an enthusiasm to debate the open challenges common between various detection approaches. According to the characteristics of fake news as well as the contemporary state of fake news research, this section focuses attention on the subsequent possible research opportunities that may simplify an in-depth comprehension of fake news and advance the explainability and efficiency of existing fake news detection solutions.

6.1. Multimodal fake data analysis

social media is not only text media, but also a combination of text, image, video, and audio. performing a multimodal analysis that can detect many types of data analysis is considered a challenging research area. Because of differences in processing techniques from one media type to another. But many research studies obtain multimodal fake news analysis on a combination of text and image such as **[2],[11-13].** There is a lack of studies that can perform analysis on a combination such as text and video, text and audio, and image and video. These combinations become very important to analyze especially during appearing of a social platform that depends on only one type of these media such as YouTube (Video), Instagram (image), and Clubhouse (audio). So, further effort is needed in the future to implement such combination models to detect fake information in any media.

6.2. Fake news detection on different SIoT platforms

Because consumers are using various social media platforms, fake news propagates all over multiple channels and platforms, difficult to know the origin of the information. It is a research opportunity to trace the source of misleading information across various online media platforms [16]. As a result, several aspects of the data must be regarded. However, the majority of available approaches focus solely on one method to identify misinformation: content analysis, propagation, style, and so on. The analysis must then take into account various attribute domains such as topics, websites, images, and URLs [22]. Also, the complex nature and dynamics of social media interaction structures aggravate recognizing and tracing of articles. As a result, complicated data structures that represent the dynamics of connections in social networking sites are required to obtain knowledge about the propagation of misinformation all across the network.

6.3. Earlier detection of fake news

Most studies consider the detection of fake news, spam messages, accounts, bots, and attacks as the main objective. However, it is highly challenging to perform the detection at an early stage prior to the proliferation of fake news so that appropriate reactions and mitigation decisions could be taken. Following fake news has come to be pervasive and reaped clients' trust, it's almost difficult to modify individuals' opinions in later times. Therefore, much research efforts have to be dedicated to deep learning-based detection models to easily attain the origins of false information **[55]**.

6.4. Support different languages in fake news analysis

Users then use social media platform posts opinions, news, and articles in different language such as English, Arabic, Chinese, etc. Most performed studies detect fake news in the English language. So, there is an essential need to obtain good performance misinformation analysis for different languages, especially during elections, revolutions, or healthcare pandemics such as Covid-19. Further research work is needed to cover this issue **[14]**.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

6.5. Mixed language use in the social media platform

Social media allow users to post their status or opinion in any form or language they need. So, in many social media texts, there exists combined language in the same article or post. Which consider a big challenge for data mining techniques because of the difference in techniques between language and another. For example, the pre-processing stage is different if it is implemented in the English language than in the Arabic language. So, more efforts are needed to implement models that can deal with this issue **[14]**.

6.6. Implementation on only a few social media platforms

In our review, we observed that the most used dataset is twitter. Although Twitter is a huge platform on which many users share their opinions and discussions. But there are lots of platforms that need to be discovered too. Especially after the Facebook problem during the 2016 elections. So further studies will obtain trustworthiness to other platforms **[14]**.

6.7. Trustworthiness issues:

Although social media platform allows people to share information and opinions, these platforms such as Facebook can give people data to other organizations. The organization may target users for advertisements or political motivations. Also, users help with more sharing and spreading of fake news. So, these issues must be addressed and discussed. Also, providing the criteria that must exist in the trustworthiness model is needed **[54]**.

6.8. Cross-domain analysis

The majority of deep learning solutions emphasize fraud detection from only a single form of input information that belongs to the same data distribution. It is noted in the literature that multi-domain data often provide richer and more insightful analytics. However, learning from such multi-domain data is an extremely challenging task for a deep-learning community. Thus, cross-domain information opens a great opportunity for developing exceptional non-changing features and delivering early and efficient detection of deceitful content.

6.9. Real-time learning

The rapidly evolving nature of web-based applications and social networks necessitates detection solutions to be able to learn from newly generated content in a real-time manner. Continual or incremental deep learning offers a great opportunity for retraining the deep learning using a newer training set thereby extending the model's knowledge with up-to-date experience.

6.10. The availability of fake news dataset

The issue of broadly accepted and available benchmark datasets lack, particularly for fake news and related online posts and reviews, should be handled. This is critical for monitoring the performance within each technique and comparing them, which existing resources cannot be adequate for obtaining a novel understanding of associated features of fake news and developing approaches that can work correctly in a realistic case. The research on data collection for this type of study could perhaps focus on creating large-scale datasets of real-world cases and identifying a straightforward and approved criterion for evaluation. The much more promising data collection attempts have been devoted in relation to online media information and debate all through breaking headlines and events [47], [52], [72].

6.11. Unlabeled Data

The massive amount of unlabeled data over the social network necessitates heavy burdens to be annotated and labeled accurately. Therefore, unlike prevailing supervised learning solutions, is highly required to develop a learning solution to learn from unlabeled, partially labeled, or noisy labeled data. unsupervised learning techniques provide a promising solution for learning from unlabeled data, while semi-supervised learning offers a great opportunity to learn from partially labeled data. Moreover, the formation of considerable global standard datasets on this ground is extremely essential as furthermost of the current research efforts are performed using

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

custom datasets. Thanks to the nonexistence of freely accessible big-scale datasets a benchmark comparison between various could not be performed.

6.12. Extracting the most significant features

For classification, the much more comprehensive solutions use both news content and social context features [22]. It has now become particularly obvious in fake news research, which uses as much detail as possible for detection. Notwithstanding the more complicated modeling techniques, existing data, and a number of features, hybrid methods that can synchronously design diverse aspects of fake news, such as the actual text, diffusion patterns, and stance towards the news, may be better suited to solve the problem and should be pursued [74]. Current research for the extraction of textual characteristics is concentrated on embedding techniques like word embedding and deep learning approaches, which have the opportunities to succeed in better depicting the features [16]. Visual features obtained from pictures can also be used to identify fake news. The use of deep learning provides a research chance in the mining of visual features for the detection of fake news [75].

6.13. Attacks on NLP for fake news detection

According to Zhou et al. [76], NLP for identifying fake news is vulnerable to ML attacks, through identifying three types of attacks: factual distortion, subject-object exchange, and cause confusion. The distortion is to overestimate or alter a few tokens. Linguistic features such as characters and time can be altered, resulting in an erroneous interpretation. The exchange between subject and object is intended to befuddle the audience as to who practices and who suffers from the observed action. The attack of cause confusion involves building non-existent causal relationships between two separate events or having to cut parts of a story, having left just the parts that the intruder tries to show to the audience.

6.14. Visualization for fake news detection

Data visualization is a strong technique for demonstrating diverse aspects and distribution patterns of social media posts due to the real-time and heterogeneous nature of social communication data [15]. Visualization is a significant element of an online fake news monitoring system, which can improve human comprehension and provide new perspectives for describing time-sensitive data. A visual analytics system can give various aspects and viewpoints of information, enable human oversight and knowing, expose temporal-based patterns and behaviors of data, and summarize key aspects in a more concise manner [77]–[79].

6.15. Identifying check-worthy content

Through new knowledge being made available on the internet at an extraordinary speed, trying to recognize check-worthy content or topics can enhance the productivity of fake news detection and intervention by emphasizing check-worthy information or topics. Newsworthy can be evaluated in various cases like determining whether the headline of the news story is clickbait [80], whether its information will spark broad social media debate [81], or whether its subject is related to national politics and corresponds to community opinions [82]. Defining check-worthy segments of news content is also a route to the explainability of fake news detection [17].

7. Interpretable Fake News Detection

Enabling the interpretability of results has been of prodigious interest in deep learning research. In the case of fake news detection, interpretability might be realized via mining social reactions such as the stance engaged within tweets and posts, and mining expert investigates presented on fact-inspection platforms, whereas both have seldom usage. The interpretability of the model's outcomes can be further improved by performing interdisciplinary research. Whilst a stream of studies has investigated theory-based or pattern-based feature engineering for fake news detection within conventional machine learning solutions, however, limited research efforts have been dedicated to investigating domain knowledge or associated theories to lead the learning of deep learning models.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

7.1. Non-traditional fake news detection

Fake news may also be media stories with outdated knowledge or false claims in certain segments of the news stories where text and images in the media stories may be partially correct or incorrect [17]. These non-traditional shapes of fake news highlight diverse components of detection and encourage the development of more systematic and complete detection strategies. To identify disinformation of outdated knowledge, for instance, a dynamic KG is recommended; which can be upgraded on a regular and automatic basis to reflect the variations in a rapid world [75] and to identify false information that would only be partially right, expanding fake news detection to a multi-label classification or regression issue can be preferable to specifying it as a binary classification issue [17].

7.2. Fake News Intervention

Fake news research efforts have underlined the significance of innovative business models approved by social networks to tackle fake news intervention, which recommends changing the prominence from expanding client commitment to that improving the value of information. Besides the design of new strategies and procedures, effectively stopping and alleviating the propagation of fake news also necessitates technological changes and advancements. Technologically, the design of the intervention strategy could be dependent on either users or network structure. From a network structure perspective, one aims to stop fake news from proliferation by stopping its transmission routes, depending on the analysis of the network structure of its proliferation and forecasting the way the fake news follows to spread widely. According to the user viewpoint, intervention in fake news depends on certain responsibilities the users perform in fake news propagation. For instance, in the case of leading user, the blocking of these dominant broadcasters result in more useful intervention contrasted to those having an insignificant social impact on others. In addition, the correctors on social networks have active responsibility in alleviating the propagation of fake news by assigning links to their tweets or shared content that demystify the fake news. Moreover, the intervention strategy for normal and malicious users must be dissimilar in such a way that the malicious users are penalized for fake news, whilst the normal ones have to be empowered to advance their capability to differentiate fake news. For example, personal endorsement of true news or news having disproving evidence may be supportive to normal users. This suggestion ought to not only accommodate the subjects that the clients would like to read but include those subjects that they are highly naive to because of their political preferences or foregoing experience.

8. Conclusion

As part of this research, we present the first systematic examination of methods for identifying fake news across many social media sites. There is a distinction between misleading content information that is unimodal and multimodal, and we outline what that is. As a result, we provided an overview of the vast majority of research that has used either unimodal or multimodal implementations, categorizing them as either ML or DL and including the outcomes of each. In this section, we examine the variations between models. Major and important uses of fake news detection are also discussed, including the identification of bots, cyberbullying, fraudulent accounts, and privacy and security concerns in social media. We conclude by highlighting a novel perspective and an intricate research topic.

References

[1] F. Amin, A. Majeed, A. Mateen, R. Abbasi and S. O. Hwang, "A Systematic Survey on the Recent Advancements in the Social Internet of Things," in IEEE Access, vol. 10, pp. 63867-63884, 2022, doi: 10.1109/ACCESS.2022.3183261.

[2] A. Arooj, M. S. Farooq, T. Umer, G. Rasool and B. Wang, "Cyber Physical and Social Networks in IoV (CPSN-IoV): A Multimodal Architecture in Edge-Based Networks for Optimal Route Selection Using 5G Technologies," in IEEE Access, vol. 8, pp. 33609-33630, 2020, doi: 10.1109/ACCESS.2020.2973461.

[3] P. He and T. Tang, "Community-Oriented Multimedia Content Maximization Mechanism in Social Internet of Things," in IEEE Access, vol. 8, pp. 22826-22833, 2020, doi: 10.1109/ACCESS.2020.2970453.

[4] Q. Li, Y. Song, B. Du, Y. Shen and Y. Tian, "Deep Neural Network-Embedded Internet of Social Computing Things for Sustainability Prediction," in IEEE Access, vol. 8, pp. 60737-60746, 2020, doi: 10.1109/ACCESS.2020.2982986.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

[5] B. Wang, Y. Sun, T. Q. Duong, L. D. Nguyen and L. Hanzo, "Risk-Aware Identification of Highly Suspected COVID-19 Cases in Social IoT: A Joint Graph Theory and Reinforcement Learning Approach," in IEEE Access, vol. 8, pp. 115655-115661, 2020, doi: 10.1109/ACCESS.2020.3003750.
[6] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.
[7] X. Fan, Y. Li, J. Sun, Y. Zhao and G. Wang, "Effective and Efficient Steiner Maximum Path-Connected Subgraph Search in Large Social Internet of Things," in IEEE Access, vol. 9, pp. 72820-72834, 2021, doi: 10.1109/ACCESS.2021.3079468.
[8] M. J. Aslam, S. Din, J. J. P. C. Rodrigues, A. Ahmad and G. S. Choi, "Defining Service-Oriented Trust Assessment for Social Internet of Things," in IEEE Access, vol. 8, pp. 206459-206473, 2020, doi: 10.1109/ACCESS.2020.3037372.
[9] K. C. Chung and S. W. -J. Liang, "An Empirical Study of Social Network Activities via Social Internet of Things (SIoT)," in IEEE Access, vol. 8, pp. 48652-48659, 2020, doi: 10.1109/ACCESS.2020.2978151.
[10] W. Yang, H. Huang, X. Jing, Z. Li and C. Zhu, "Social Interaction Assisted Resource Sharing Scheme for Device-to-Device Communication Towards Green Internet of Things," in IEEE Access, vol. 8, pp. 71652-71661, 2020, doi: 10.1109/ACCESS.2020.2986785.
[11] G. A. Stelea, V. Popescu, F. Sandu, L. Jalal, M. Farina and M. Murroni, "From Things to Services: A Social IoT Approach for Tourist Service Management," in IEEE Access, vol. 8, pp. 153578-153588, 2020, doi: 10.1109/ACCESS.2020.3018331.
[12] Y. Huo, J. Fan, Y. Wen and R. Li, "A cross-layer cooperative jamming scheme for social internet of things," in Tsinghua Science and Technology, vol. 26, no. 4, pp. 523-535, Aug. 2021, doi: 10.26599/TST.2020.9010020.
[13] F. Alzamzami and A. E. Saddik, "Monitoring Cyber SentiHate Social Behavior During COVID-19 Pandemic in North America," in IEEE Access, vol. 9, pp. 91184-91208, 2021, doi: 10.1109/ACCESS.2021.3088410.
[14] T. -H. Hsu and Y. -M. Tung, "A Social-Aware P2P Video Transmission Strategy for Multimedia IoT Devices," in IEEE Access, vol. 8, pp. 95574-95584, 2020, doi: 10.1109/ACCESS.2020.2995274.
[15] M. F. Mridha, A. J. Keya, M. A. Hamid, M. M. Monowar and M. S. Rahman, "A Comprehensive Review on Fake News Detection With Deep Learning," in IEEE Access, vol. 9, pp. 156151-156170, 2021, doi: 10.1109/ACCESS.2021.3129329.
[16] D. Rohera et al., "A Taxonomy of Fake News Classification Techniques: Survey and Implementation Aspects," in IEEE Access, vol. 10, pp. 30367-30394, 2022, doi: 10.1109/ACCESS.2022.3159651.
[17] S. Jamialahmadi, I. Sahebi, M. M. Sabermahani, S. P. Shariatpanahi, A. Dadlani and B. Maham, "Rumor Stance Classification in Online Social Networks: The State-of-the-Art, Prospects, and Future Challenges," in IEEE Access, vol. 10, pp. 113131-113148, 2022, doi: 10.1109/ACCESS.2022.3216835.
[18] A. Gupta et al., "Combating Fake News: Stakeholder Interventions and Potential Solutions," in IEEE Access, vol. 10, pp. 78268-78289, 2022, doi: 10.1109/ACCESS.2022.3193670.
[19] W. Shahid, Y. Li, D. Staples, G. Amin, S. Hakak and A. Ghorbani, "Are You a Cyborg, Bot or Human?—A Survey on Detecting Fake News Spreaders," in IEEE Access, vol. 10, pp. 27069-27083, 2022, doi: 10.1109/ACCESS.2022.3157724.
[20] S. M. Ghafari et al., "A Survey on Trust Prediction in Online Social Networks," in IEEE Access, vol. 8, pp. 144292-144309, 2020, doi: 10.1109/ACCESS.2020.3009445.
[21] K. Shu, A. Sliva, S. Wang, J. Tang and H. Liu, "Fake news detection on social media: A data mining perspective", *ACM SIGKDD Explorations Newslett.*, vol. 19, no. 1, pp. 22-36, 2017.
[22] R. Oshikawa, J. Qian, and W. Y. Wang, "A survey on natural language processing for fake news detection," 2020.
[23] Manzoor, S.I. and Singla, J., 2019, April. Fake news detection using machine learning approaches: A systematic review. In *2019 3rd international conference on trends in electronics and informatics (ICOEI)* (pp. 230-234). IEEE.
[24] Zhou, X. and Zafarani, R., 2020. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys (CSUR)*, *53*(5), pp.1-40.
[25] Alonso, M.A., Vilares, D., Gómez-Rodríguez, C. and Vilares, J., 2021. Sentiment analysis for fake news detection. *Electronics*, *10*(11), p.1348.
[26] Zhang, X. and Ghorbani, A.A., 2020. An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, *57*(2), p.102025.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

[27] Freire, P.M.S., da Silva, F.R.M. and Goldschmidt, R.R., 2021. Fake news detection based on explicit and implicit signals of a hybrid crowd: An approach inspired in meta-learning. *Expert Systems with Applications*, *183*, p.115414.
[28] Mishra, S., Shukla, P. and Agarwal, R., 2022. Analyzing machine learning enabled fake news detection techniques for diversified datasets. *Wireless Communications and Mobile Computing*, *2022*.
[29] Hu, L., Wei, S., Zhao, Z. and Wu, B., 2022. Deep learning for fake news detection: A comprehensive survey. *AI Open*.
[30] Zervopoulos, A., Alvanou, A.G., Bezas, K., Papamichail, A., Maragoudakis, M. and Kermanidis, K., 2022. Deep learning for fake news detection on Twitter regarding the 2019 Hong Kong protests. *Neural Computing and Applications*, *34*(2), pp.969-982.
[31] Mishra, S., Shukla, P. and Agarwal, R., 2022. Analyzing machine learning enabled fake news detection techniques for diversified datasets. *Wireless Communications and Mobile Computing*, *2022*.
[32] Amer, E., Kwak, K.S. and El-Sappagh, S., 2022. Context-Based Fake News Detection Model Relying on Deep Learning Models. *Electronics*, *11*(8), p.1255.
[33] Ahmad, T., Faisal, M.S., Rizwan, A., Alkanhel, R., Khan, P.W. and Muthanna, A., 2022. Efficient Fake News Detection Mechanism Using Enhanced Deep Learning Model. *Applied Sciences*, *12*(3), p.1743.
[34] Palani, B., Elango, S. and Viswanathan K, V., 2022. CB-Fake: A multimodal deep learning framework for automatic fake news detection using capsule neural network and BERT. Multimedia Tools and Applications, 81(4), pp.5587-5620.
[35] Hanshal, O.A., Ucan, O.N. and Sanjalawe, Y.K., 2022. Hybrid deep learning model for automatic fake news detection. *Applied Nanoscience*, pp.1-11.
[36] Jain, V., Kaliyar, R.K., Goswami, A., Narang, P. and Sharma, Y., 2022. AENeT: an attention-enabled neural architecture for fake news detection using contextual features. *Neural Computing and Applications*, *34*(1), pp.771-782.
[37] Cvitanović, I. and Babac, M.B., 2022. Deep Learning with Self-Attention Mechanism for Fake News Detection. In *Combating Fake News with Computational Intelligence Techniques* (pp. 205-229). Springer, Cham.
[38] Galli, A., Masciari, E., Moscato, V. and Sperlí, G., 2022. A comprehensive Benchmark for fake news detection. *Journal of Intelligent Information Systems*, pp.1-25.
[39] Buzea, M.C., Trausan-Matu, S. and Rebedea, T., 2022. Automatic fake news detection for romanian online news. *Information*, *13*(3), p.151.
[40] N. Ruchansky, S. Seo, and Y. Liu, "Csi: A hybrid deep model for fake news detection," in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, Nov. 2017, pp. 797–806.
[41] K. Shu, D. Mahudeswaran, S. Wang, and H. Liu, "Hierarchical propagation networks for fake news detection: Investigation and exploitation," in *Proceedings of the International AAAI Conference on Web and Social Media*, Mar. 2020, vol. 14, pp. 626–637.
[42] S. M. Mohammad, P. Sobhani, and S. Kiritchenko, "Stance and sentiment in tweets," *ACM Transactions on Internet Technology (TOIT)*, vol. 17, no. 3, pp. 1–23, Jun. 2017.
[43] K. Wu, S. Yang, and K. Q. Zhu, "False rumors detection on sina weibo by propagation structures," in *2015 IEEE 31st international conference on data engineering*, May 2015, pp. 651–662.
[44] J. Ma, W. Gao, and K.-F. Wong, "Rumor detection on twitter with tree-structured recursive neural networks," May 2018.
[45] Y. Wang *et al.*, "Eann: Event adversarial neural networks for multi-modal fake news detection," in *Proceedings of the 24th acm sigkdd international conference on knowledge discovery & data mining*, Jul. 2018, pp. 849–857.
[46] G. C. Santia and J. R. Williams, "Buzzface: A news veracity dataset with facebook user commentary and egos," Jun. 2018.
[47] K. Shu, D. Mahudeswaran, S. Wang, D. Lee, and H. Liu, "Fakenewsnet: A data repository with news content, social context, and spatiotemporal information for studying fake news on social media," *Big data*, vol. 8, no. 3, pp. 171–188, Jun. 2020.
[48] R. L. S. Santos, R. A. Monteiro, and T. A. S. Pardo, "The Fake. Br corpus-a corpus of fake news for Brazilian Portuguese," in *Latin American and Iberian Languages Open Corpora Forum (OpenCor)*, 2018, pp. 1–2.
[49] W. Y. Wang, "' liar, liar pants on fire': A new benchmark dataset for fake news detection," *arXiv preprint arXiv:1705.00648*, Jun. 2017.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

[50] W. Ferreira and A. Vlachos, "Emergent: a novel data-set for stance classification," in *Proceedings of the 2016 conference of the North American chapter of the association for computational linguistics: Human language technologies*, Mar. 2016, pp. 1163–1168.
[51] J. Thorne, A. Vlachos, C. Christodoulopoulos, and A. Mittal, "Fever: a large-scale dataset for fact extraction and verification," *arXiv preprint arXiv:1803.05355*, Apr. 2018.
[52] T. Mitra and E. Gilbert, "Credbank: A large-scale social media corpus with associated credibility annotations," 2015.
[53] B. Horne and S. Adali, "This just in: Fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news," in *Proceedings of the International AAAI Conference on Web and Social Media*, Mar. 2017, vol. 11, no. 1.
[54] M. Potthast, J. Kiesel, K. Reinartz, J. Bevendorff, and B. Stein, "A stylometric inquiry into hyperpartisan and fake news," *arXiv preprint arXiv:1702.05638*, Feb. 2017.
[55] A. Zubiaga, M. Liakata, R. Procter, K. Bontcheva, and P. Tolmie, "Towards detecting rumours in social media," Apr. 2015.
[56] B. Riedel, I. Augenstein, G. P. Spithourakis, and S. Riedel, "A simple but tough-to-beat baseline for the Fake News Challenge stance detection task," *arXiv preprint arXiv:1707.03264*, Jul. 2017.
[57] J.-P. Posadas-Durán, H. Gómez-Adorno, G. Sidorov, and J. J. M. Escobar, "Detection of fake news in a new corpus for the Spanish language," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 4869–4876, May 2019.
[58] E. Tacchini, G. Ballarin, M. L. della Vedova, S. Moret, and L. de Alfaro, "Some like it hoax: Automated fake news detection in social networks," *arXiv preprint arXiv:1704.07506*, Nov. 2017.
[59] A. Vlachos and S. Riedel, "Fact checking: Task definition and dataset construction," in *Proceedings of the ACL 2014 workshop on language technologies and computational social science*, Jun. 2014, pp. 18–22.
[60] C. Burfoot and T. Baldwin, "Automatic satire detection: Are you having a laugh?," in *Proceedings of the ACL-IJCNLP 2009 conference short papers*, Jan. 2009, pp. 161–164.
[61] F. Torabi Asr and M. Taboada, "Big data and quality data for fake news and misinformation detection," *Big Data & Society*, vol. 6, no. 1, p. 2053951719843310, May 2019.
[62] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, "Finding deceptive opinion spam by any stretch of the imagination," *arXiv preprint arXiv:1107.4557*, Jun. 2011.
[63] J. Ma *et al.*, "Detecting rumors from microblogs with recurrent neural networks," Jul. 2016.
[64] J. Ma, W. Gao, and K.-F. Wong, "Detect rumors in microblog posts using propagation structure via kernel learning," Jul. 2017.
[65] J. Nørregaard, B. D. Horne, and S. Adal, "Nela-gt-2018: A large multi-labelled news dataset for the study of misinformation in news articles," in *Proceedings of the international AAAI conference on web and social media*, Apr. 2019, vol. 13, pp. 630–638.
[66] Y. Jang, C.-H. Park, and Y.-S. Seo, "Fake news analysis modeling using quote retweet," *Electronics*, vol. 8, no. 12, p. 1377, Nov. 2019.
[67] O. Papadopoulou, M. Zampoglou, S. Papadopoulos, and I. Kompatsiaris, "A corpus of debunked and verified user-generated videos," *Online information review*, Nov. 2019.
[68] C. Boididou, S. Papadopoulos, Y. Kompatsiaris, S. Schifferes, and N. Newman, "Challenges of computational verification in social multimedia," in *Proceedings of the 23rd International Conference on World Wide Web*, Apr. 2014, pp. 743–748.
[69] C. Boididou, S. Papadopoulos, M. Zampoglou, L. Apostolidis, O. Papadopoulou, and Y. Kompatsiaris, "Detection and visualization of misleading content on Twitter," *International Journal of Multimedia Information Retrieval*, vol. 7, no. 1, pp. 71–86, Dec. 2018.
[70] C. Boididou *et al.*, "Verifying information with multimedia content on twitter," *Multimedia tools and applications*, vol. 77, no. 12, pp. 15545–15571, Jun. 2018.
[71] J. Golbeck *et al.*, "Fake news vs satire: A dataset and analysis," in *Proceedings of the 10th ACM Conference on Web Science*, May 2018, pp. 17–21.
[72] M. Gruppi, B. D. Horne, and S. Adal, "NELA-GT-2020: A Large Multi-Labelled News Dataset for The Study of Misinformation in News Articles," *arXiv preprint arXiv:2102.04567*, Feb. 2021.
[73] M. Gruppi, B. Horne, and S. Adalı, "NELA-GT-2019: A Large Multi-Labelled News Dataset for The Study of Misinformation in News Articles." Mar. 2020.
[74] A. Bondielli and F. Marcelloni, "A survey on fake news and rumour detection techniques," *Information Sciences*, vol. 497, pp. 38–55, May 2019.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022

[75] K. Sharma, F. Qian, H. Jiang, N. Ruchansky, M. Zhang, and Y. Liu, "Combating fake news: A survey on identification and mitigation techniques," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 3, pp. 1–42, Jan. 2019.
[76] Z. Zhou, H. Guan, M. M. Bhat, and J. Hsu, "Fake news detection via NLP is vulnerable to adversarial attacks," *arXiv preprint arXiv:1901.09657*, Jan. 2019.
[77] P. Cogan, M. Andrews, M. Bradonjic, W. S. Kennedy, A. Sala, and G. Tucci, "Reconstruction and analysis of twitter conversation graphs," in *Proceedings of the First ACM International Workshop on Hot Topics on Interdisciplinary Social Networks Research*, Aug. 2012, pp. 25–31.
[78] R. Nishi *et al.*, "Reply trees in twitter: data analysis and branching process models," *Social Network Analysis and Mining*, vol. 6, no. 1, p. 26, May 2016.
[79] V. Gómez, H. J. Kappen, N. Litvak, and A. Kaltenbrunner, "A likelihood-based framework for the analysis of discussion threads," *World Wide Web*, vol. 16, no. 5–6, pp. 645–675, Mar. 2013.
[80] X. Zhou, A. Jain, V. v Phoha, and R. Zafarani, "Fake news early detection: A theory-driven model," *Digital Threats: Research and Practice*, vol. 1, no. 2, pp. 1–25, Jan. 2020.
[81] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146–1151, Mar. 2018.
[82] N. Hassan, F. Arslan, C. Li, and M. Tremayne, "Toward automated fact-checking: Detecting check-worthy factual claims by claimbuster," in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Aug. 2017, pp. 1803–1812.

Doi: https://doi.org/10.54216/FPA.100103
Received: June 12, 2022 Accepted: October 26, 2022