



**NEAR EAST UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
DEPARTMENT OF COMPUTER INFORMATION
SYSTEMS**

**FAKE NEWS DETECTION WITH ARTIFICIAL
INTELLIGENCE TOOLS IN ONLINE SOCIAL NETWORKS
BASED ON CLOUD COMPUTING**

Ph.D. THESIS

Murat GÖKSU

**Nicosia
Nov, 2024**

MURAT GÖKSU

**FAKE NEWS DETECTION WITH ARTIFICIAL INTELLIGENCE TOOLS
IN ONLINE SOCIAL NETWORKS BASED ON CLOUD COMPUTING**

2024

NEAR EAST UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

FAKE NEWS DETECTION WITH ARTIFICIAL INTELLIGENCE
TOOLS IN ONLINE SOCIAL NETWORKS BASED ON CLOUD
COMPUTING

Ph.D. THESIS

Murat GÖKSU

Supervisor






Prof.Dr. Nadire ÇAVUŞ

Nicosia

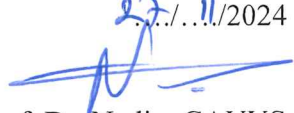
Nov, 2024

Approval

We certify that we have read the thesis submitted by Murat GÖKSU titled “**Fake News Detection with Artificial Intelligence Tools in Online Social Networks Based on Cloud Computing**” and that in our combined opinion it is fully adequate, in scope and in quality, as a thesis for the degree Doctor of Philosophy of Computer Information Systems.

Examining Committee	Name-Surname	Signature
Head of the Committee:	Prof. Dr. Ahmet ADALIER	
Committee Member :	Prof. Dr. Murat AKKAYA	
Committee Member :	Assoc. Prof. Dr. Boran ŞEKEROĞLU	
Committee Member :	Assoc. Prof. Dr. Nuriye SANCAR	
Supervisor :	Prof. Dr. Nadire ÇAVUŞ	

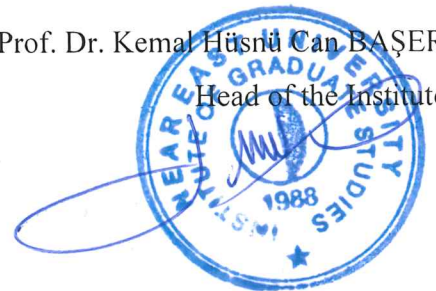
Approved by the Head of the Department

27/.../2024

Prof. Dr. Nadire ÇAVUŞ
Head of Department

Approved by the Institute of Graduate Studies

.../.../2025

Prof. Dr. Kemal Hüsnü Can BAŞER
Head of the Institute



To my dear wife, sons and mother

I wish my father was alive to see this success...

Declaration

I hereby declare that all information, documents, analysis and results in this thesis have been collected and presented according to the academic rules and ethical guidelines of Institute of Graduate Studies, Near East University. I also declare that as required by these rules and conduct, I have fully cited and referenced information and data that are not original to this study.

Murat GÖKSU

15/10/2024

Acknowledgments

I would like to thank my thesis advisor, Prof. Dr. Nadire ÇAVUŞ, who inspired me and contributed a lot with her vast knowledge and experience, and whose support I always felt during my doctoral education program and thesis process.

I would like to thank Prof. Dr. Murat AKKAYA and Assoc. Prof. Dr. Boran ŞEKEROĞLU for their invaluable contributions to the Thesis Monitoring Committees with their comments and suggestions.

I would like to thank the esteemed members of the Thesis Defense Committee, Prof. Dr. Ahmet ADALIER and Assoc. Prof. Dr. Nuriye SANCAR, for their valuable contributions, comments and suggestions.

I would like to thank my dear brother Ph.D.(c) Bora OKTEKIN, whose knowledge and experience I have greatly benefited from throughout my thesis work and who has been a lifelong friend of mine.

I would like to thank my family for their unwavering support throughout my doctoral education and my whole life, who have had the greatest share in my success and in reaching these days.

Murat GÖKSU

Abstract

Real-Time Fake News Detection in Online Social Networks: FANDC Cloud-Based System

GÖKSU, Murat

PhD, Department of Computer Information Systems

Prof.Dr. Nadire ÇAVUŞ

Nov, 2024, 136 pages

Online social networks (OSNs) have become a common way for people to communicate with each other and exchange ideas thanks to their rapid information-sharing features. The use of OSN is increasing day by day and accordingly, the number of users is increasing rapidly. However, fake news spread in OSNs can cause problems in social life, economic problems, and even political problems. Malicious people want to mislead and exploit OSN users by effectively using this loophole in OSNs. OSN users are greatly harmed by this situation and experience the negative effects of fake news in their daily lives. For this reason, it is considered that a fake news detection system is needed to facilitate the detection of fake news spreading in OSNs. However, there are no online and real-time fake news detection systems in the literature. This study aims to fill this literature gap and address the fake news detection problem with a cloud computing-based system called FANDC. In this context, the fake news detection in question was evaluated in seven different categories. The main purpose of this study is to detect fake news on Twitter, one of the OSNs, and divide it into seven subcategories. The system was developed based on the CRISP-DM methodology. To protect against possible cyber threats, the system running on MS-Azure cloud computing used the corpus created with approximately 99 million tweets downloaded from the GitHub repository during the COVID-19 period and the BERT algorithm. In terms of training accuracy, the system was trained in two periods with 100% accuracy during the modeling phase. Experimental results of the FANDC system achieved real-time detection and classification of fake news into seven subcategories with 99% accuracy. When previous

studies in the literature were examined, it was determined that the success rate in question was around 90%. However, other studies focused only on a single feature of fake news and relied on the success of the created system rather than real-time detection online. The FANDC system, on the other hand, can detect fake news and determine which category it is in with a 99% success rate. It is evaluated that this developed system will greatly help social network users detect fake news in real-time, as well as identify them in seven subcategories.

Keywords: Fake news detection, online social networks, artificial intelligence, cloud computing, text mining

Özet

Çevrimiçi Sosyal Ağlarda Gerçek Zamanlı Sahte Haber Tespiti: FANDC Bulut Tabanlı Sistem

GÖKSU, Murat

Doktora, Bilgisayar Enformatik Sistemleri Anabilim Dalı

Prof.Dr. Nadire ÇAVUŞ

Kasım 2024, 136 sayfa

Çevrim içi sosyal ağlar (ÇSA), hızlı bilgi paylaşım özellikleri sayesinde insanların birbirleriyle iletişim kurmasının ve fikir alışverişinde bulunmasının yaygın bir yolu haline gelmiştir. ÇSA kullanımı gün geçtikçe artmakta ve buna bağlı olarak kullanıcı sayısı da hızla yükselmektedir. Bununla birlikte ÇSA'lar da yayılan sahte haberler, sosyal hayatta yaşanan problemlerden, ekonomik problemlere ve hatta politik problemlere dahi neden olabilmektedir. Kötü niyetli kişiler ÇSA'larda ki bu boşluğu etkili bir şekilde kullanarak, ÇSA kullanıcılarını yanıltmak ve istismar etmek istemektedirler. ÇSA kullanıcıları bu durumdan oldukça zarar görmekte ve sahte haberlerin olumsuz etkilerini günlük hayatlarında yaşamaktadırlar. Bu nedenle ÇSA'larda yayılım gösteren sahte haberlerin tespitini kolaylaştırmak için bir sahte haber tespit sistemine ihtiyaç olduğu değerlendirilmektedir. Ancak literatürde çevrimiçi ve gerçek zamanlı sahte haber tespit sistemleri bulunmamaktadır. Bu çalışma, bu literatür boşluğunu doldurmayı ve sahte haber tespit problemini FANDC adı verilen bulut bilişim tabanlı bir sistemle ele almayı amaçlamaktadır. Bu kapsamda söz konusu sahte haber tespiti yedi farklı kategoride değerlendirilmiştir. Bu çalışmanın temel amacı ÇSA'lardan biri olan Twitter'da sahte haberlerin tespit edilerek yedi alt kategoriye ayrılması oluşturmaktadır. Sistem, CRISP-DM metodolojisi esas alınarak geliştirilmiştir. Olası siber tehditlerden korunmak için MS-Azure bulut bilişim üzerinde çalışan sistemde, COVID-19 döneminde GitHub deposundan indirilen yaklaşık 99 milyon tweetle oluşturulan külliyat ve BERT algoritması kullanılmıştır. Sistem eğitim doğruluğu açısından modelleme aşamasında 100% doğrulukla iki periyotta eğitilmiştir. FANDC sisteminin deneysel sonuçları, sahte haberlerin gerçek zamanlı tespitini ve yedi alt kategoriye ayrılmasını 99% doğrulukla gerçekleştirmiştir.

Literatürde daha önceki çalışmalar incelendiğinde söz konusu başarı oranının 90% civarında olduğu tespit edilmiştir. Bununla birlikte diğer çalışmalar sadece sahte haberin bir tek özelliğine odaklanmış ve çevrimiçi gerçek zamanlı tespit etmekten öte oluşturulan sistemin başarısı esas alınmıştır. FANDC sistemi ise sahte haberi tespit ederek hangi kategoride olduğunu 99% başarı oranıyla tespit edebilmektedir. Geliştirilen bu sistemle, sosyal ağ kullanıcılarının sahte haberleri gerçek zamanlı olarak tespit etmelerinin yanı sıra onları yedi alt kategoride tespit edebilmelerine büyük ölçüde yardımcı olacağı değerlendirilmektedir.

Anahtar kelimeler: Sahte haber tespiti, çevrim içi sosyal ağlar, yapay zekâ, bulut bilişim, metin madenciliği,

Table of Contents

APPROVAL	i
DECLARATION.....	iii
ACKNOWLEDGMENTS	iv
ABSTRACT.....	v
ÖZET	vii
TABLE OF CONTENTS	ix
LIST OF TABLES.....	xii
LIST OF FIGURES.....	xiii
LIST OF ABBREVIATIONS.....	xiv

CHAPTER I

INTRODUCTION	1
Background.....	1
Problem Statement.....	4
Aim and Objectives	5
Contribution of the Study to the Field	6
Significance of the Study.....	7
Limitations of the Study	7
Overview of the Thesis.....	8

CHAPTER II

LITERATURE REVIEW.....	9
Theoretical Framework.....	9
Online Social Networks and Fake News	9
Fake News Concept	13
How To Spread of Fake News on Online Social Networks.....	19
Malicious Accounts in OSNs	23
Echo Chamber Effect	25
Fake News Detection Methods	26
Content-based methods	28
Language/Style-Based Methods.....	29
Stance-Based Methods	29

Propagation/Network-Based Methods.....	29
Source Based Methods	30
Hybrid Methods.....	30
Fake News Consequences in Online Social Networks	30
Health Impact	31
Financial Impact	31
People Impact	31
Related Research	32
Systematic Literature Review	32
The Gap in the Literature	43

CHAPTER III

METHODOLOGY	45
CRISP-DM Methodologies	45
Business Understanding.....	48
Data Understanding	49
Data Preparation.....	49
Modelling.....	50
Evaluation	52
Deployment.....	53
Data Collection	53
Algorithm Selection.....	54
Developed Fake News Detection System.....	55

CHAPTER IV

RESULTS	60
Results	60

CHAPTER V

DISCUSSION	68
Discussion.....	68

CHAPTER VI

CONCLUSION AND RECOMMENDATIONS	74
Conclusion	74
Recommendations	75
Recommendations For Researchers	75
Recommendations For OSN User	76
Recommendations For Policy Maker	76
REFERENCES	78
APPENDICES	99
APPENDIX I: Ethics Approval	99
APPENDIX II: Similarity Report	100
APPENDIX III: Curriculum Vitae	115

List of Tables

Table 2. 1 Inclusion criteria	33
Table 2. 2 Exclusion criteria	34
Table 3. 1 The success rate of the post-training classification stage of the FANDC System .	58
Table 5. 1 Comparison of the success rates of FANDC and other studies	73

List of Figures

Figure 2.1: Overview of the adoption and use of the connected device and services as of January 2022	11
Figure 2.2: Change in the use of connected devices and services over time of January 2022	12
Figure 2.3: Buzzfeed Analysis	16
Figure 2.4: Bat-eating Chinese Twitter screenshot	18
Figure 2.5: Number of internet and social media users worldwide as of January 2023	20
Figure 2.6: Number of social network users in selected countries in 2022 and 2027.....	21
Figure 2.7: Most popular social networks worldwide as of January 2023.....	22
Figure 2.8: Daily Time Spent Using social media as of January 2023	23
Figure 2.9: Systematic Literature Review Process.....	35
Figure 2.10: Data Analysis Process.....	36
Figure 2.11: Research Approach for Data Analysis	36
Figure 2.12: Mini Literature Revive Process	40
Figure 3.1: CRISP-DM Methodology Diagram.....	47
Figure 3.2: A Sample of BERT for MLM	55
Figure 3.3: The general design of the FANDC model	57
Figure 3.4: FANDC System Post-training Accuracy	57
Figure 3.5: FANDC System Confusion Matrix of Post-training.....	58
Figure 3.6: FANDC System K=5 Fold Cross-Validation Accuracy.....	59
Figure 4.1: FANDC System Example of Click Bait Query Result.....	61
Figure 4.2: FANDC System Example of Disinformation Query Result.....	62
Figure 4.3: FANDC System Example of Hoax Query Result.....	63
Figure 4.4: FANDC System Example of Junk News Query Result.....	64
Figure 4.5: FANDC System Example of Misinformation Query Result	65
Figure 4.6: FANDC System Example of Propaganda Query Result.....	66
Figure 4.7: FANDC System Example of Satirical Query Result	67

List of Abbreviations

5G:	Fifth Generation Communication Systems
AI:	Artificial Intelligence
ANN:	Artificial Neural Networks
API:	Application Programming Interface
AUC:	Area Under the ROC Curve
BBC:	British Broadcasting Corporation
BERT:	Bidirectional Encoder Representations from Transformers
CNN:	Convolutional Neural Network
COVID-19:	Coronavirus Disease 2019
CPS:	Cyber-Physical Systems
CPU:	Central Processing Unit
CRISP-DM:	Cross Industry Standard Process Model for Data Mining
DDOS:	Distributed Denial-of-Service
DDPG:	Deep Deterministic Policy Gradient
DL:	Deep Learning
DNN:	Deep Neural Networks
DQN:	Deep Q Neural Network
F1-score:	Harmonic Mean of Precision and Recall
FANDC:	Fake News Detection on Cloud
FN:	False Negative
FP:	False Positive
GANs:	Generative Adversarial Networks
GB:	Giga byte
GitHub:	Web-Based Version Control and Collaboration Platform
GRU:	Gated Recurrent Unit
HDD:	Hard Disk Drive
HER:	Hindsight Experience Replay
IaaS:	Infrastructure as A Service
IEEE:	Institute of Electrical and Electronics Engineers
IoT:	Internet of Things
LSTM:	Long Short-Term Memories

ML:	Machine Learning
MLM:	Masked Language Modeling
MLPs:	Multilayer Perceptrons
MLR:	Mini Literature Review
MongoDB:	Mongo Database Program
MS Azure:	MS Azure Cloud computing Services
MS:	Micro Soft
NLP:	Natural Language Processing
NSP:	Next Sentences Prediction
OSN:	Online Social Networks
PaaS:	Platform as A Service
RAM:	Random Access Memory
RBFNs:	Radial Basis Function Networks
RNN:	Recurrent Neural Network
ROC:	Receiver Operating Characteristic
SaaS:	Software as A Service
SARSA:	State-Action-Reward-State-Action Algorithm
SOMs:	Self-Organizing Maps
SLR:	Systematic Literature Review
SQL:	Structured Query Language
SSD:	Solid-State Drive
TN:	True Negative
TP:	True Positive
URL:	Uniform Resource Locator
WHO:	World Health Organization

CHAPTER 1

INTRODUCTION

The introduction of this thesis is divided into six subsections. In the first part; the background of the problem, the statement of the problem in the second part, the aims and objectives in the third part, the significance and limitations of the study in the fourth and fifth parts, respectively, and the overview of the thesis organization are presented in the six sub-headings. In these sub-headings, the background in the formation of the problem is explained respectively, then the definition of the problem is made and the aim and objectives are discussed within the scope of the limitations of the study. In the last part, the thesis organization, which guides the detailed description of the study, is presented.

1.1 Background

Fake news is defined as viral content that looks like real news, based on fake information, that is, shared by too many users. Fake news may consist of completely false, incomplete, or false information, or it may also be an incomplete or biased presentation of true information. Fake news is intended to deceive its readers. Through traditional media or social media, it tends to give false information to the reader and mislead him. Some of this news attempts to mislead the reader or influence the reader's thinking about a topic. Some of these types of news, on the other hand, aim to increase the number of visitors to the website by giving an eye-catching headline and completely fabricating the content of the news. Fake news, by its very nature, is expected to cause an information disorder (Seddari et al., 2022a).

With the Industry 4.0 revolution, the rapidly digitalizing world has begun to evolve from an industrial society to an information society, and the age we live in has been named the information age. There is an increasing correlation between the abundance of information we face in the information age and the news circulating in traditional media and social networks. The relationship between attempts to mislead the public and fake news dates to the early days of journalism. However, with the spread of the internet and especially social media, this relationship gained a new dimension and moved to a more advanced stage. Digitization, which has caused great changes in the format, presentation, distribution, and consumption of news as well as news content, has also increased the

possibilities of the formation and dissemination of fake news. Manipulations can be made over news texts as well as images such as photographs and videos (Shu et al., 2017).

In the pre-internet era, news was under the control of professional journalists, such as journalists, editors, and news directors, called gatekeepers. They decide what is and isn't shared with the public. With the spread of the Internet, the influence of educated professionals in the news flow has decreased and it has become difficult to distinguish between true news and false news. The fact that everyone is a broadcaster, along with OSNs, has made it easier for fake news of unknown origin to be produced and circulated. Fake news has become a social problem as users share this fake news, sometimes consciously and sometimes unconsciously (Shu et al., 2020a).

Unfortunately, Turkey is one of the leading countries in the world in the production and prevalence of fake news. According to the Digital News Report published by Reuters every year, it shows that in 2022, approximately 62% of users in Turkey encounter at least one fake news every week (Newman, 2022). One of the main reasons for the prevalence of fake news is that users share news without checking whether it is true. Anyone can produce fake news for various purposes. The most important thing is how widespread fake news is, which is a situation related to users. Therefore, the fight against fake news begins with increasing the digital literacy skills of users. Obtaining a critical point of view, not sharing unverified information, approaching the information encountered in social media with suspicion, and having an idea about the sources from which information is obtained are among the things that users should do to combat fake news. A digitally literate user should be able to distinguish between right and wrong, the nature and quality of the accessed content while analyzing the content he encounters on the internet.

There are some ways to spot fake news encountered on the Internet and OSNs (WHO, 2024). These can be listed as:

- *To be skeptical of headlines*, fake news often has catchy headlines in all caps with an exclamation point. If the shocking claims in the headline sound preposterous, it's probably fake news.
- *Taking a close look at the web address (URL)*, a fake or fake web address may indicate false news. Many false news sites imitate real news sources by making minor changes to their internet address.
- *Researching the source*, it should be ensured that the news is written by a reliable source with a reputation for accuracy. If the news comes from an unknown organization, see the "About" section on the website for more

information. News sites that do not contain information about the owner should not be trusted.

- *Watch out for unusual typefaces*, many fake news sites have typos or weird page layouts.
- *Beware of photos and videos*, false news often contains manipulated images or videos. Sometimes the photo may be used out of context even though it is real. It's important to confirm the photo or image using Image Searches to understand where the image came from.
- *Examining dates*, the date and timeline in false news may be illogical or the dates of events may have been changed.
- *Checking the evidence*, check the author's sources to make sure they are correct. Lack of evidence or reliance on unnamed experts may indicate that the news is fake.
- *Looking at other news sources*, the absence of another news source reporting the same news may indicate that the news is fake. If the news is reported by more than one trusted source, the news is more likely to be true.
- *Is the news a joke?* sometimes it can be difficult to distinguish false news from humor or satire. Check if the news source is known for the parody and try to understand from the details and tone of the news if it is just for entertainment purposes (Affelt, 2019).

Human beings generally tend to believe in fake news that confirms what they believe. If some news coincides with the believed realities, it becomes difficult to doubt that news. Fake news is designed following this feature of people. It is important to be skeptical of news encountered on the Internet and not to share news that is not sure of its accuracy.

However, it will be very difficult to personally confirm as mentioned above. There are some fake news detection studies in the literature. However, none of these yielded real-time results but mostly remained at the experimental level. For the research, this study will detect fake news spread on Online Social Networks (OSNs) in real-time and evaluate it in seven sub-categories. In this context, Artificial Intelligence (AI) applications as well as Machine Learning (ML) algorithms were systematically reviewed to detect fake news quickly and accurately. Thus, possible difficulties were identified, and suggestions were made for both ML-based and AI-based detection systems in real life. However, the

available literature has shown that it is at the experimental level as previous studies focused more on the performance of algorithms to increase accuracy and precision, working with pre-labeled data rather than a dynamic dataset.

1.2 Problem Statement

The main challenge in the research area, unlike studies in the literature (Ahmad et al., 2022), is the real-time detection of fake news spread on OSNs. Since the studies in the literature focused on the success of ML algorithms (Goksu & Cavus, 2019a; Ahmed et al., 2021; Hakak et al., 2021; Lahby et al., 2022; Pal & Pradhan, 2023; Rawat et al., 2023) with previously labeled data, they could not reveal a real-time approach. However, in these studies, the detection of one or more types of fake news such as disinformation, misinformation, or hoax was generally studied. In addition, some other studies only used data collected from some news sources or websites (Ozbay & Alatas, 2020a; Umer et al., 2020; Huang & Chen, 2020a; Kaliyar et al., 2020a; Jiang et al., 2021; Li et al., 2021a; Verma et al., 2021a; Choudhary & Arora, 2021a; Liao et al., 2021a; Seddari et al., 2022b; Wei et al., 2022; Shihah et al., 2022) other than OSNs, that spread fake news and either rumors or hoaxes. However, the detection of fake news emerges as a problem that needs to be addressed holistically. As explained in detail in the literature review, which is the second part of the study, the types of fake news that are considered to be most widespread in OSNs were identified and divided into seven subcategories, which formed the basis of this study. In this study, each of the fake news, which is evaluated in seven subcategories: clickbait, disinformation, hoax, junk news, misinformation, propaganda, and satire, is discussed separately (Cavus et al., 2023).

A unique corpus has been created to fill this gap in the literature, detecting fake news spreading on OSNs and, in doing so, providing real-time feedback to OSN users across seven different categories while avoiding potential cyber threats (Cavus et al., 2023). Creating this corpus unique to the system has been achieved as a result of the complete and meticulous implementation of the text preprocessing steps of text mining (Işık & Dağ, 2020), which is a sub-category of data mining. Accordingly, it is considered that real-time fake news detection, implemented with the system called FANDC, will guide future studies.

Recently, there has been an increasing number of studies on fake news detection within the framework of developments in ML (Alghamdi et al., 2023; Altheneyan & Alhadlaq, 2023), NLP techniques (Al-Garadi, Yang & Sarker, 2022; Salloum et al., 2022), AI algorithms (Thang & Trang, 2023; Al-Asadi & Tasdemir, 2022) and text mining (Li et al., 2022; Tavana et al., 2022). However, in most of the studies, it is seen that the success rates

fluctuate at certain levels since the researchers do not create their corpus and they skip the data pre-processing stage classically (Çetin & Yildiz, 2022; Werner de Vargas et al., 2023). It has been seen that these studies are mostly carried out by using data belonging to a certain period and they are far beyond making a dynamic or real-time determination. These studies do not go beyond optimizing an algorithm or proving the stability of a data set (Goksu & Cavus, 2019b; Tsfati et al., 2020a; Ahmed et al., 2021; Al-Asadi & Tasdemir, 2022). Thus, the fake news detection problem is of interest at the experimental level. Secondly, the problem of detecting fake news is tried to be solved through traditional media tools related to this issue. There is many fake news sites created on this subject (theonion.com, newyorker.com, Abcnews.com.co, AmericanNews.com, etc.), or websites that hoax and make fun of the news, etc. exists. The data obtained from such sources is used as a reference source, which cannot go beyond being a source for repeated studies after a while. Third, it is known that fake news is circulated more in online social networks in parallel with today's technological developments. Traditional media tools, which have undergone a rapid transformation in the last decade, have been replaced by online social networks and have become daily news and information sources (twitter.com or x.com, Facebook.com, Instagram.com, web.whatsapp.com, linkedin.com, etc.). The development of mobile phone capacities and speeds as well as the speed of internet technologies is considered another trigger of this problem (Herrero-Diz et al., 2020). Finally, being able to be online and in real-time detection in fake news detection systems is inevitably the target of certain focal points or some legal/illegal organizations that are hostile to the country. Therefore, the system to be put forward must be online, avoiding cyber threats or being protected. Since this is considered to be a detailed study of a separate study, it is considered that the system's work on cloud computing will make a similar contribution. In this context, the absence of an online and real-time detection system represents a gap in the literature, while protecting or at least avoiding cyber threats is considered the biggest vulnerability in the literature.

1.3 Aim and Objectives

The main aim of this study is to develop a system that detects real-time fake news in OSNs in seven sub-categories with the BERT algorithm, an AI algorithm, avoiding cyber-attacks based on cloud computing. In this context, to achieve the main purpose of the study, the sub-objectives are listed as follows.

- With the developed system, is it possible to detect online and real-time fake news spread on OSNs?

- Is it possible to classify fake news spread in OSNs with the developed system?

In this context, the objectives of the study are as follows:

- To collect big data from Twitter via API and create a corpus to perform the analysis uniquely.
- To ensure that the corpus to be created is error-free by completely fulfilling all stages of data mining and text mining.
- To ensure that the data obtained in this framework is stored and operated dynamically in the database.
- To enable OSN users to make online and real-time inquiries.
- To ensure that the created system runs smoothly on the cloud.
- To avoid cyber-attacks.
- To detect whether the news is fake or not.
- To identify the type of fake news.

1.4 Contribution of the Study to the Field

The main contribution of this study to the field of Computer and Information systems is the real-time detection of fake news in OSNs within the framework of the purpose of the study and the active use of cloud computing systems to avoid cyber threats while doing this. The system, which works as a backup with the container structure created in the cloud, is more advantageous from possible cyber threats than a classic domain (teyitet.net). It is considered that cloud computing researchers will contribute to the production of more cyber security for the increasing security needs of such important websites. Within the framework of the data obtained from Twitter, the creation of the corpus produced for the system itself, together with a good data preprocessing process, will also contribute to researchers who want to work in the fields of computer science, text mining, and natural language processing. Thus, it is thought that future research will encourage researchers to create their corpus, excluding datasets shared on social networks or websites produced for fake news detection. In addition, the situation encountered when the literature is examined shows that fake news detection studies have a stagnant structure. In other words, a database obtained from social networks cannot go beyond an understanding in which a model is created and algorithms are tried or compared within the framework of this model. With this study, a system created with different algorithms such as BERT, ChatGPT, Bard, and Bing is recommended to researchers

working/will be working in the field of algorithm development, which will contribute to the creation of more different and text mining-specific models in the future.

1.5 Significance of the Study

With the Covid-19 pandemic, the rapidly increasing use of OSN and the changes in information/news practices have revealed the problem of fake news, which has a pretty widespread effect. To cope with this problem that affects daily life and behavior, this problem, which is handled differently from the studies in the literature, is important in that it is real-time and gives real-time feedback to OSN users by handling fake news in seven categories, and while doing all this, it works cloud-based and avoids cyber threats. Since there is no similar study in its field, the importance of this study increases even more. This study will contribute to OSN users and protect them from the possible harmful effects of OSNs by making fake news detection in OSNs in seven sub-categories and in real-time.

1.6 Limitations of the Study

The limitations of this research are limited to Twitter, which is one of the OSNs and is considered a micro-blogging network and is often used text-based. Because other OSNs usually have more complex sharing than text sharing. For example, pictures and short videos are usually shared on Instagram, and short texts are written under these posts. On the other hand, it is used by OSN users in the same context in parallel with the purpose of its emergence on Facebook. The study was limited to Twitter, as it requires more complex work to process images and videos and detect fake news on these networks. In addition, to create the FANDC corpus, 99 million tweets were sent from Twitter, which was used extensively during the Covid-19 pandemic period, between 01 January and 01 April 2020, and data were collected from certain tags. These tags are #pandemic, #covid, #Covid-19, #fakenews, #corona, #coronavirus, #coronavaccine, #vaccine, etc. consists of tags.

In this study, since ML algorithms are frequently studied in the literature, unlike ML algorithms, it is limited to Google's state-of-the-art BERT algorithm.

The fake news spread in OSNs is handled in only seven categories, which is unprecedented in the literature such as clickbait, disinformation, hoax, junk news, misinformation, propaganda, and satirical thus it has been limited to these seven categories.

Finally, since the *FANDC* system works with big data, it is thought that the storage capacity and processor of a computer will be insufficient, so the studies were carried out in

the cloud, not on the local computer. It was run on MS Azure Cloud Computing with 20 GB RAM, 500 GB SSD HDD, and 8 Core CPU processing power.

1.7 Overview of the Thesis

The present thesis contains five distinct chapters described as follows:

The first chapter is the introductory part of the thesis report that explains the main study aim and statement of the problems that motivated embarking on the study, it also highlights the significance of carrying out the study, as well as some of the limitations faced.

The second chapter entitled “Literature Review” is the backbone of the research that updates readers on what was done on the research topic, what is the research gap, and what we could foresee from the future. Accordingly, the second chapter portrays the systematic approach followed in searching, analyzing, and discussing related works thematically, methodologically, and chronologically. And, the “theoretical framework”, explains the information needs of the information society, which the thesis deals with, and how it is tried to be achieved individually. Afterward, the relationship between online social networks and fake news as a means of accessing information or news is conceptually discussed. How fake news spreads in online social networks their detection methods and possible effects on society are explained.

The third chapter titled “Methodology” describes the recommended research procedure used during research data collection, data analysis, and report writing.

The fourth chapter of the thesis explains the results obtained with the created system.

The fifth chapter of the thesis includes the discussion section and its subcategories within the framework of the results obtained.

The sixth chapter, which is the final chapter of this thesis, concludes with the conclusions obtained within the framework of the findings, and recommendations for future studies.

CHAPTER 2

LITERATURE REVIEW

Research-related conceptual definitions, descriptions, and information related to the subject that already exists in the literature are given in this chapter. This chapter as the backbone of the research updates readers on what was done on the research topic, what is the research gap, and what we could foresee from the future. Accordingly, the second chapter portrays the systematic approach followed in searching, analyzing, and discussing related works thematically, methodologically, and chronologically.

2.1 Theoretical Framework

This section provides explanations of the theoretical basis for efforts to detect fake news in OSNs using ML and AI models. This research effort includes expertise in computer science, data science, text mining, cloud computing and AI. Specifically, this section will discuss in detail the processes of obtaining information and reaching news from traditional media to social media, the concepts of online social networks and fake news, how fake news spreads in OSNs, its effects on society and detection methods.

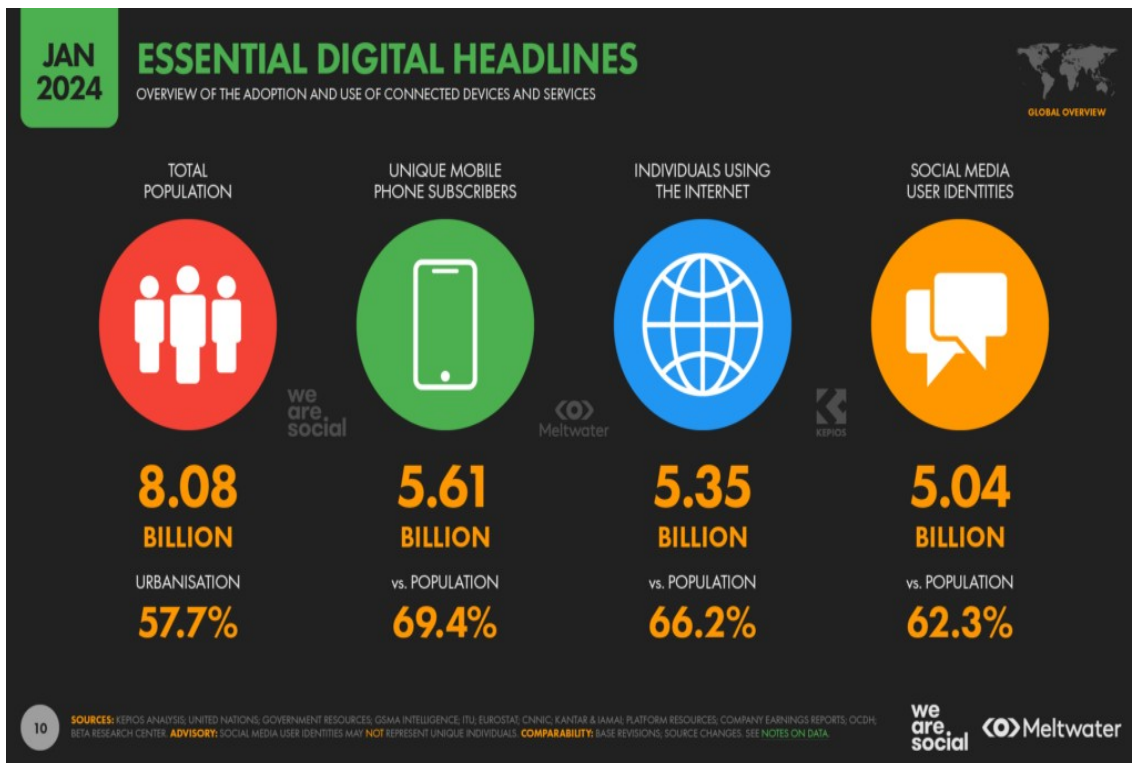
2.1.1 Online Social Networks and Fake News

To fully understand online social networks, it is necessary to examine the concept of “new media” first. New Media is an innovative concept that has taken part in all human lives all over the world with the digital transformation of media. It is the general name given to the types of media that use digital technology together with the use of social media and the internet (Zinderen, 2020). It can also be defined as new methods developed for old technologies. Newspapers and magazines include instant digital sharing, unlike older media, which refers to traditional forms of media such as television and radio. In general, the term “new media” identifies content that is available on-demand by humans over the internet from any place in the world (Walther & Whitty, 2021). This content can be viewed by the user on any smart device such as mobile devices, mobile phones, etc. at any place that has an internet connection in the world. Also, it allows users to interact with the content in real-time by adding their own opinions and making it easy for them to share the content with their friends just in time and socially. On the other hand, network society, which emerged as a result of these technological developments, has started to use more online social networks in accessing

information (Van Dijk, 2016). In this context, the first quarter of the 2000s we are in has been named “new media age” or “information age” (Duff, 2023). With the introduction of internet technology into our lives, the circulation speed of information has increased accordingly. In the beginning, internet technology, called Web 1.0, was not open to the active participation of users. Later, with the development of Web 2.0 technology, which allows the participation and interaction of users, individuals have become active users of the internet with many ideas and designs of their own (Ersöz, 2020). The features of new media, which can be listed as digitality, interaction, multimedia, user-based content production, hypertextuality, diffusion and virtuality, have triggered the development of social networks. Within the framework of all these features, social media or social networks have emerged with the individual use and spread of the internet. Thanks to social networks, users can not only communicate with their environment, but also share many contents and messages such as information, news, photos, videos from these platforms. Accordingly, social media/networks, unlike traditional media, are environments in which individuals actively participate. Social networks, in which users play an active role, eliminate one-way communication and allow mutual interaction. Messages, news, or any information created on social media networks belong to the users themselves. Social networks also can be defined as environments where people can produce content as they wish and publish their ideas and thoughts. Social networks, blogs, wikis, microblogs, photo and video sharing sites are examples of social media/networks applications (Sasahara et al., 2021). All these processes are directly proportional to the increase in the adoption of mobile technologies, as seen in Figure 2.1(Kemp, 2024a).

Figure 2.1

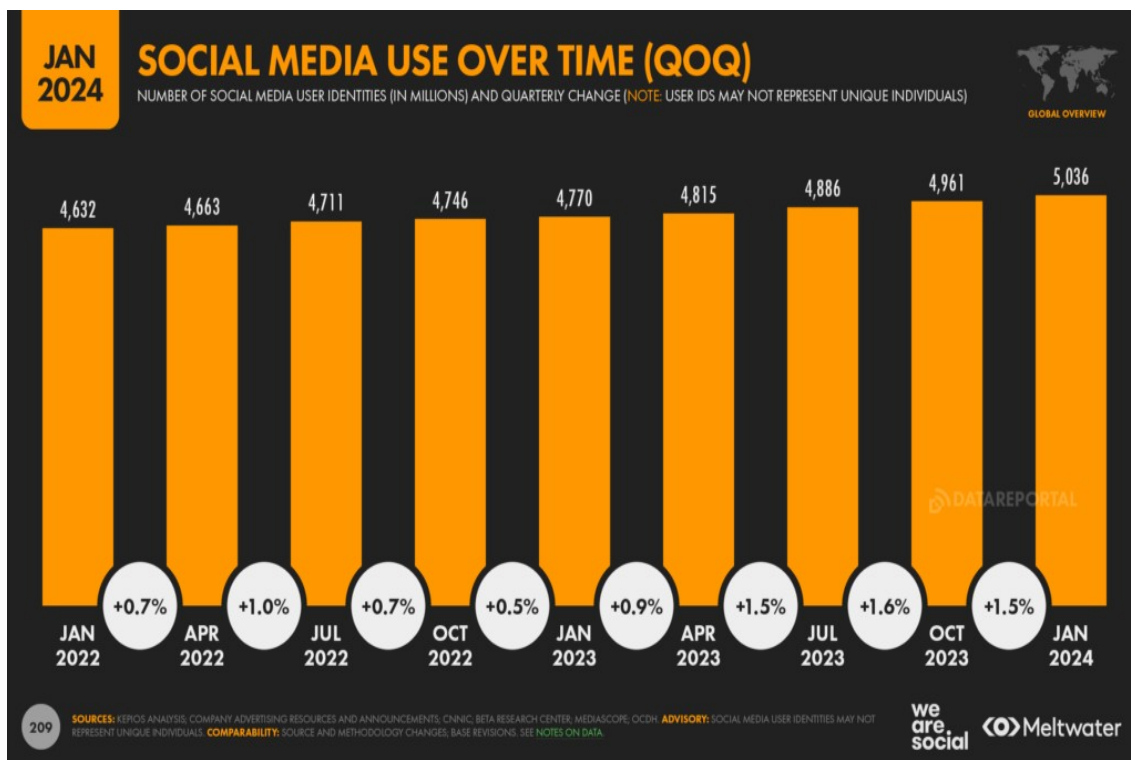
*Overview of the adoption and use of the connected device and services as of January 2024
(Kemp, 2024a)*



Undoubtedly, the developing communication technology and mobile phones have a great impact on this increase. As can be seen in Figure 2.2, the use of social networks is increasing every year (Kemp, 2024b).

Figure 2.2

Change in the use of connected devices and services over time of January 2024 (Kemp, 2024b)



Social networks have a very important effect on creating consumption patterns that can be considered uniform throughout the world, converging the standards of access to information, and creating a global mass culture in the world through social networks. In this context, it is considered that the role of the Internet in changing the flow of daily life through social networks in the transition from “the information age” to “the disinformation age” is quite effective. The change in the new social structure brought about by the accelerating globalization, accompanied by the accelerating effect of social networks in accessing information, resulted in the deterioration of social life and daily social life rapidly shifted to social networks. As a result, people who are users of social networks have begun to be seen as an object rather than a subject by social network service providers. In other words, the human being, the consumer of social networks, has become the main product. In social networks, each product, that is, human perceptions, has been manipulated and kept somewhere between reality and truth and has become the object of future transactions. In social networks, the number of users and the constant online presence of users are important. Because people with

high consumption potential have the potential to see and read all kinds of information sent to them on social networks, and to share it with their followers, as well as being affected. For example, on Twitter, which is considered a microblogging network, it is known that fake news spreads six times faster than real news. Due to this feature, Twitter is the social network with the most misinformation and disinformation. At this point, one of the biggest manipulative problems of social networks such as misinformation and disinformation spread because of the post-modern age has emerged.

2.1.2 Fake News Concept

Fake news, which is considered to have emerged with the widespread spread of daily news after the invention of the printing press, highlighted its actuality in parallel with the technological developments of the fourth industrial revolution. However, there is no agreed definition of the term “fake news”. If we look at some of the commonly used definitions of fake news in the literature, it would be possible to briefly define it as “news articles that are intentionally and verifiable false and may mislead readers” (Tandoc Jr et al., 2018). Fake news contains false information that can be verified and is created with dishonest intentions to mislead consumers.

This definition has been widely adopted in recent studies. If we look at the broader definitions of fake news, the focus is on the authenticity or purpose of the news content. Treating deceptive news that includes clickbait, disinformation, hoax, junk news, misinformation, propaganda, and satire directly as fake news offers the broadest framework that fits this definition. In this context, fake news is divided into seven categories in this study. Looking at the concepts in these seven sub-categories of fake news;

- *Clickbait*, is defined as the use of exaggerated and eye-catching headlines to get users to click on the link. The most striking feature of the clickbait is that the title and the content are unrelated to each other. While the title makes exaggerated promises to readers, the content doesn't deliver on that promise. When the link is clicked, the information to be accessed is not included in the content (Zhou, 2017).
- *Disinformation*, the deliberate dissemination of dirty information in OSNs or media organs to mislead the public is called 'disinformation'. Disinformation is a method often used to create public opinion or cause chaos with distorted and false information. Disinformation activities start with the dissemination of small bits of information through certain individuals and groups and can grow

to cause outrage. Unconfirmed information, inadvertently or deliberately magnified by OSN users, quickly manipulates audiences, and leads to greater confusion (Alam et al., 2021).

- *Hoax*, deceptive message or humour is content based on fake news or false information created to influence audiences or defame brands. The highest possible social claims can be defined as fabricated news and its dissemination with the aim of influencing large numbers of people. The aim here is to trick the victims into accepting the claim or news without thought (Shu et al., 2020b).
- *Junk News*, it's a sarcastic term used on OSNs for news that includes sensationalized, personalized, and homogenized unimportant junk. It is very easy to generate and propagate in OSNs as it does not contain specific information. Most of the time, it is not used for reading, but only for affecting the target audience in some way (Venturini, 2019a).
- *Misinformation*, is defined as misinformation shared without the intention of harm and its spreading process. In other words, disseminating false, inaccurate, or incomplete information, with good or bad intentions, can be defined as misinformation (Wu et al., 2019).
- *Propaganda* is defined as ensuring the systematic dissemination of certain ideologies by making use of various means of communication and forcing individuals to accept a system of thought or fulfill the requirements of the system. On the other hand, propaganda is also described as a predefined form of communication made by individuals or state bodies and aimed at influencing and manipulating people's behavior in a certain way. Propaganda has two indispensable features as influence and manipulation (Chaudhari & Pawar, 2021).
- *Satire* can be expressed as the content produced by satirical news sites or the posts prepared for parody but with the potential to be mistaken for real by the users, or it can be defined as the realization of the fictional content created for the purposes such as sarcasm, criticism, entertainment, although its main purpose is not to create or spread false news (Onan & Toçoğlu, 2020).

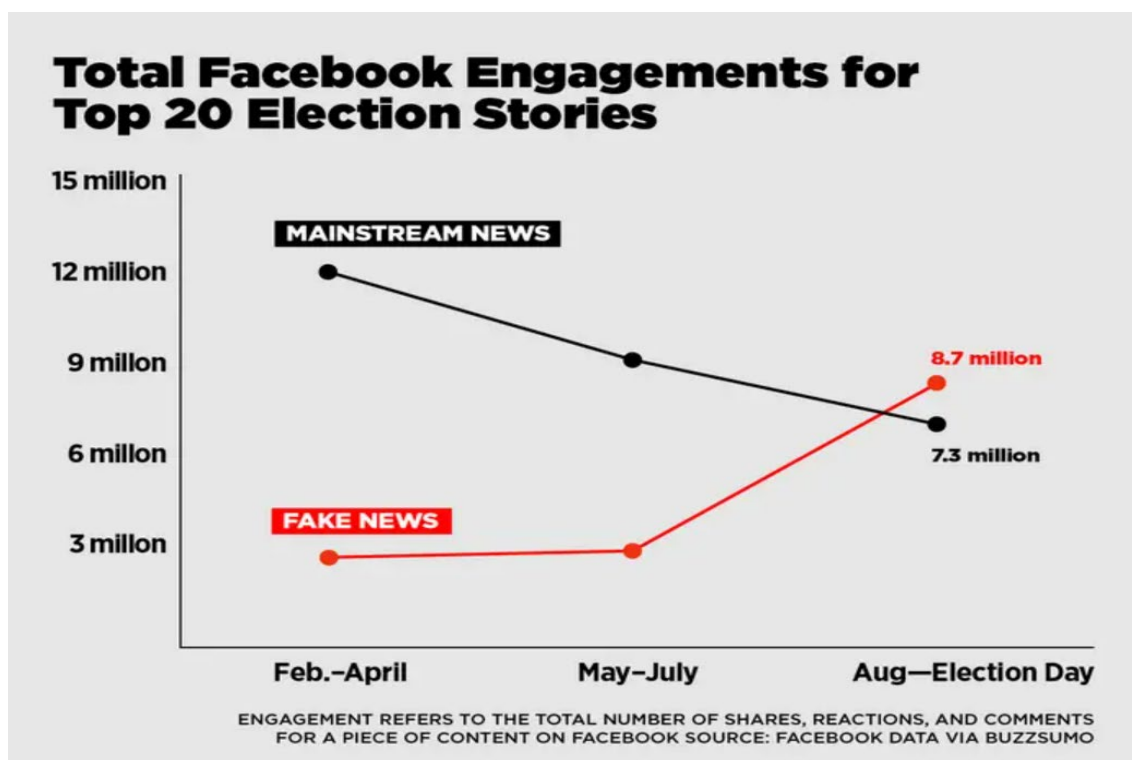
The influence of the media, especially social networks, on societies in the post-truth era should not be denied. Thanks to OSNs such as Twitter and Facebook, whose content is

created by users and which enable bilateral/simultaneous sharing of information on the internet, billions of people have access to information in a very short time. In addition to the positive features of OSNs such as speed, and easy and cheap accessibility, the fact that the information they contain is often unchecked is an important problem (Tsao et al., 2021).

OSNs influence in social events showed itself in the anti-globalization protests protesting the meeting of the World Trade Organization (WTO) in Seattle in 2000 (Seattle Municipal Archives, 2000) the Green Movement that emerged in Iran in 2009 and then the Middle East in 2010 (Milani, 2010). OSNs had an unexpected effect on societies in the Arab Spring that broke out in the Middle East. In fact, the Arab Spring has begun to be called the “Facebook Revolution” by many (Wolfsfeld et al., 2013). Similarly, the influence of OSNs in daily politics has increased noticeably and US President Barack Obama took the title of “digital president” by using OSNs very effectively in the 2008 elections (Bimber, 2014). However, it can be said that manipulation, disinformation and distorting the truth with fake news emerged mostly in the Brexit vote and the US elections in 2016. Although the information pollution in OSNs during Donald Trump's presidential election campaign did not directly affect the election results, the effect of these news on the voters was partially accepted (Hall et al., 2018). In this context, Gabler is not wrong to use the definition that *“Twitter is to Trump what radio is to Franklin D. Roosevelt and television is to JFK”* (Walter & Andersen Tuttle, 2023). Groups supporting Trump, who throughout the campaign claimed that President Obama and Hillary Clinton were the founders of ISIS, that Obama was not a US citizen, and that Hillary Clinton laughed at a 12-year-old rape victim, said that, they occupied the public's agenda for a long time with fake news such as *“He Will Call to War”*, *“Barack Obama Confessed Born in Kenya”*, *“FBI Agent Involved in Hillary's Corruption Infiltration Dies”*. If we consider the rate of spread of this news and its position against the mainstream media, it would be useful to look at BuzzFeed's analysis in Figure 2.3 (Silverman, 2016). According to this research, while sharing and commenting fake news by US users on Facebook in the USA increased from 3 million to 8.7 million in 2016, this number decreased from 12 million to 7.3 million for the news of the mainstream media.

Figure 2.3

Buzzfeed Analysis (Silverman, 2016)



Although fake news has come to the fore with the 2016 presidential election in the USA, it still maintains its old popularity (Stahl, 2018). Fake news, information pollution, misinformation and disinformation are widely used in all kinds of thoughts and opinions in the form of propaganda, rumors, hoaxes, and trivial news (Meel & Vishwakarma, 2020). In this context, OSNs are generally used to gather users around a certain idea or to manipulate users who gather around the same idea to direct them according to their own social-political or economic interests. In fact, although the purpose is very different, the primary goal is to manipulate users by creating information pollution in OSNs. Economic crises, low-intensity regional wars, political conflicts arising from border violations between the two countries or extraordinary situations such as the current Covid-19 pandemic are also frequently seen, especially in country elections. Both scientists and journalists argue that OSNs that emerged within the framework of technological developments trigger social movements.

For instance, The Yellow Vests movement, which broke out on 17 November 2018 when more than 280 thousand people took to the streets in France to protest the government, is perhaps the most current and sharp manifestation of the anti-austerity protest wave in Europe. Aside from the global background of these protests, the Yellow Vests have historical

significance for France. Because the Yellow Vests are claimed to be the biggest social event that France has experienced since the 1968 movement. The main reason for the social movement that started with the Yellow Vests protest in France was the desire to cancel the additional environmental tax enacted by President Macron. The movement, which initially started as a democratic right-seeking movement, became increasingly violent as the activists multiplied. Even the mass of the people, who remained outside of this situation and did not take kindly to the action issues, began to lean towards the events. We can state that the main communication tool in the protest movements that started in France is social media. Hours before the government canceled the proposed tax hike on 06 December, 2018, a poll for French newspaper Le Figaro found that 78% of the public believed the Yellow Vests were fighting for the general interest of France (Ramaciotti Morales et al., 2022). According to BFM TV, the date when the fuel tax was withdrawn on the same day was the day when the active groups on Facebook, La France en colère (AngryFrance), Gilet Jaune and Gilet jaune, interacted the most. Users across France shared images and texts on Facebook expressing their anger and condemning the government. While these pages have come to the fore, so-called “angry groups” have started appearing on Facebook since January 2018. For regions in the country's geography, such groups were organized to share people's grievances on political and economic issues. Also, the speed and popularity of these groups in their spread coincide with the change in Facebook's algorithm too (BBC, 2018).

Fake news is frequently seen in situations such as extraordinary situations, especially in country elections, economic crises, low-intensity regional wars, political conflicts arising from border violations between two countries or the ongoing Covid-19 pandemic. The aim here is to manipulate the environment as desired by inciting people to fear and panic in OSNs (Zhang & Ghorbani, 2020). However, even though OSNs such as Facebook and Twitter try to take some precautions for their users, malicious people continue to exploit these networks (Iosifidis & Nicoli, 2020). For example, if we go back to the days when the corona virus first appeared, it is seen that there are extremely unfounded and misleading news and even pictures (Figure 2.4, <https://twitter.com/Michael61070620/status/1252751416109617152>) circulating on social networks that it is transmitted to people from foods such as bat and dog meat, which is usually consumed by the Chinese.

Figure 2.4

Bat-eating Chinese Twitter screenshot

(<https://twitter.com/Michael61070620/status/1252751416109617152>, Retrieved from Apr., 30, 2020)



Regardless of whether the content of these shares is correct or not, the circulation of OSNs has caused interaction between people by making propaganda material. It has occupied the public by being shared again and again by people who do not have good intentions. Arguments such as fake news, misinformation, disinformation, and propaganda, which were only seen in small-scale events/crises that occurred in local regions before the Covid-19 pandemic, lead people to suspect what is true and false with the epidemic becoming global (World Health Organization, 2020). For instance, while the fifth-generation communication system trials in the UK continue in certain regions, completely unfounded and fake news that 5G antennas emitted from OSNs triggered the coronavirus and increased its spread ended with the burning of 5G antennas, and 5G trials had to be postponed for a while (United Kingdom Government, 2020). In addition to the extremely realistic and natural measures such as masks, distance, and cleaning rules taken to protect against the coronavirus, the lie that colloidal silver treats Covid-19, which is also spread from OSNs and which has no scientific evidence, would prevent people from coronavirus, has also been used in history as a disinformation tool in the era of information abundance (Jeremiah et al., 2020a). Undoubtedly, the most important and still ongoing discussion of the corona pandemic is the issue of vaccination. Although it was thought at first that a vaccine could protect people from

this pandemic, when the necessity of a second dose of vaccination was reported by the authorities in the future, it caused great reactions all over the world (Centers for Disease Control and Prevention, 2022). The WHO, which could not remain indifferent to all of these, published a statement on its website entitled 12 Myths about the Coronavirus and declared the situation an "infodemic" (World Health Organization, 2022).

As a result, it can be seen from the examples above the most important innovation brought by social networks to the field of communication is that human communities who communicate face to face and socialize come together in virtual environments and share ideas, news and information in such environments. With this feature, social networks play an important role in the emergence and organization of social movements.

2.1.3 How To Spread of Fake News on Online Social Networks

OSNs are emerging networks to meet the daily news needs of people at all levels, from local to global, as well as to socialize and communicate with their surroundings. Especially they have emerged and become popular over the past 20 years. Nowadays, it does not seem possible to think of people without internet or in other words as separate from the network. In this sense, concepts such as "network society", "informationalism", "Fourth World" put forward by Castells (2016) have been the keywords used to explain the global changes and transformations in our age.

"The emergence of a new technological paradigm organized around new, more powerful, and more flexible information technologies has allowed information itself to become a product of the production process. By transforming the information processing process, new information technologies have become effective in all areas of human activities, making it possible to establish infinite connections between various fields, as well as connecting representatives and members of these activities" (Castells, 2008: p.75).

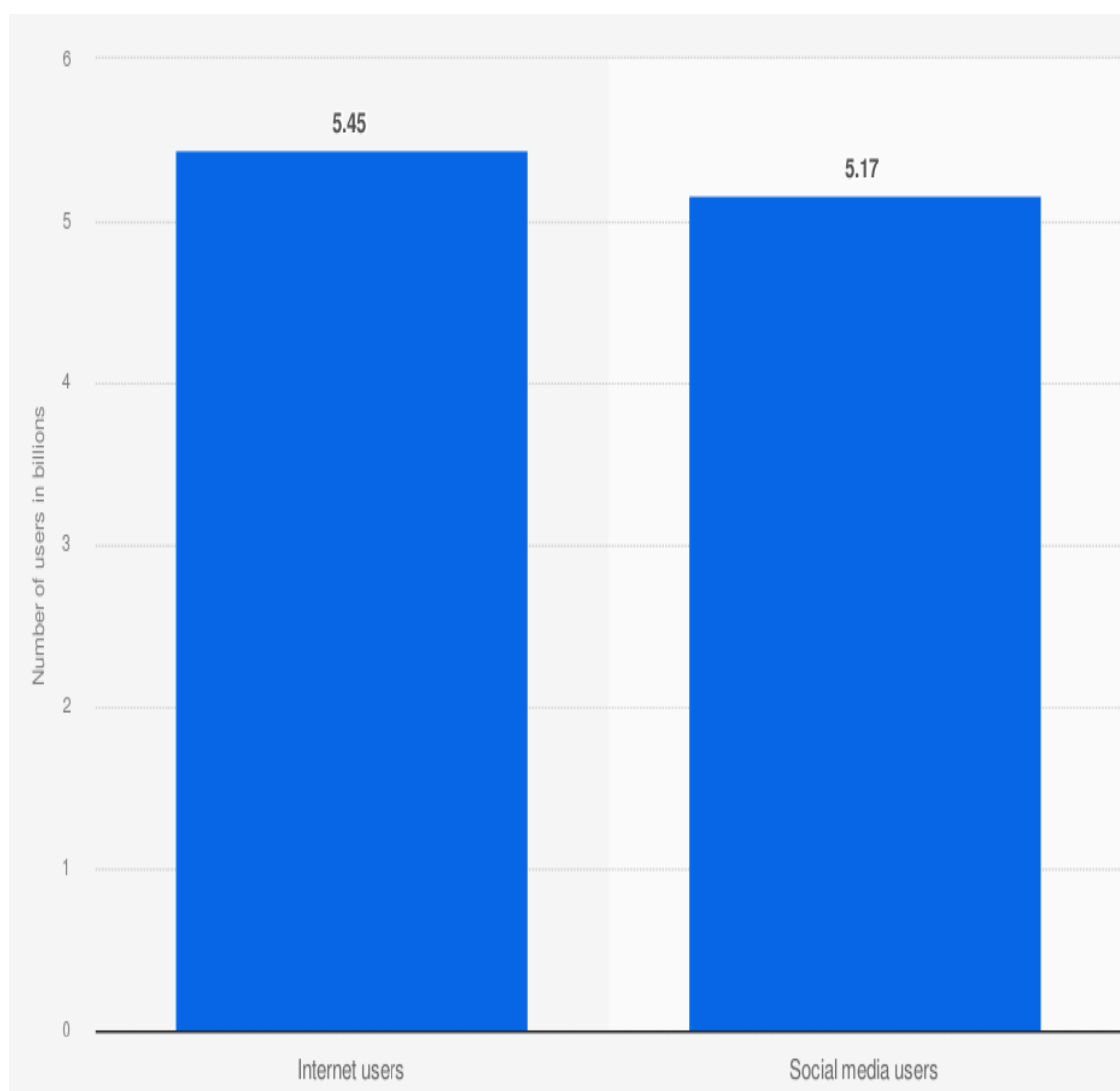
Again, according to Castells' this definition, "in such an uncontrolled, confusing world of change, people have become inclined to regroup around their essential, i.e., ethnic, religious, territorial, national identities (p.130)". In this sense, with the emergence of new identities in social networks, traditional grouping mechanisms are seen to differ even more in OSNs.

Dijk (2016b), on the other hand, has defined the term "network society" as a form of society that increasingly organizes its relations in media networks, replacing or complementing social networks of face-to-face communication. This means that social and media networks have shaped the most important organizational form and most important structures of modern society.

In this context, the number of internet and social media users worldwide published by Statista is shown in Figure 2.5 (Petrosyan, 2024, in billions). Accordingly, it is seen that the use of social media has increased in parallel with the increase in internet use. In this respect, increasing OSN usage means an increase in the amount of data spread on these platforms, thus indicating the amount of news spread on OSNs.

Figure 2.5

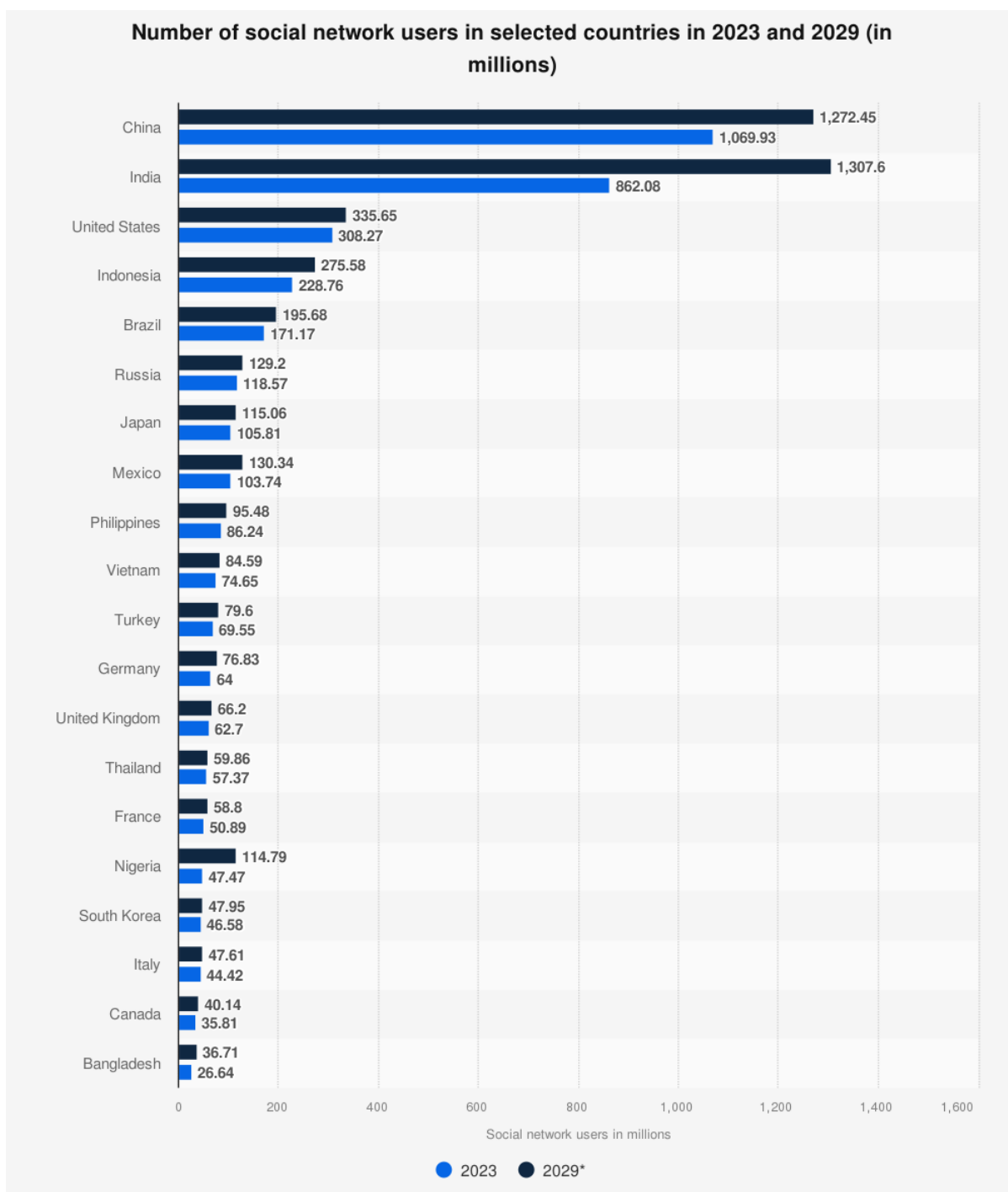
Number of internet and social media users worldwide as of January 2024 (Petrosyan, 2024)



The forecast for the increase in social network usage in selected countries between 2023 and 2029 is given in Figure 2.6 (Dixon, 2024a). It is evaluated that OSNs will be used even more with this increase.

Figure 2.6

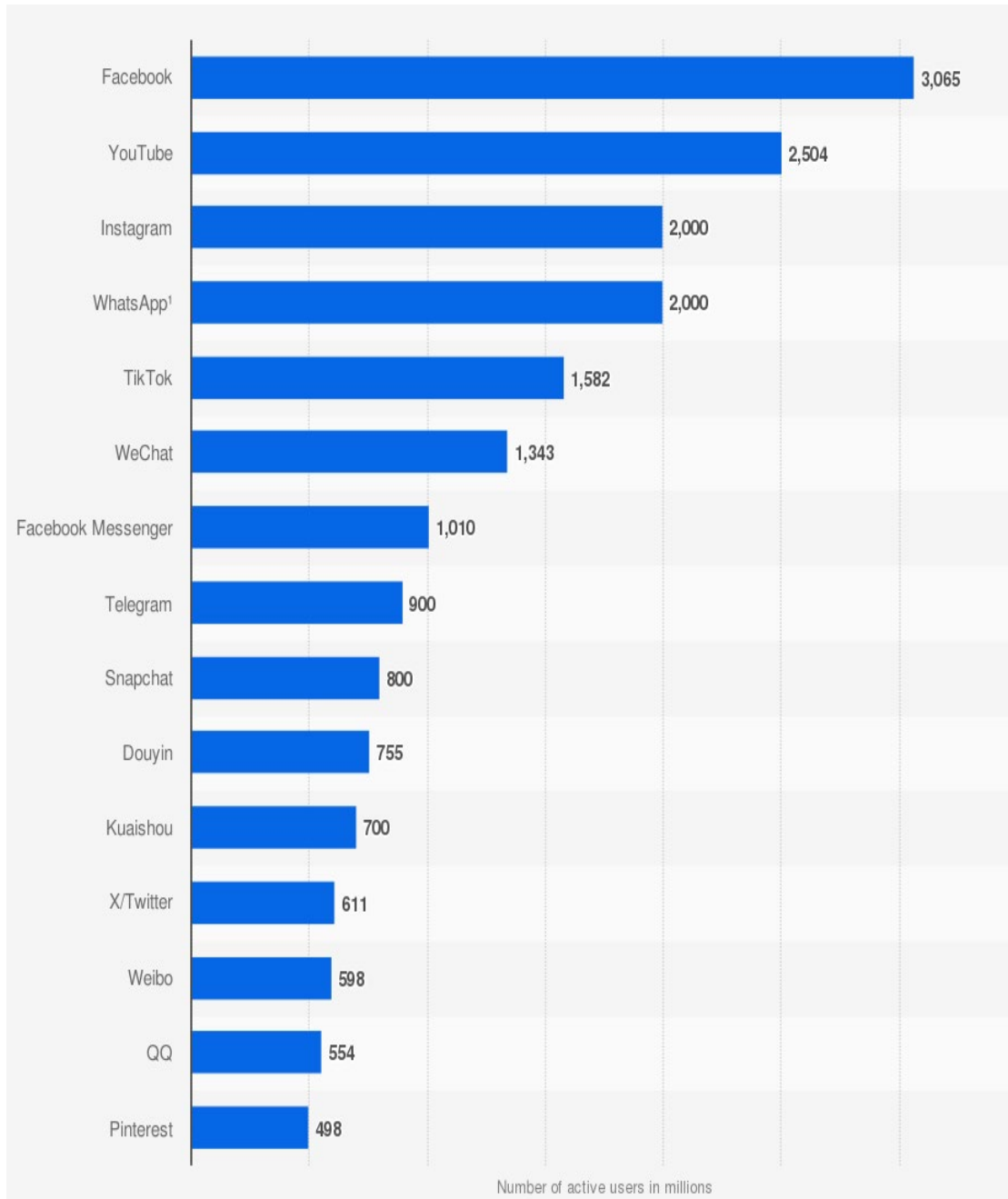
Number of social network users in selected countries in 2023 and 2029 (Dixon, 2024a)



According to Dixon (2024b), the ranking of the most popular social networks according to the number of monthly active users published in the research he conducted for Statista is shown in Figure 2.7. In the light of this data, the most used social platforms are listed as Facebook, YouTube, Instagram, and WhatsApp.

Figure 2.7

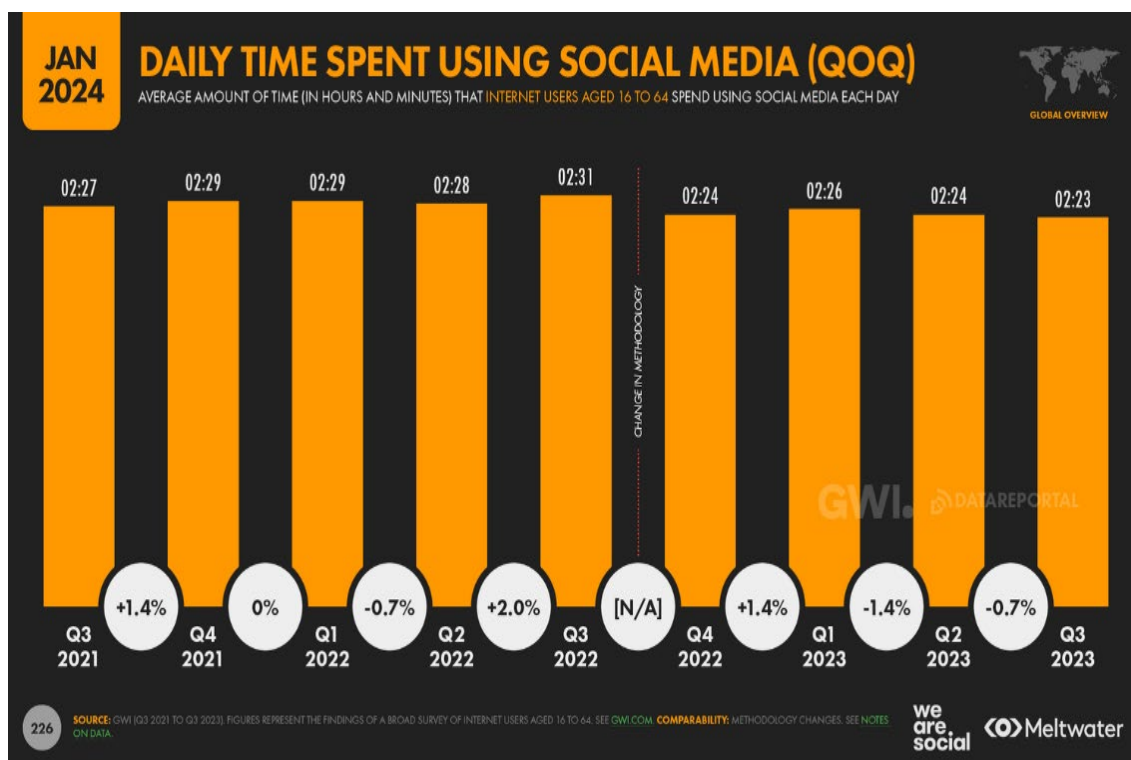
Most popular social networks worldwide as of January 2024 (Dixon, 2024b)



According to the Datareportal, Figure 2.8 shows (Kemp, 2024c) the average daily use of social networks in the quarter of the last three years.

Figure 2.8

Daily Time Spent Using social media as of January 2024 (Kemp, 2024c)



In the light of these data, it is strikingly understood that OSNs are gaining importance day by day and that we are a network society that grows with the information society. In this context, fake news spread on OSNs occurs in two ways. Malicious/bot accounts and echo chambers.

2.1.3.1 Malicious Accounts in OSNs

Social network users ubiquitously can socialize on OSNs for various reasons, interact with their friends, and be informed about regional and global developments anytime, anywhere (Du et al., 2019). Sometimes, for example, organizations use social networks to promote their products and reach customers directly through their own networks (Kauffmann et al., 2020). The situation is no different in academia. Academics or academic institutions use them to publish articles and record citations. Similarly, the classical news media announces breaking news on these platforms (Alkhodair et al., 2020). However, this popularity of OSNs also causes them to be misused from time to time. These abuses often stem from accounts called bots. Bot accounts are malicious accounts specially designed to cause harm, such as manipulating fake news, misinformation, disinformation,

and dissemination on OSNs (Orabi et al., 2020). Maybe they were created for a short time by well-intentioned people just to spread deception and rumors. But, these bot accounts in OSNs have the purpose of manipulating users to misinform, mislead, hide the facts, cover up, and confuse them. “Bot”, short for robot, is a software program that runs repetitively, and automatically, and performs predefined tasks. Bots often imitate or replace the behavior of human users (Wu et al., 2021). Because they are automatic, they work much faster than human users. They can perform useful functions such as customer service or indexing search engines, or unlike they can be used in the form of malware to gain full control over a computer (Xia et al., 2019). Organizations or individuals use bots for repetitive tasks that would normally need to be done by a human. The tasks undertaken by bots are usually simple and performed much more quickly compared to human activity. While the tasks performed by bots are generally useful, sometimes bots are also used in criminal activities such as data theft, fraud, or DDoS attacks. In OSNs, bot accounts are automated social media accounts that look like real profiles but are actually run by an algorithm. Bot accounts, also called social bots, are malicious accounts specially designed to cause harm such as manipulating and spreading fake news on OSNs (Derhab et al., 2021). For example, it is known that 19 million bot accounts manipulated OSNs in the 2016 US presidential election. Although these accounts, which are frequently encountered in OSNs, have been discussed for their role in online public discussions in recent years, OSNs do not only harbor malicious bots. For example, there are also bot accounts that automatically post poems, photos, or weather.

On the other hand, there are also users called Trolls, who are frequently encountered in social networks from other malicious accounts in OSNs. A Troll is defined as someone who interacts with other online users using controversial comments or provocative posts. Their aim is not to create a critical or constructive speech, but to sabotage the discussion, polarize the parties, and create an environment where no one listens to each other by causing impulsive reactions and where prejudices deepen (Tomaiuolo et al., 2020). While troll content does not always carry an obvious political motivation, it is used to describe OSN users who make such provocations for entertainment purposes. Where we come from today, the term troll is also used for people who attack other users with discriminatory, xenophobic, sexist, and homophobic comments, interrupt the discussion and use mostly anonymous or fake accounts (Freelon et al., 2022). Trolls are separated from bot accounts because there is a real person behind the account, which acts to provoke and deliberately deepen the discussion. Bot accounts are

automated OSN accounts that look like real profiles but are actually run by an algorithm (Mazza et al., 2022). However, it is also known that in some cases, troll accounts support the news they want to spread with bot accounts.

Research conducted by Carnegie Mellon University has revealed that almost half of the posts about the Covid-19 outbreak on Twitter are bot activity (Allyn, 2020). Another study reveals that 25 percent of the posts about the climate crisis belong to bot accounts and that climate denial is at the center of these posts (Marlow et al., 2021). It is shown that for whatever reason, the primary purpose of manipulating bot accounts is to try to change perceived facts. It is estimated that 25% of the fake news spread on Twitter, which is a very popular micro-blogging site in OSNs, originates from bot accounts. Taking the example of the 2020 US presidential election, for example, bot account activity on OSNs has increased more than ever before (Ferrara et al., 2020). From this point of view, such malicious bot accounts try to change their election behavior by influencing the emotions and thoughts of OSN users. Likewise, fake news that the Sars-Cov-2 virus, which emerged during the Covid-19 period and was heavily promoted in OSNs in the first days of the Pandemic (Goksu & Cavus, 2023), is transmitted from animals to humans and is the most important proof of this can be given as an example, which is the news that spread rapidly in OSNs and the Chinese who consumed dog meat (Yang, 2021). In this framework, OSN users, who were under intense information pollution after a while, started to think and share the same things, and a natural disinformation environment was formed.

2.1.3.2 Echo Chamber Effect

As stated above, OSN users, who start to think and share the same things under intense information pollution, begin to fall under the influence of echo chambers and filter bubbles. In this context, with the outbreak of the Covid-19 pandemic throughout the world, there are concepts such as "echo chambers" and "filter bubbles" at the beginning of the problems that occurred during the information age people's access to information, changes in information-seeking practices, and the abundance of information revealed (Cinelli et al., 2021). Everything that is clicked on the internet creates a digital footprint. Search engines and OSNs follow these tracks using different algorithms and offer personalized content to users. Thanks to the algorithms, it is aimed to get more clicks, more views and more interaction. For example, a product viewed on one site appears as an advertisement on another site. Filtering the personal data from the digital footprint and exposing it to similar content that the user is interested in or may be interested in creates filter bubbles (Mir et

al., 2022). The best example of filter balloons is when looking at a product on shopping sites or when the product is added to the cart, they direct people to another product they think you can buy with their content in the form of "Similar products you can buy" (Aridor et al., 2020). Although it is thought that search engines are used more effectively and efficiently thanks to filter balloons, it is thought that search engines take control by deciding what information the user should see. The fact that filter balloons and echo chambers leave the user to a biased and uniform information flow paves the way for their use as censorship to control public opinion. The information age we live in has turned into the age of disinformation because of concepts such as misinformation, disinformation, propaganda, and fake news that emerged with the shift from social life to digital channels, especially during the Covid-19 period. In this period when reality and truth lose their meaning, following a certain group on OSN or being dependent on certain news headlines can lead to information pollution, be it personal preferences or the filter bubbles applied by OSNs. As social beings, people will want to be in social environments that they find reliable within the framework of information-seeking practices by exhibiting similar behavior patterns in OSNs. Thus, they will gravitate towards sources of information that are considered safe, which will result in the OSNs creating their echo chamber even if they are not caught in the filter bubbles. Another paradox of OSNs is that often-shared information is shared assuming it is true. For example, as Jeremiah et al. (2020b) mentioned, the news that colloidal-silver water has been effective in protecting people from viruses since ancient times in the Covid-19 pandemic has been reflected in OSNs and indirectly in the society. This has transformed the users, both producing and consuming information, into a homogeneous structure. As a result, it has become an important argument in the dissemination of fake news, as the extremes of ideas and opposing views occur in homogeneous communities.

2.1.4 Fake News Detection Methods

The amount of information shared in OSNs has increased in parallel with the increase in processor speeds and data storage capacities, especially thanks to the technological developments that have occurred with the Industrial 4.0 revolution. Increasing information sharing has led to the spread of the aforementioned fake news concept (Tsfati et al., 2020b). ML (Ahmed et al., 2021) and AI (Al-Asadi & Tasdemir, 2022) methods are widely used in the literature to detect fake news in many forms such as propaganda, disinformation, misinformation, clickbait, hoax and so on. ML is the ability to use the optimal algorithm to

transform a dataset into a model. ML algorithms are a kind of engine of ML, that is, they are algorithms that transform a dataset into a model. Which type of algorithm works best depends on the type of data analyzed, such as supervised or unsupervised, classification, regression, available resources, the nature of the data, and what is desired at the end of all processes (Nasir et al., 2021). In this sense, fake news detection is considered as a classification and regression problem. For example, identifying types of fake news can be a clustering exercise that can be handled with ML. As there are many studies in the literature on fake news detection, the most basic requirement is the linguistic analysis of the texts that make up a large part of the news data.

AI, on the other hand, can be summarized as “the ability of a computer or computer-controlled robot to perform various activities in a similar way to intelligent living things”. AI, perhaps one of the most important concepts of our age, is a very detailed field that can be studied on its own (Madani et al., 2021). Systems that can exhibit behaviors that are observed in living beings, especially humans, and which are characterized as intelligent behavior, have found a wide range of applications in Natural Language Processing (NLP), as in many other disciplines (Saquete et al., 2020). In this context, ML methods are a very popular approach to solving the fake news detection problem. Detecting fake news with tools like ML and AI is a classification problem. For this, a corpus is created by labeling the data that is considered both false and correct in the pre-trained model, and the result is obtained by comparing it with the existing data to be tested in this framework (Goksu & Cavus, 2019c). In all techniques to be created for fake news detection, steps such as preparation of the data set, preprocessing, selection, and creation of the model are applied first (Hickman et al., 2022). However, besides these techniques, there are also classically created and human-centered fake news detection sites. For example, while there are international websites such as Politifact.com, Newsbusters.org, and FactCheck.org, there are local websites such as Teyit.org, Malumatfurus.org, and DogrulukPayi.com in Turkey. News verification on these websites is done manually. When investigating the source of the news, experts look at some criteria such as the date of the news, access to reliable sources, reading and questioning the accuracy of the news objectively, verifying it from official sources, and verifying it on other verification platforms. As might be expected, such verification or detection of fake news on the Internet with OSNs is rather slow, expensive, and subjective. It may contain the evaluator's biases and is difficult to apply to large volumes of data. In this context, when the fake news ecosystem is examined, usually encounters a structure consisting of the source, title, content of the news,

and the picture or video shared in the content of the news, and fake news detection approaches are generally considered into four categories.

2.1.4.1 Content-based methods

It is considered that fake news detection works have gained intensity, especially during the Covid-19 period. Firstly, in the content-based approach, the text to be analyzed focuses only on the content and does not need more auxiliary elements (Mathews & Preethi, 2022; Capuano et al, 2023). Content-based methods are also examined in three parts: knowledge-based, language/style-based, and stance-based (Qureshi et al., 2021).

- **Knowledge-based** Since fake news by its nature contains elements such as misinformation or information pollution, the main purpose is to check the accuracy of the claims in the content to detect this. It is carried out in two ways; manually and automatically. Fact-checking is usually done manually, based on knowledge, and by a team. Some systems automatically check for accuracy. Current fact-checking approaches can be categorized as expert-focused, crowdsourced, and computationally focused (Seddari et al., 2022c).
- **Expert-focused** fact-checking relies heavily on manpower and, accordingly, labor-time relationship to verify the source that is thought to be inaccurate or contains false information, in other words, to confirm its falsity. Examples of these are websites such as Teyit.org, Dogrulukpayi.com, and Malumatfurus.org from Turkey (Unver, 2020).
- **Crowdsourcing** fact-checking makes an evaluation based on the result that will emerge by presenting the accuracy of the news content to the information of the participants and thus confirms a generally accepted news based on the knowledge of the society (Allen et al., 2022).
- **Computational-focused** fact-checking often includes network-based semantic approaches. It deals with the criterion of semantic closeness between the concepts on the data set to be analyzed. The important thing in this analysis is to find the complexity of case-control by finding the shortest path between the concepts. Also, Fact checks using infographic aims to check whether the claims in the news content can be deduced from the existing facts in the infographic (Ciampaglia et al., 2015).

2.1.4.2 Language/Style-Based Methods

Language-based approaches may be perhaps the best approach to detecting fake news in OSNs, but they are difficult to succeed when the focus shifts. Given that bot accounts often use this kind of linguistic approach in OSNs, and from time-to-time official language usage may shift to another specific area, such methods are very difficult to detect evolved styles. However, malicious fake news publishers use certain writing styles to impress large communities, spread distorted misleading information, and build a specific audience. In the style-based approach, the news contents are analyzed, and they are tried to be determined by the similarities/differences in the writing style (Jiang & Wilson, 2018). However, detecting misleading statements and claiming in the news content constitutes an important step in the style/language-based approach. In addition to this method, it is one of the main elements of this approach in cases where the objectivity in the news content decreases and turns into a more rhetorical form (Mahyoob et al., 2020; Choudhary & Arora, 2021b)

2.1.4.3 Stance-Based Methods

The stance-based approach in OSNs is generally focused on the content of the news in question. The author uses rhetorical language to be misleading and direct on any news, and the subject is evaluated only from his critical point of view. The author may take a stand on an issue related to Covid-19. For example, he may take a cynical attitude towards the news that colloidal silver water has a healing effect on the corona. Or he can ironically launch the positive/negative aspects of corona vaccines from his perspective. Different arguments can be made against other points of view. We can identify this with the like button on Twitter posts (De Magistris et al., 2022).

2.1.4.4 Propagation/Network-Based Methods

Propagation/network-based fake news detection usually focuses on users' profiles, but they can show homogeneous and heterogeneous features. It is quite difficult to detect propagation/network-based fake news spread by generating an informational (flood) from different networks. To be detected, they must spread quite a bit and infect among OSNs. However, even if they cannot be detected for the first time inhomogeneous OSNs, especially on Twitter, it is easy to detect with the use of several different fake news detection models. An example of fake news that spreads based on propaganda inhomogeneous networks is that the posts on Twitter are spread by retweeting and this process is usually done by bot accounts (Shu et al., 2017; Zhou & Zafarani, 2019).

2.1.4.5 Source Based Methods

Detection of source-based fake news is one of the structures that can be detected quite easily today. Because they spread in OSNs by certain groups, mostly political and ideological ideas around a certain focus, and they usually aim to infect people close to their environment. A hybrid detection method is seen as a more effective coping method with the application of several fake news detection methods together (Mu & Aletras, 2020).

2.1.4.6 Hybrid Methods

Detecting fake news spread in OSNs with only one method is not considered possible because OSNs show both a homogeneous and heterogeneous structure. For example, while taking a knowledge-based or expert-based approach in any OSN that stance-based news is infecting, the news in question will be quite fast considering the interaction speed of OSNs. Instead, if a hybrid approach is adopted, firstly the analysis of suspected fake news with computational methods and then its analysis by experts in the field can prevent the speed of fake news spreading in OSNs from stopping or enable earlier action to be taken. In this context, we may encounter hybrid methods in different combinations (De Beer & Matthee, 2021).

2.1.5 Fake News Consequences in Online Social Networks

Even if all kinds of information shared in OSNs are assumed to be true by many, any information that has not been confirmed contains false information and causes disinformation, in addition to all kinds of information inserted in the filter balloons of OSNs, which has a consequence on users (Huang and Carley, 2020). Because, as stated by Simko et al. (2021), users who are both producers and consumers of the information shared in OSNs now exhibit a homogeneous structure. Within the framework of the information obtained from OSNs, users' view of the world is shaped differently as well as their daily life (Peng et al., 2018). Their decisions can change in many fields, including social (Bastick, 2021), economic (Petratos, 2021), and political (Rhodes, 2022). Sometimes, users who have to make critical decisions based on information, whether it is an investment decision or a choice decision, may make wrong decisions by being affected by unconfirmed false information, and as a result, they are adversely affected by the information they obtain from OSNs. The main implications of this fake news are as follows:

2.1.5.1 Health Impact

OSN users see no harm in sharing information that they perceive as simple and daily, which can often have critical and vital consequences, from eating and drinking to the pain reliever they will use in their social interaction. However, some false information or fake news obtained through OSNs potentially have negative effects on users. Dealing with this growing number of fake news is one of the biggest challenges for OSNs (Pulido et al., 2020). WHO, which could not cope with this situation, especially during the Covid-19 period, declared this situation as an infodemic as mentioned before and had to put information about fake news on its web page.

2.1.5.2 Financial Impact

With the Covid-19 epidemic, anxiety, and fear all over the world brought home closures. However, the social and business life, which had to continue, made it necessary to comply with the rules of the mask, distance, and cleaning. In almost every society, people/institutions trying to gain financial benefits by exploiting such basic rules tried to take advantage with their increasing advertisements over OSNs. At first, they created an environment of information pollution by misinforming people, and this situation was followed by non-stop propaganda processes. Thus, an incredible amount of fake news began to spread on OSNs. The cycle was so fast that after a while, everything started to be thought real. In this process, the increasing need for cleaning materials allowed these companies to generate more income than ever before. And again, in this process, flexible working hours and disruptions in the supply chain caused negative fluctuations in the market (Tan, 2021).

2.1.5.3 People Impact

Considering the need to obtain information from OSNs that interest and follow people during the Covid-19 period, they may be under the influence of abusive behaviours such as rumors and fallacy, hoaxes, or satirical. When these people are exposed to such activities through OSNs, they may be affected in a way they may not expect. They can have very serious problems in their real life. That's why people shouldn't rely on unconfirmed, invalid, and misleading information on OSNs. Or they should not make a prejudice based on their posts that contain misinformation and disinformation (Apuke & Omar, 2021).

2.2 Related Research

In this section, after determining the theoretical framework regarding the detection of fake news, a literature review was conducted. The ways and methods of how fake news spread in social networks can be detected within the framework of computer science and information systems are examined. In this context, ML, one of the most popular and most important developments of the last decade, and the AI methods that emerged with it will be examined in depth. In addition, cloud computing will be examined in this context in order to avoid and protect today's cyber threats.

Increasing its importance day by day, OSNs have caused the work and daily lives of people, who are social beings, to shift more towards social networks, especially with the Covid-19 pandemic. In this process, social and cultural life has started to take place in OSNs due to pandemic restrictions as well as obligations such as remote working and distance education. As stated in the previous sections, internet and social network usage, which has already increased, has entered a faster increasing trend. Inevitably, these platforms have turned into a medium where the economy, regional and global developments, and even cultural developments are followed, as well as the daily routine. Thus, although OSNs were not used that much before the pandemic, they also emerged as a source of news and information during and after the pandemic. As a result of this intensive use, the authenticity, confirmation or accuracy of news and information shared on OSNs has often been doubtful. In this context, whether the content shared on OSNs is correct or not has attracted the attention of both the academic community and users. In recent years, many studies have been carried out on the detection of fake news that tend to spread in OSNs. However, a comprehensive literature review is important in terms of identifying the gap in the field and conducting studies in this field. While giving an idea about the recent studies with the literature review, the shortcomings of the studies in question will be revealed and it will be a guide for researchers who want to work in this field. In this section, the place and importance of fake news in the literature and research on the subject will be discussed.

2.2.1 Systematic Literature Review

The systematic literature review (SLR) considered in this framework was carried out within the framework of the following principles to identify the most relevant studies in the field. A systematic online literature search was conducted, as shown in Figure 2.9, to identify publications on the detection of fake news by AI tools in OSNs. In this context, we included Web of Science and ScienceDirect, which are the most prestigious databases, as well as IEEE

Xplore (IEEE) and SpringerLink databases, which are more technical and information systems related. In order to reach articles that may be relevant to the search model, a search was made with titles, abstracts or keywords. These topics are “artificial intelligence” or “machine learning” or “deep learning” or “natural language processing” and “fake news” or “fake news detection” or “false news” or “propaganda” or “disinformation” or “misinformation” and “online social network” or “social network” or “Twitter” or “Facebook” and “cyber threat” or “cyber-attack”. This filtering consists of words and concepts that will be included and excluded from the review as seen in Table 2.1, and Table 2.2. In the research, the last five-year date range, that is, the publications between 2010 and 2019, were taken as a standard. As a result of the research, 351 articles were obtained. However, in order to reach more specific results regarding our research purpose and to eliminate the articles that are not/will not be in our area of interest, it has been reanalyzed according to some search concepts.

Table 2. 1

Inclusion criteria

-
- Empirical works
 - Artificial Intelligence (AI)
 - Machine learning (ML)
 - Deep Learning (DL)
 - Natural Language Processing (NLP)
 - Fake News
 - Fake News Detection
 - False News
 - Propaganda
 - Disinformation
 - Misinformation
 - Online Social Networks
 - Social media
 - Twitter
-

Table 2. 2*Exclusion criteria*

- Theoretical works
 - Untried or untested technologies
 - Book chapters
 - Filtering
 - Email and Junk Email
 - Bot and Bot Detection
 - Phishing and Click Bait
 - Emotional Features and Sentiment
Analysis
 - Credibility Analysis
 - E-commerce and Chatbot Analysis
-

Figure 2.9

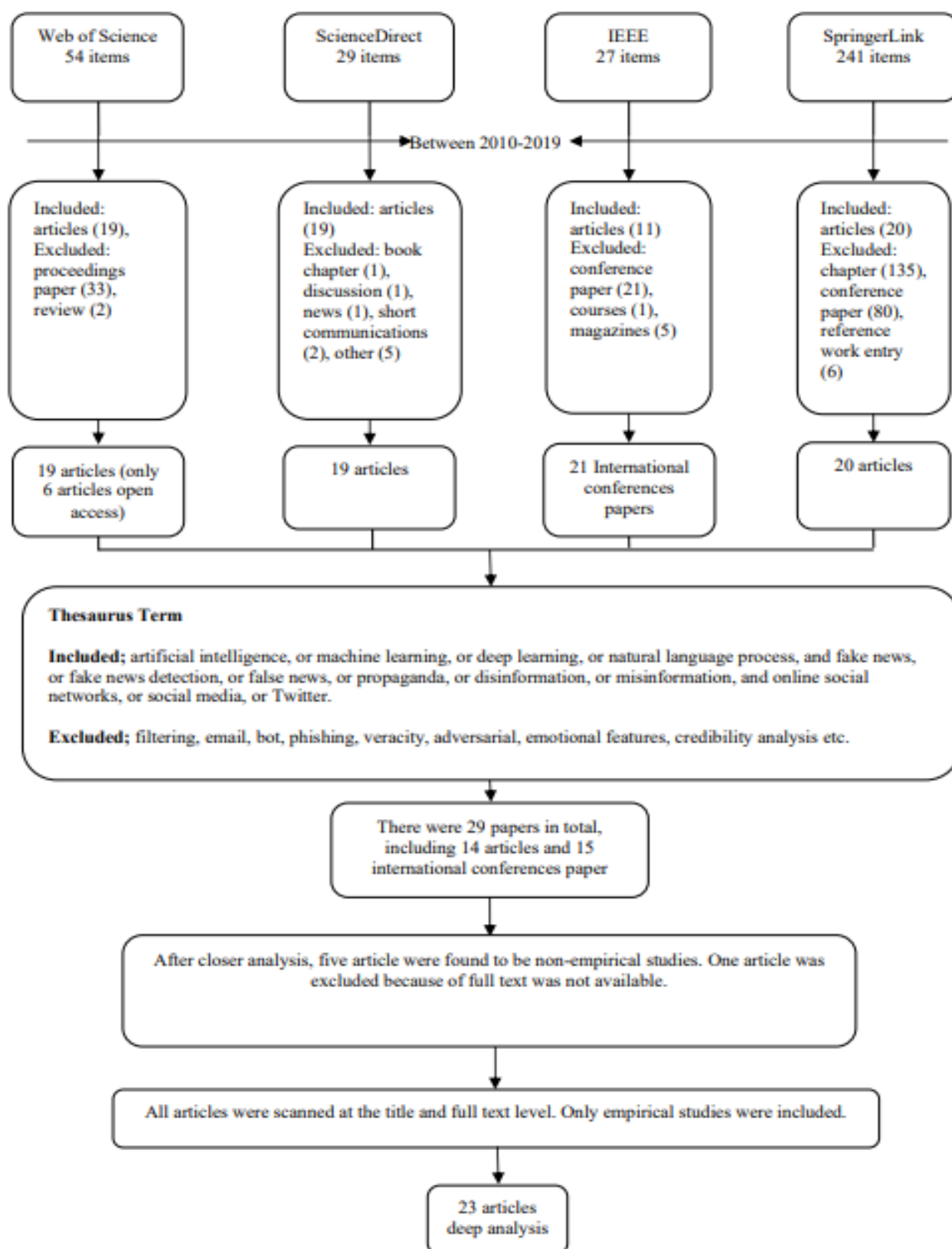
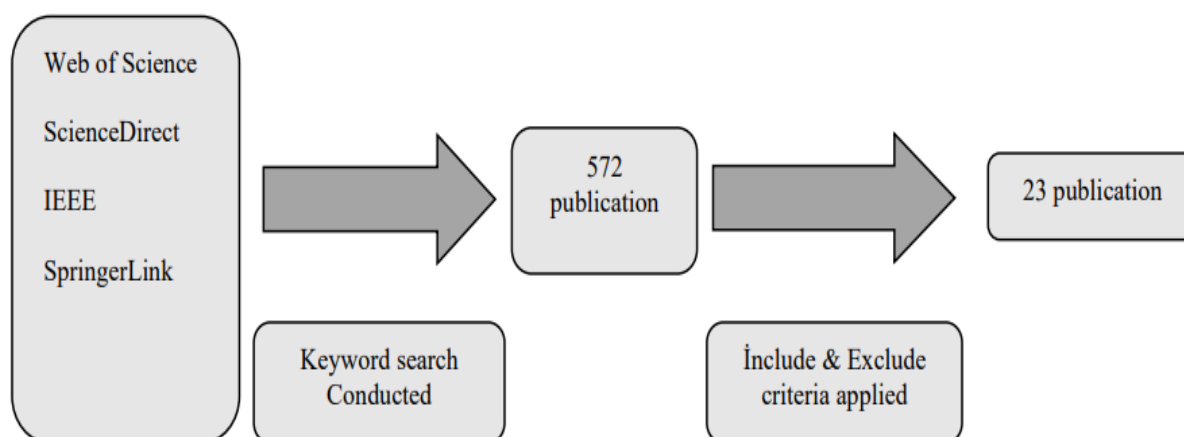
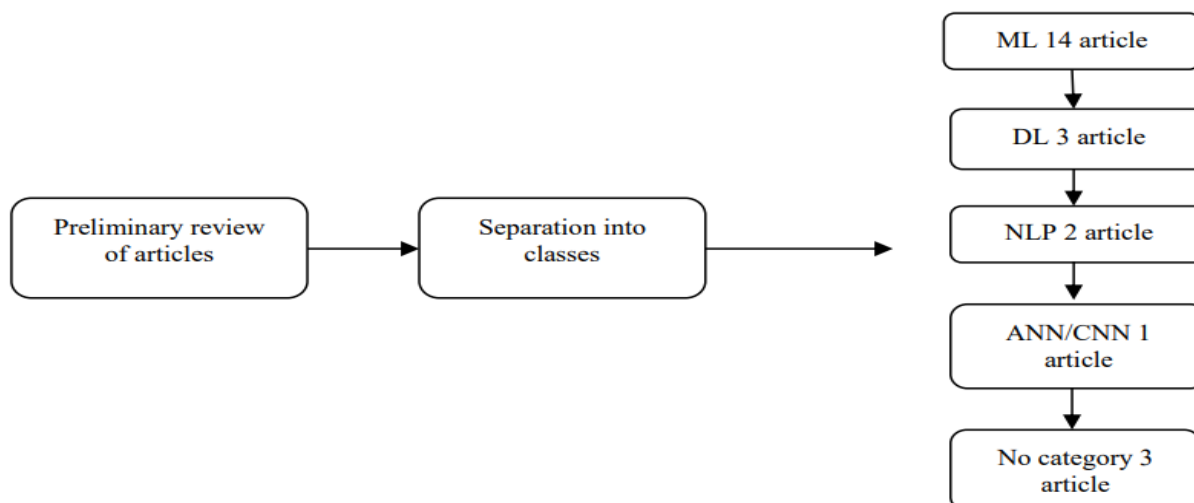
Systematic Literature Review Process of the Study

Figure 2.10*Data Analysis Process of the Study*

The data analysis process applied to the remaining 23 articles after this filtering is shown in Figure 2.10. As a result of the search criteria applied in the first stage of the review, a separate screening criterion was created for the articles obtained in each database too. These criteria include features such as that the articles obtained from these results do not consist of conferences, papers, discussions, courses, journals and pre-study samples. At this stage, only journal articles were considered. Finally, as a result of the examination, the remaining 23 articles were firstly divided into categories, read from beginning to end and analyzed in depth, as shown in Figure 2.11.

Figure 2.11*Research Approach for Data Analysis of the Study*

2.2.1.1 Artificial Intelligence Tools in Fake News

ML and DL methods are used in the detection of fake news from AI tools. As a result of the literature review, it is seen that especially ML methods are used more frequently in general. In this context, more ML will be emphasized. It is possible to define AI as a whole of software and hardware systems that have many capabilities such as human behavior, digital logic execution, motion, speech, and sound detection. In other words, AI makes computers think like humans (Ongsulee, 2017). For example, the winner of the quiz, IBM's AI Watson (Shah, 2011), and the GO intelligence, the Google AI that defeats the world chess champion can be shown. Nowadays, the rising power of personal computers and mobile devices enables the concept of AI to be applied in traditional educational environments such as schools and universities. ML is considered a kind of AI that can even expose results that are not programmed (Burkov, 2020a). In 1959, Arthur Samuel defined ML as the machine's ability to learn results that were not specifically programmed (Zhang et al., 2018). ML can also be expressed as solving the problem by using statistical methods on the problem-based data set (Kachalsky et al., 2017). For this, the machine needs to perform the learning process on the problem-based data set. In this context, learning consists of four categories supervised (Yuan & Yu, 2016), semi-supervised (Nijhawan et al., 2017), unsupervised (Dharani & Sivachitra, 2017), and reinforced (Mukhopadhyay et al., 2018). Deep learning is the most current approach used to develop AI for machines to perceive and understand the world. The aim of deep learning is to prepare the software for a computer model instead of constructing the software step by step (Qu et al., 2018). In DL, in the face of the scenarios encountered in solving the problem, the model in question can produce alternative solutions. DL is mainly used in the areas of face recognition, voice recognition, defense and security, and health (Akyön et al., 2018).

The use of AI tools in the detection and analysis of fake news and their successful results are instrumental in increasing the confidence in AI every day. In addition to teaching and learning content of ML from AI methods, it shows that there are more willing and interested users to deal with the fake news problem (Jeong et al., 2018a; Della Vedova et al., 2018a; Cardoso Durier da Silva et al., 2019a; Aborisade & Anwar, 2018a; Aldwairi & Alwahedi, 2018a; Aphiwongsophon & Chongstitvatana, 2018a; Gilda, 2017a; Kotteti et al., 2018a; Jain & Kasbe, 2018a; Granik & Mesyura, 2017a; Shabani and Sokhn, 2018a; Zhuk et al., 2018a; Helmstetter & Paulheim, 2018a) The biggest problem in the detection of fake news is to reach the content and dataset to be able to analyze. In this context, it has been observed that ML classifiers have high level of success in reaching the dataset and content in

detecting fake news (Helmstetter and Paulheim, 2018b). As a result of research on data collected from social networks such as Twitter, it was found that ML methods can detect fake news with an accuracy of 91% (Aborisade & Anwar, 2018b) and 99,9% (Aphiwongsophon & Chongstitvatana, 2018b). In addition, some social networks that use clickbait's and phishing methods to increase advertising revenue have achieved 94% accuracy (Aldwairi & Alwahedi, 2018b). The study (Gilda, 2017b) (11051 articles), which consisted of small data compiled from news articles, resulted in an accuracy of 77.2%. In another study (Kotteti et al., 2018b) if the data collected were lost or noisy data, data evaluation techniques were used to determine how the missing data affected the result. The focus is on data preprocessing. Accordingly, the success was determined to be 16%. Jain & Kasbe's (2018b) study on Facebook, a popular social network, examined 11000 articles as titles and content, although the rate of detecting fake news in headlines is around 80%, this rate is 92% in content analysis. Granik and Mesyura's (2017b) work focused on spam messages on Facebook and achieved an average success rate of 74%. The method used in (Shabani & Sokhn, 2018b), unlike all other studies, focused on fake news and satirical news and produced a hybrid model that predicts the human factor, the ML approach, and the classification confidence of algorithms and determines whether the task requires human input. Therefore, the results differ from other studies and the measurement of success is more specific. Zhuk et al. (2018b) focused on the classification of fake news by analyzing the delivery and distribution mechanisms. As a result, it is remarkable that it creates awareness in terms of adding human factor to the subject. Alom et al. (2018a) focused on Twitter features of Twitter users in order to improve existing spam detection mechanisms on twitter and achieved 91% successful results. As a result of the examination and evaluation conducted on 14 articles where ML was applied, it was observed that ML tools were extremely successful in detecting fake news.

In studies using DL methods (Granik & Mesyura, 2017c; Girgis, Amer & Gadallah, 2018a; Seo et al., 2018a) in Deep Neural Networks (DNN) (Granik & Mesyura, 2017d), Recurrent Neural Network (RNN), Long Short-Term Memories (LSTM), Gated Recurrent Unit (GRU) and Convolutional Neural Networks (CNN) In (Girgis, Amer & Gadallah, 2018b) and in (Seo et al., 2018b) Convolutional Neural Networks (CNN) algorithms are used. It was observed that the in terms of results were very close to ML algorithms.

In the study (Traylor et al., 2019), NLP method was used among AI methods and 69.4% success was obtained in terms of the result. Atodiresei et al. (2018) scored twitter and users on the twitter data using the Forensic Asset Recognition method from the AI tools.

Vijayan and Mohler (2018) focused on tweet data during the election period. In their studies, retweets and their distribution were examined.

When the articles which are not categorized by the authors (Gupta et al., 2018a; Figueira and Oliveira, 2017a; Vosoughi et al., 2018a) are examined; In (Gupta et al., 2018b), DL methodology is applied, (Figueira & Oliveira, 2017b) is based on more qualitative research where no quantitative values are used, and (Vosoughi et al., 2018b) is based on a general classification of twitter data and the spread of false news is measured.

The SLR showed that only literature research was conducted with the superficial data in the field of fake news (Cardoso Durier da Silva et al., 2019b) and that there was a large gap in this field caused us to do literature research on this subject. The use of AI tools to detect fake news is undoubtedly a very broad topic. However, when it is seen that AI technologies have started to separate their sub-branches as a state-of-the-art, it is considered that the selected topic is suitable for research. When it is seen that AI is subdivided into sub-branches such as ML, DL, NLP, and the specific studies of each field are examined, it is seen that AI is a product of advanced technology. It is known that each sub-branch uses different methodologies that serve different purposes in their own branches. However, investigating the detection of fake news that is the most common problem in social networks and reaching a common consensus makes the research valuable. The success levels of the researches problem (Jeong et al., 2018b; Della Vedova et al., 2018b; Cardoso Durier da Silva et al., 2019c; Aborisade & Anwar, 2018; Aldwairi & Alwahedi, 2018c; Aphiwongsophon & Chongstitvatana, 2018c; Gilda, 2017c; Kotteti et al., 2018c; Jain & Kasbe, 2018c; Granik & Mesyura, 2017e; Shabani & Sokhn, 2018c; Zhu et al., 2018; Helmstetter & Paulheim, 2018c) which applied to different algorithms of ML were higher than other studies. Although the content of each research is different, it is seen that the spread of fake news is examined in different ways and each one is evaluated correctly in its own field. However, it should be noted that DL and other methodologies (e.g., NLP, ANN/CNN) are still in their maturation phase. It is considered that the success rates are not very high because the methodology applied in deep learning techniques takes longer time in ML and does not have enough data sets to fully understand the learning techniques (Granik & Mesyura, 2017f; Girgis, Amer & Gadallah, 2018c; Seo et al., 2018c). Likewise, the low level of success in natural language processing and other methods stems from the lack of training of the machine (Gupta et al., 2018c; Figueira & Oliveira, 2017c; Vosoughi et al., 2018c).

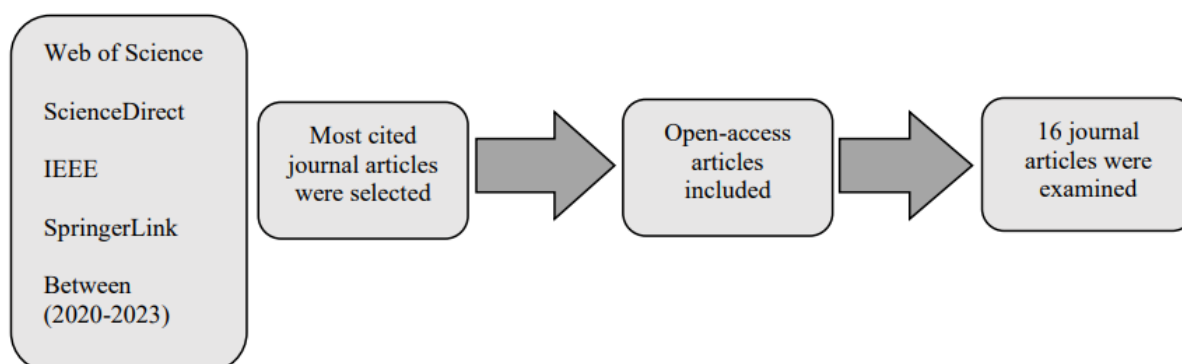
AI is suitable for use in social networks, and many applications that successfully implement AI tools to improve fake news detection were identified in the study. However, AI

should not be seen as a magic bullet in social networks. Each AI implementation is unique and therefore the benefits described may not apply in all contexts. In order to take advantage of the benefits, each application must be fully implemented to avoid drawbacks in user interaction or system success rates. It is considered that this study will fill a gap in this field and shed light on further research. This study is thought to be a guide for researchers and individuals interested in the detection of fake news.

In addition to the SLR detailed above, the Mini Literature Review (MLR) on the detection of fake news in OSNs was conducted between 2020-2023. 16 journal articles are included in the MLR, over the years. Starting from 2020, the most cited journal articles were examined. The MLR process is shown in Figure 2.12.

Figure 2.12

Mini Literature Review Process of the Study



In their study, Ozbay and Alatas (2020b) used datasets that they obtained from a website (Buzzfeed) that already exists in the literature and that usually publishes fake news such as hoaxes and satirical for various purposes. The datasets in question are those that have already been labeled as real and fake. Therefore, researchers do not have an original corpus. In addition, researchers have supervised artificial intelligence algorithms (BayesNet, JRip, OneR, Decision Stump, ZeroR, Stochastic Gradient Descent (SGD), CV Parameter Selection (CVPS), Randomizable Filtered Classifier (RFC), Logistic Model Tree (LMT), Locally Weighted Learning (LWL), Classification Via Clustering (CvC), Weighted Instances Handler Wrapper (WIHW), Ridor, Multi-Layer Perceptron (MLP), Ordinal Learning Model (OLM), Simple Cart, Attribute Selected Classifier (ASC), J48, They examined the performance of Sequential Minimal Optimization (SMO), Bagging, Decision Tree, IBk, and Kernel Logistic Regression (KLR) algorithms. The aim of this study was to measure the success of AI

algorithms with existing data rather than presenting a unique study to the literature. On the other hand, Umer et al. (2020) used the Fake News Challenge-1 (FNC-1) dataset, which is also available in the literature, in their study. Prominent in the research is stance-based fake news detection. In this framework, an evaluation was made with the titles agree, disagree, discuss, unrelated. The most prominent feature of the research is that it brought together highly correlated variables by reducing the parts of the data that should not be included in the analysis with Principal Component Analysis (PCA) and Chi-Square method, and created fewer artificial variable sets called principal components, which constitute the most variation in the data. After this stage, they analyzed the data with the CNN-LSTM model and achieved a success rate of 97.8%. However, with the CNN-LSTM model k-fold cross-validation with PCA, the success achieved at the end of the 10-fold training reached 99%. 10-fold training of the dataset after it is so small and optimized with PCA can indicate overtraining. Huang and Chen (2020b) in their work, tagged data obtained from data sharing platforms such as GitHub and Kaggle in their studies. In addition, an ensemble learning model that combines four different models for fake news detection, namely embedding LSTM, depth LSTM, LIWC CNN and N-gram CNN, is proposed. In addition, optimized weights of the ensemble learning model were determined using the Self-Adaptive Harmony Search (SAHS) algorithm to obtain higher accuracy in fake news detection. The most important feature of the study is that researchers focus on the problem of intractability between cross-domains. The model in question provided a 99.4% success rate in detecting fake news, while the success rate cross-domains was 72.3%. Kaliyar et al. (2020b) in their study, they used the data set obtained from Kaggle, one of the data sharing platforms, as in the previous study. They do not have an original corpus. For this reason, singular value decomposition (SVD) and Global Vector (GloVe) methods were used in data set training in order to maximize the results. They achieved a success of 99.74% with 10-fold training using deep CNN-LSTM with their model named FNDNet. However, the most important detail in this study is that 10-fold learning with a data set containing non-original and limited data points to overtraining.

Jiang et al. (2021) in their study, used tagged datasets published on the KDnuggets.com website together with the data they obtained from the PolitiFact.com website, which is one of the data sharing platforms and at the same time the accuracy of political news is checked. After the classical data preprocessing stages, ML algorithms and DL algorithms were applied in the model, and the accuracy of the system was carried out with the McNemar test. In this study, the aim is academically focused on testing and evaluation of algorithms and datasets, rather than creating a real-time detection system. Li et al. (2021b),

propose the model they created with the data collected from two OSNs, such as Twitter and Weibo, which they obtained from another study (Boidu et al. 2016). In this dataset, the data is pre-labeled. The proposed system works with the Autoencoder method and is generally used for anomaly detection. In the study, in which the results of the UFNDA systems, mostly on the data sets, were evaluated, the success level was around 90%. Verma et al. (2021b) in their research, they propose a two-stage benchmarking model, WELFake, based on linguistic features-based word embedding (WE) for fake news detection using machine learning classification. However, the striking feature in this study is the use of data sets obtained from ready-made data sharing sites (Kaggle, McIntire, Reuters, and BuzzFeed Political), as in other studies. Due to the fact that they did not create an original data set, it could not go beyond a study in which the measurements of ML or AI algorithms were presented, as in other studies. In the language feature set based on word embedding made with the data set created in this framework, a success rate of approximately 96.73% was achieved with four different ML algorithms. In the research of Choudhary and Arora (2021c), In their study, used two different data sets in their proposed fake news detection system, as in previous studies. These datasets are published on GitHub and BuzzFeed. In the study conducted with limited and small amount of data, Matlab and Linguistic Deep Learning Model ready tools were used in Google Colab environment. In fact, by training such limited data in 50 and 100 epochs, it is inevitable that it enters the spiral of overtraining. For this reason, it is considered that the results are not linear and the study in question cannot go beyond an experimental attempt. In this context, the average results were between 72% and 80.22% in 50 epochs of education, and between 77.67% and 84.52% in 100 epochs of education.

On the other hand, when the studies conducted with the detection of fake news in 2022 are examined, Liao et al. (2021b), it is seen that they propose an innovative fake news detection system. Accordingly, fake news detection was examined in two categories. Firstly, the news headlines are examined with a higher percentage and secondly, the intention of the authors who publish this news to publish fake news is discussed. The researchers designed the system they created in their research called fake news detection multitasking learning (FDML) in two main frameworks as a representative learning part and a multitasking learning part. In this study, LIAR ready data set was used. The important feature of the data set is that it consists of short news. With this feature, it resembles Twitter data. In the study, a multi-source, multi-class fake news detection model that provides additional information from other sources along with hybrid CNN and LSTM attention models, the results were around 70%. Seddari et al. (2022d) used a hybrid method combining linguistic and knowledge-based

approaches in their research. In the linguistic approach, elements such as the title of the news, the number of words, and ease of reading were examined, while in the information-based approach, the reputation of the published site, how many sources were quoted or verified, and finally the opinion of the relevant confirmation bodies. The research is highly sophisticated and remarkable. In this context, IBM Watson Studio was used to determine the best ML algorithm during the training phase of the system. As a result, Random Forest (RF), Logistic Regression (LR), Additional Trees Discriminant (ATD), and eXtreme Gradient Boosting (XGBoost) algorithms were included in the study. Despite such a sophisticated study, no original corpus was created and the BuzzFeed Political News dataset was used. As a result, 89.4% success rate was achieved in the linguistic approach, while this rate was around 81.2% in the knowledge-based approach. However, the result increased up to 94.40% in the hybrid method. Wei et al. (2022) uses an innovative approach called Modality and Event Enemy Networks (MEAN) for fake news detection. This approach consists of two parts, a multimode generator and a pair splitter. The results obtained by the researchers who proposed a system using DL algorithms on the data set obtained from Twitter and Weibo, two of the OSNs, were around 90% in the first approach and 78% in the second approach, respectively. On the other hand, in the study of Shishah (2022), a system created by using the BERT algorithm on four different fake news datasets created in Arabic is suggested. In order to avoid over-learning in the transformer phase of the BERT algorithm, ADAM optimization and GeLu activation from DNN implementations are used. Four different algorithms applied to four different data sets have different scores ranging from 51% to 96%.

2.2.2 The Gap in the Literature

Especially during the Covid-19 pandemic, people, who are social beings, have to leave their work and daily life, and use online social networks more and more, a critical situation such as education plays an essential role in accessing information, socialization, entertainment, etc. Such needs have increased the importance of online social networks. In this context, much information/news, etc. shared in OSNs. Whether the content shared in these OSNs is correct or not attracts the attention of both the academic community and the users. In this section, the place of fake news in the literature, its importance, and research on the subject will be given.

This chapter aims to explore advances in the use of AI tools in fake news detection. In this section, a systematic review of recent publications on the detection of fake news with AI tools has been made. Thus, the difficulties in detecting fake news and the gap in the literature

were determined and it was aimed to be a guide for future studies. The successful results in the use of AI tools in the detection and analysis of fake news are effective in increasing the trust in AI, which is developing and getting stronger day by day. However, it is seen that ML, one of the AI tools, is used more to deal with the fake news problem. One of the most important problems in detecting fake news is accessing a trained dataset and content to analyse. In this context, it has been evaluated that ML algorithms are more successful in reaching and analysing the content and data set. As a result of the research made with the data obtained from Twitter, a microblogging network, it was determined that ML algorithms were successful between 91% (Aborisade & Anwar, 2018) and 99% (Aphiwongsophon & Chongstitvatana, 2018d). Detection of clickbait and phishing methods, one of the types of fake news, resulted in an accuracy of 99.4% (Aldwairi & Alwahedi, 2018d). In another study (Gilda, 2017d) conducted on a data set compiled from news sites, an accuracy of 77.2% was obtained. In another study (Kotteti et al., 2018d), data evaluation techniques were used to determine how missing data affected the outcome if the data collected was missing or noisy data, the focus of this study being data pre-processing. Accordingly, the success of the study was 16%. Jain & Kasbe's (2018d) research on Facebook, a popular OSN, analyzed articles by title and content. Accordingly, although the result is around 80% when only news headlines are analyzed, this rate has reached 92% in content analysis. The focus of Granik and Mesyura's (2017g) work was spam messages on Facebook, which is considered one of the types of fake news. This study achieved a success rate of 74%. The method used by Shabani and Sokhn, (2018d) unlike all other studies, focused on fake news and satirical news and produced a hybrid model that estimates the human factor, ML approach and classification confidence of algorithms and determines whether the task requires human input. Therefore, the results differ from other studies and the measurement of success is more specific. Alom et al. (2018b) to improve the spam detection mechanisms available on Twitter, it focused on the user characteristics of Twitter users and achieved 91% successful results. As a result of the examination and evaluation studies in which ML was applied, it was observed that ML tools were extremely successful in detecting fake news.

Considering these studies, the biggest gap in the literature is the lack of a fake news detection system that can work in real time and online while avoiding cyber threats, and also has a unique structure with its own corpus.

CHAPTER 3

METHODOLOGY

This section describes the Cross Industry Standard Process Model for Data Mining (CRISP-DM) methodology used to model the FANDC system for fake news detection in OSNs. Categorically, in this section, in-depth information is given about the principles on which the system was established, and the approaches and hypotheses adopted at these stages. In this section, data mining and text mining methods are discussed and explanations about the CRISP-DM methodology applied in fake news detection are presented. It also explains why fake news detection is based on cloud computing within the framework of the CRISP-DM methodology.

3.1 CRISP-DM Methodologies

CRISP-DM is a standardized methodology used to describe how business problems are solved with data-based solutions and to increase the efficiency of business applications. Because CRISP-DM is a high-level methodology, the steps outlined in the model can be implemented in many ways, sequences, and technologies to meet business needs. In this thesis, the problem of detecting fake news in OSNs is handled as a business problem, and the sub-diffractions of each process are adapted and applied for the solution of the problem (Huber et al., 2019).

CRISP-DM consists of four levels:

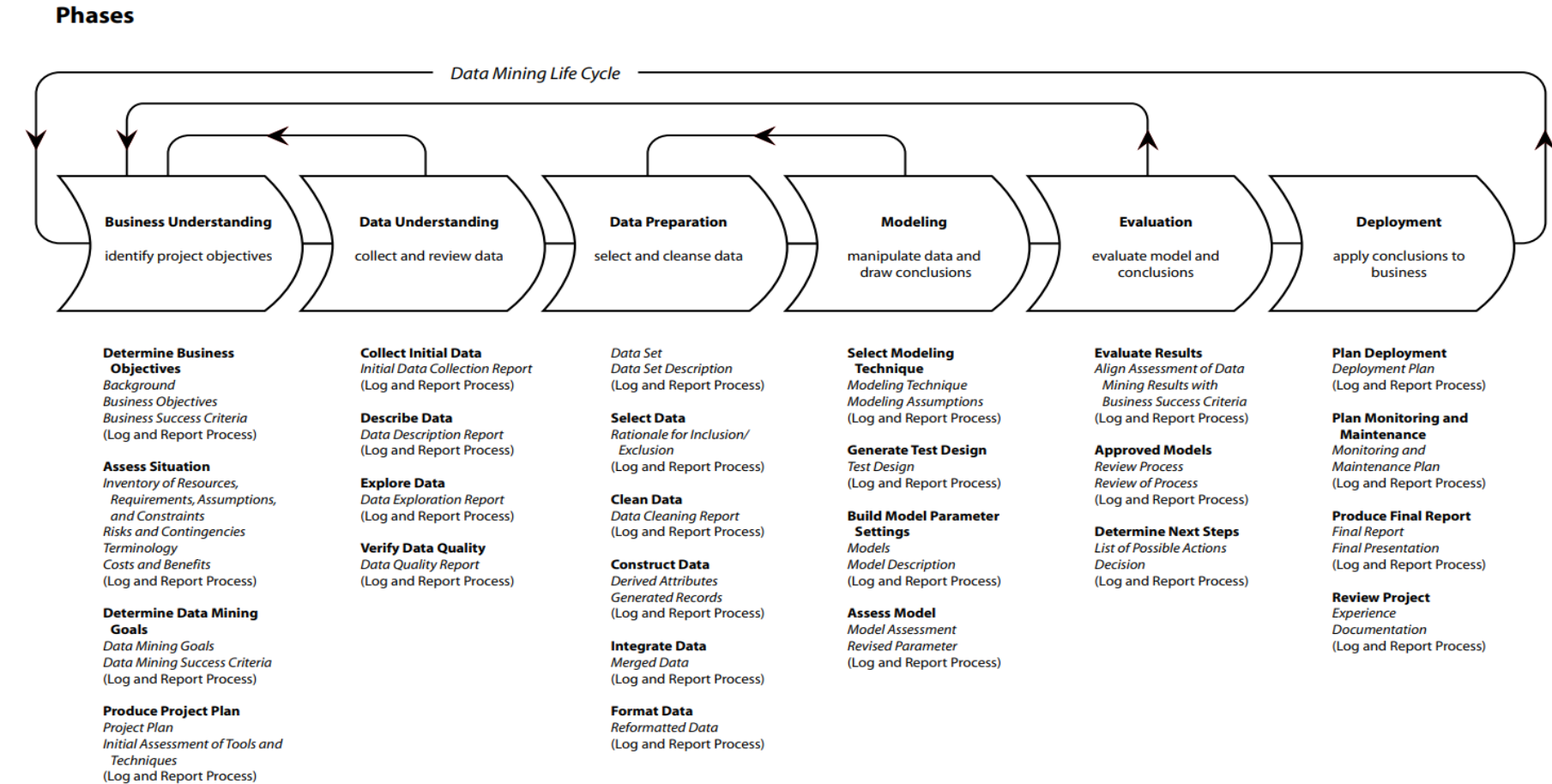
- **Phases**, phases form the top level of the model and are the main tasks of data mining processes.
- **General Tasks**, general tasks determine the tasks that need to be fulfilled for the phase to take place, regardless of the special circumstances, regardless of the situation encountered.
- **Specialized Missions**, special tasks take different situations into account. For example, if there is a general task called cleaning the data regardless of the nature of the data, there may be two special tasks under this task: cleaning the categorical data and cleaning the numeric data.
- **Process Examples**, the fourth and lowest stage of process examples is the retention of what has been accomplished in relation to what will be

accomplished rather than what will be accomplished. One could think of it as a project diary that is one-to-one mapped to the CRISP-DM model.

The CRISP-DM methodology shown in Figure 3.1 (Wirth & Hipp, 2000) was chosen to deal with the fake news detection problem in OSNs. Because the fake news detection to be used in the FANDC system includes text mining, natural language processing, AI and today's social networks carried out on the basis of data mining. The problem in question was seen as a business problem within the framework of this methodology and the sub-diffractions of each stage were applied as stated below (Schröder et al., 2021). The phases of the CRISP-DM process model are business understanding, data understanding, data preparation, modelling, testing, and implementation.

Figure 3.1

CRISP-DM Methodology Diagram (Schröer et al., 2021)



3.1.1 Business Understanding

At the stage of understanding the work, which is the first stage, it is tried to be clarified what kind of contributions the data mining study will make to the work being tried to be done. In this thesis, it has been evaluated that the data collection and pre-processing stages of data mining processes will provide significant contributions in terms of obtaining a unique corpus and increasing the accuracy and precision of the tests and analyzes to be made afterwards. Thus, it was ensured that the project objectives were usefully clarified and that all activities in the project were goal-oriented. At this stage, the most important problem was identified as fake news detection in OSNs. that is, the problem is reduced to a data mining problem. The stage of understanding the work as sub-diffraction consists of the following tasks (Saltz, 2021);

- At the stage of determining the business objectives, it is tried to determine what the researcher aims at. The aim of the researcher in this thesis; The fake news detection problem in OSNs is the task of collecting and analyzing data to detect fake news spreading on social networks. For example, in order to detect fake news that tends to spread on Twitter, it is to examine the content of users' posts and to ensure that any user has an idea about the post in case of doubt.
- While assessing the current situation, the resources and risks in the project are discussed. At this stage, questions such as what data we have, what software we can use, what our hardware is, what problems we might encounter during the project were discussed. In this context, the stream API was first requested to collect data from Twitter. Thus, the first step was taken to reach the data. Since it is thought that the data to be obtained from here will be large, the storage capacity of the local computers will be insufficient, so a local server has been provided where the data will be stored. MongoDB database management system, which is an open-source software, was used to save the data in a database on a regular basis. It was carried out using .NET in the MS Visual Studio software development environment, which can also be used as open source to pull data from Twitter with the streaming API. This stage is crucial to make the right decisions that will be carefully considered.
- The stage of determining data mining goals is to express the problem solution with data mining terminology. At this stage, it has been determined whether it is possible to detect fake news in OSNs, whether users have information about

the content with a simple query, and whether all these processes can be continued uninterruptedly.

- During the creation of the project plan, the dates and resources for all the steps in the FANDC project were determined.

3.1.2 Data Understanding

At the stage of understanding the data, the quality, number and accessibility of the data to be used throughout the thesis were evaluated. Understanding the data consists of the following stages (Kristoffersen et al., 2019):

- At the stage of loading/collecting the data, the data is drawn from the relevant sources and loaded into the software to be analyzed. If data from different sources needs to be used together, problems with integration need to be resolved. Since the data to be collected from Twitter has a homogeneous structure, no problems were foreseen in this regard. The collected data was transferred to MongoDB, an open-source database application.
- At the stage of describing the data, information such as how many records are available and how many fields (features) the records consist of are collected. The data collected at this stage consisted of approximately 99 million tweets.
- At the stage of data exploration, what can be said about the data is determined with simple statistical or visualization methods. For example, determinations are made about the distribution of the available data, their mean values, or the correlation between the data, if any. This section will be explained in detail in the data analysis section.
- During the Verification of Data Quality phase, it is determined whether the available data is sufficient, whether it covers all different situations, and the amount of missing and incorrect data. It has been evaluated that the data collected at this stage is sufficient to create a corpus and covers the fake news detection problem to be examined in seven sub-categories. Regarding the missing and incorrect data, it was decided to carry out the data pre-processing step carefully.

3.1.3 Data Preparation

At this stage, the collected data is made ready for model building. Data preparation consists of the following stages (Purbasari et al., 2021):

- It was determined which of the data obtained during the data selection stage would be used in the modeling. At this stage, tweets containing emojis and tweets containing excessive data, pictures and videos, which are thought to affect the model negatively, were not included in the model.
- During the cleaning phase of the data, the data that could prevent the model formation or corrupt the model were removed. At this stage, tweets such as “OMG”, “R U Ready”, “ASAP” and similar retweets, as well as tweets containing only emojis or sent without comment, have been cleaned as they may break the model.
- During the data construction phase, new data fields are created using existing data. However, since more data cleaning was done at this stage and our data set was big enough, no new data was produced.
- In the data integration phase, data from different sources are combined. However, since the tweets obtained at this stage were obtained only from Twitter, as stated above, integration was not required.
- During the formatting of the data, the data is brought into the format needed for modelling. At this stage, only the text segments were formatted with data cleaning.

3.1.4 Modelling

At this stage, different modelling techniques are applied by selecting the most suitable one for the data at hand and the job to be done. Modelling consists of the following stages (Martínez-Plumed et al., 2019):

- At the stage of choosing the modelling technique, the technique to be used during modelling is determined. At this stage, the BERT algorithm (Devlin et al., 2018a), which is a state-of-the-art technology, was used and the system was modelled on it, as a result of a SLR for fake news detection in OSNs, since the performance rates of classical ML algorithms were low, and the focus was on detecting fake news with higher accuracy than the performance of the algorithms.
- At the stage of determining the test, after the model is created, it is determined by which test the quality of the model will be verified. For example, if classification is to be made, some of the data is used for the development of the model and the rest for the test of the model, and it is determined in what

percentage of the classifications the model created during the test made the wrong decision. In this project, 80% training and 20% test data are allocated. Various evaluation criteria were used to evaluate the performance of the BERT algorithm we used for detecting fake news in OSNs. In this section, we reviewed these metrics. Below are formulas for assessment criteria for other assessment criteria such as accuracy, precision, recall, and F1 scores (Burkov, 2020b).

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recal} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F1 Score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

Where TP: True Positive, TN: True Negative, FP: False Positive, and FN: False Negative. These are all defined in the confusion matrix.

Looking at our dataset, where fake news datasets are often skewed, high precision can easily be achieved by making fewer positive predictions. Therefore, recall is used to measure the sensitivity or proportion of annotated fake news articles that are predicted to be fake news. F1 is used to combine precision and recall, which can provide an overall predictive performance for fake news detection. The higher the value for Precision, Recall, F1 and Accuracy, the better your performance will be. The Receiver Operating Characteristic (ROC) curve is a graph showing the performance of a two-parameter classification model against TPR versus FPR at all classification thresholds. TPR and FPR are provided as follows. The area

under the ROC Curve (AUC) measures the entire two-dimensional area under the entire ROC curve (Burkov, 2020c).

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{TPR} = \text{Sensitivity} = \text{Recall}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}$$

- During the creation of the model, the parameters of the model were determined and the system was fully run to create the FANDC model.
- During the evaluation of the model, the success of the model is technically evaluated according to the criteria in the determination of the test. The results of the system tested at this stage are presented in Figure 3.4.

3.1.5 Evaluation

In the previous stage, the results were evaluated in terms of data mining. At this stage, the results will be evaluated in terms of the targets set at the beginning of the FANDC project. Evaluation consists of the following stages:

- In the evaluation of the results, the researcher examined and evaluated the results. It has been determined whether the results meet the targets set at the beginning of the FANDC project. In this framework, it was decided to move the FANDC system running on a local system to the MS Azure Cloud computing system, considering that it was sufficient. The most important decision stage of this stage consists of performing the experiment by applying the model in real conditions, when the resources are sufficient.
- The model is validated for its results at this stage. During the review of the process, the whole process is evaluated once more as a quality control process. Answers are sought for questions such as did we use the right data or did, we give too much importance to some data. At this stage, the results are satisfactory as the test results and data preprocessing stage are meticulously studied. However, due to the nature of the CRISP-DM methodology, it has been revised.

- At the stage of deciding the next step, it is determined whether to move to the deployment phase or whether to repeat the process again. At this stage, since it is considered that the system avoids cyber-attacks and is relatively protected, it has been concluded that it would be appropriate to have a distributed and container form on cloud computing.

3.1.6 Deployment

At this stage, the model is put into use in real life. For this reason, the system, which was tested and evaluated on a local server, was migrated to MS Azure Cloud computing, and tested again and it was decided to go live after successful results were obtained.

- During the “Planning” phase of the distribution, planning was made so that the Model or results could be used as in the testing processes and without any degradation. At this stage, it is discussed whether the MongoDB database can work in harmony with the MS Azure cloud computing system.
- During the “Planning of Observation and Maintenance” continuous monitoring for the healthy operation of the system and maintenance processes are planned to avoid cyber-attacks.
- The “Preparation of The Final Report” is the creation of this thesis within the framework of the problem we are dealing with.
- In the “Project Evaluation Phase” the findings and discussion section of the Thesis will be guiding. In addition, evaluations by the researcher will be included in the conclusion and recommendations section.

3.2 Data Collection

It was considered that it would be more appropriate to collect data from Twitter, which is one of the OSNs, which is used extensively during the Covid-19 pandemic period, instead of making use of existing corpus to detect fake news correctly in OSNs. To collect the said data, the streaming API was requested from Twitter (Twitter, 2019). However, since the streaming API allocated by Twitter is in a structure that allows the collection of data for the last seven days, because of the connection problems encountered in the internet infrastructure and some errors of the local server and open-source applications where the system was created, data could not be collected continuously and stably. Meanwhile, tweets collected and published by Chen et al. (2020) on GitHub during the Covid-19 period were requested and downloaded within the framework of academic ethical rules.

January 1, 2020 is taken as the beginning of the pandemic. In this context, approximately 99 million tweets were stored until April 1, 2020. Considering the size of the data collected, it is working in a big data environment. It is important to create a corpus that will be used specifically for the FANDC system. Because when the studies on the solution of the fake news detection problem are examined in the literature, there are generally studies that have a certain corpus such as Kaggle, Hugging Face, Wikipedia or that have been previously studied on other sharing sites and focus on the testing and evaluation of algorithms instead of fake news detection.

In this context, the tweets in question on MongoDB, an open-source database management system, were transferred with .NET on the Visual Studio 2019 software development platform. The system consists of 20GB Ram, 500GB SSD, 8 Core CPU as hardware.

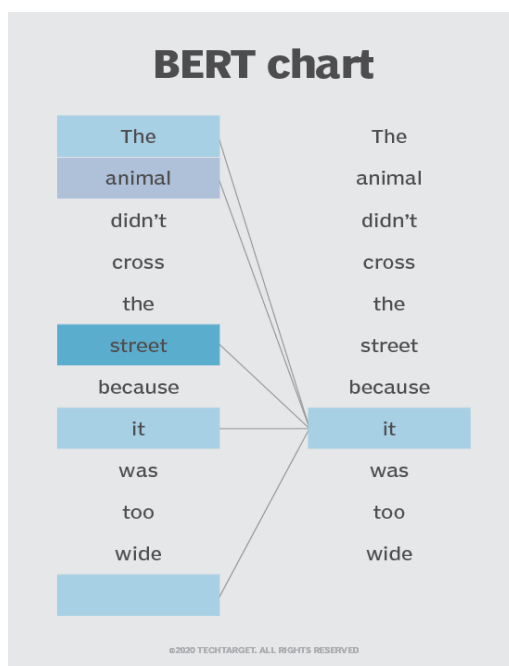
3.3 Algorithm Selection

In data mining or ML, an algorithm is expressed as a step-by-step design of a solution path to solve a specific problem or achieve a specific goal. In order to model the database created within the scope of the thesis study, it is necessary to choose the appropriate algorithm for the solution of the problem. ML algorithms use parameters that represent the large set, based on training data. As the training data expands to solve the problem more realistically, the algorithm calculates more accurate results. For this reason, 80% of the data was used as training data and 20% as test data. In the light of these data, it was decided to use the BERT algorithm, one of Google's NLP algorithms based on neural networks and DL, to solve the fake news detection problem in OSNs, which is the subject of the thesis.

BERT is an open-source ML algorithm for NLP. BERT, which stands for Bidirectional Encoder Representations from Transformers, is based on Transformers, a DL model in which the relationship of each word to another and accordingly the weights between them are calculated dynamically. The most important reason for choosing this algorithm is to apply the bidirectional training of Transformer, a popular attention model, to language modelling. This is in contrast to previous efforts that looked at a text string combining left-to-right or left-to-right and right-to-left training. BERT has shown that a bidirectionally trained language model can have a deeper language context and flow than unidirectional language models, achieved by a new technique called Masked LM (MLM) that allows bidirectional training, which was previously impossible (Rogers et al., 2021; Wu et al., 2020).

Figure 3.2

A Sample of BERT for MLM (Lutkevich, 2020)



Using this dual capability, BERT is pre-trained for two different but related NLP tasks: Masked Language Modeling (MLM) and Next Sentence Prediction (NSP). The MLM is to mask a word in a sentence, allowing it to predict which word is masked based on the context of the word. The purpose of the NSP training is to enable BERT to predict whether two sentences in the text have a logical, sequential connection or whether their relationship is random. During training, 50% of the entries are a pair where the second sentence is the next sentence in the original document, while in the other 50% a sentence is randomly selected from the corpus as the second sentence. As seen in Figure 3.2 (Lutkevich, 2020), BERT determined which word "it" refers to by bi-directional analysis of all words in the sentence. Thus, the word with the highest score calculated is correctly associated (Devlin et al., 2018b).

As a result, the BERT algorithm, which has proven itself in the field of natural language processing and is a state-of-the-art technology, has been chosen to cope with the fake news detection problem in OSNs thanks to this bi-directional capability.

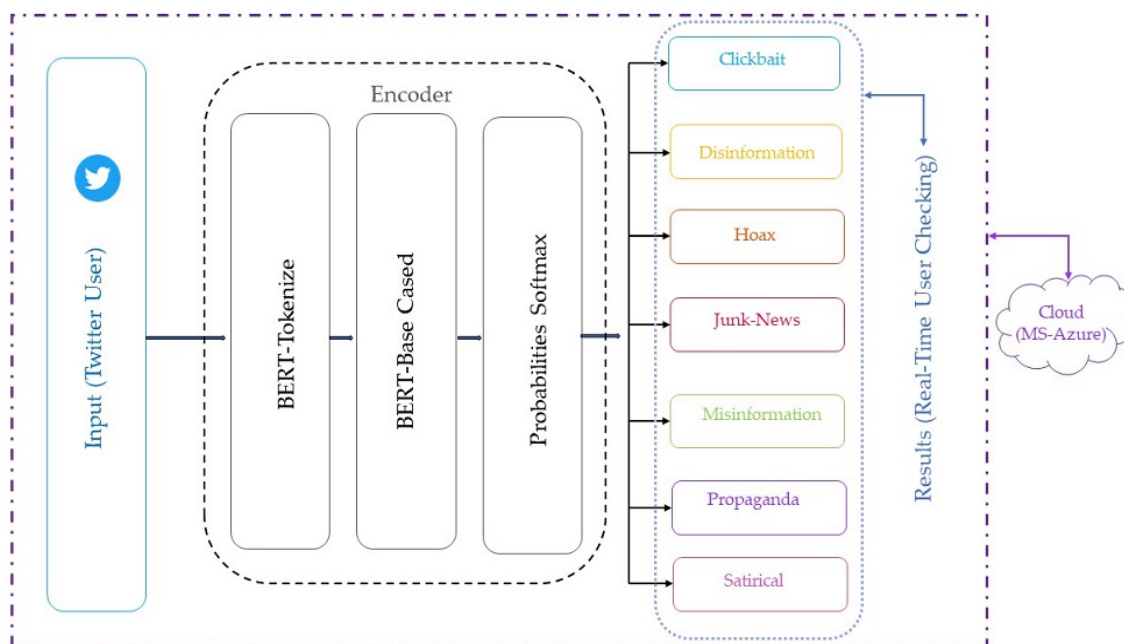
3.4 Developed Fake News Detection System

The name *FANDC* was given to the system created to solve the problem of fake news, which increased especially during the Covid-19 pandemic period in OSNs. During the Covid-

19 pandemic, also called Infodemic, the primary goal was to collect the Covid-19 related tweets on Twitter from January 1 to April 1, 2020, as the data we would collect needs to be up to date. The first issue encountered was that the Twitter streaming API only allowed data from the last 7 days to be collected when collecting data. During the data collection process, it was determined that tweets about covid19 were published on GitHub within the framework of an ongoing study on the subject. Because the *FANDC* system streaming API was in a structure that allowed data for the last 7 days and required a continuous monitoring process. When it is evaluated that there will be problems such as the disconnection of the internet, some update problems occurring in the Twitter stream, or insufficient storage space except for all these reasons, instead of receiving the data via Twitter, we downloaded that already sent 99 million tweets data in 10 different languages all over the world from GitHub, within the framework of ethical rules. Then, since the data preprocessing phase would be performed on the data, all data was transferred to the SQL server and made reportable. In the data preprocessing phase, the punctuation marks, stop-words, deleting numbers, tokenization, stemming, lemmatization, etc. were applied first to bring the data to the desired criteria (Stieglitz et al., 2018a). At this stage, we have divided fake news into seven sub-categories so that OSN users can easily understand such news that spread and cause information corruption. These are generally the categories that have been studied in the literature. *FANDC* fake news detection system is divided into seven subcategories as click-bait, disinformation, hoax, junk news, misinformation, propaganda, and satire. In this framework, the synonyms of the words to be categorized from (Wordhippo, 2022; Kadhim, 2018; Burkov, 2020d; Stieglitz et al., 2018b) were determined. The data found in the data set were trained by labeling them based on these synonyms. While these studies are continuing, the domain name of the web page has been taken Teyitet.net, so that OSN users can make inquiries online. Thus, OSN users were able to query suspicious news online and in real time on social networks, and to reach definitive conclusions about the news as a result of an inquiry as shown in Figures 5.1 and 5.7 below. The general design of the *FANDC* system is shown in Figure 4.10. In the *FANDC* fake news detection system, instead of evaluating the words in the queries one by one, the BERT algorithm is used to evaluate the previous and next words or together with similar and synonymous words. The primary goal here is to better understand complex user needs. BERT better understands how conjunctions and prepositions used in queries add meaning to a sentence. For this reason, we trained approximately two and a half million tweet data, which became ready for training after the data preprocessing stage, with the BERT algorithm. The system is trained as 80/20 training and test data.

Figure 3.3

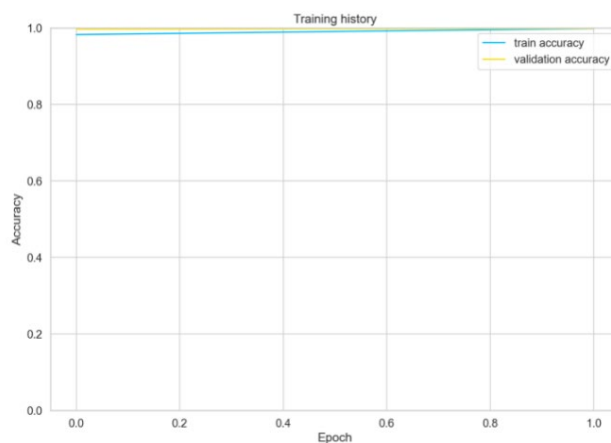
The general design of the FANDC model



The accuracy of the data set trained in two epochs with the BERT algorithm is 100% as seen in Figure 3.3. It has been moved to the MS Azure cloud system to protect against cyber-attacks (Goksu et al., 2020), which may be caused by the system's online fake news detection, such as service interruption or clickbait, and to ensure data security Teyitet Web page on Cloud (2020). The results obtained as a result of the inquiries made on Twitter are presented in the IV section of the thesis.

Figure 3.4

FANDC System Post-training Accuracy



The success rate of the classification phase after the training is shown in Figure 3.4. The confusion matrix in Figure 3.5 and the success rate of the classification phase after the training are shown in Table 3.1. Here, after the training, clickbait, disinformation, hoax, junk news, misinformation, propaganda, and satire were trained with full accuracy, whereas propaganda was trained with 99% accuracy and misinformation with 94% accuracy. Therefore, it is seen that the system successfully carries out the education process.

Figure 3.5

FANDC System Confusion Matrix of Post-training

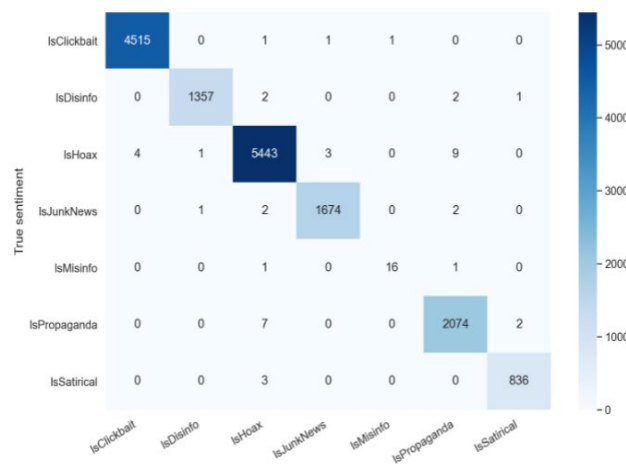


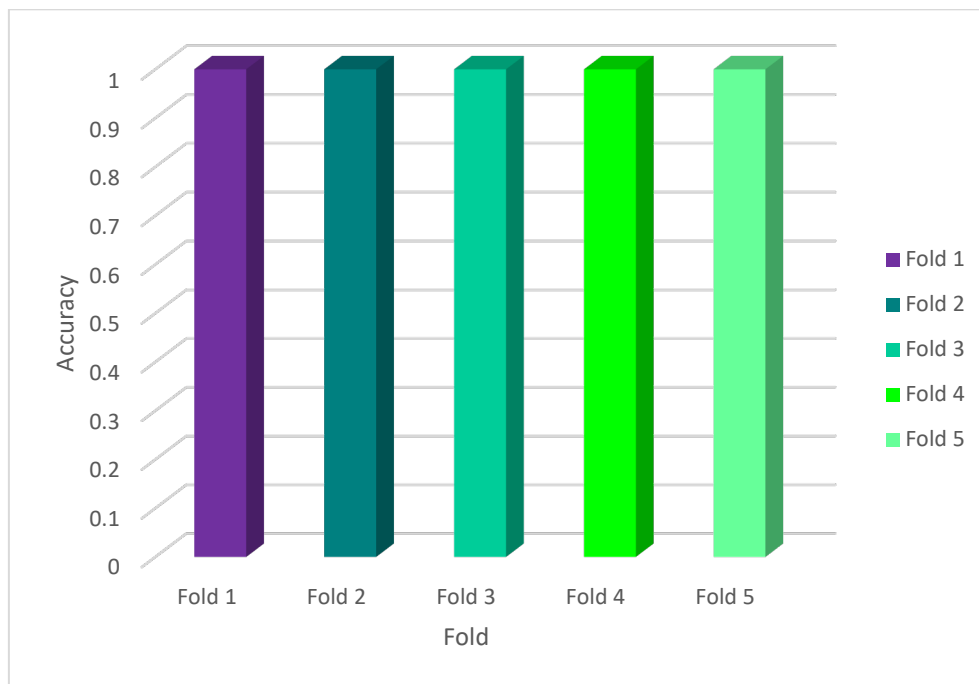
Table 3. 1

The success rate of the post-training classification stage of the FANDC System

Category	Precision	Recall	F1-Score	Support
IsClickbait	1.00	1.00	1.00	4518
IsDisinfo	1.00	1.00	1.00	1362
IsHoax	1.00	1.00	1.00	5460
IsJunkNews	1.00	1.00	1.00	1679
IsMisinfo	0.94	0.89	0.91	18
IsPropaganda	0.99	1.00	0.99	2083
IsSatirical	1.00	1.00	1.00	839
Accuracy			1.00	15959
Macro avg	0.99	0.98	0.99	15959
Weighted avg	1.00	1.00	1.00	15959

Figure 3.6

FANDC System K=5 Fold Cross-Validation Accuracy



Additionally, the K-Fold Cross-Validation method was used to evaluate the performance of the model and measure its generalization ability, as seen in Figure 3.6.

CHAPTER 4

RESULTS

This chapter provided a detailed explanation with the help of tables and figures on the results obtained based on the research methodology adopted in the present study. Accordingly, the results of fake news detection divided into seven categories are explained with the outputs from the FANDC system.

4.1 Results

We experimentally tested a FANDC system created to detect fake news in OSNs, based on cloud computing. Figure 4.1 shows an example of a click-bait query result. *“New research: Our latest memo on YouTube #misinfo shows that the most popular #junknews videos find their audiences through Facebook. Less than 1 % % of the problematic videos shared on Facebook, less than 1% flagged the platform as potentially misleading. DemTech | Covid-related misinformation on YouTube: The spread of misinformation videos on social media and the effectiveness of platform policies (ox.ac.uk)”*. In this tweet, the FANDC system categorizes it as a clickbait. The webpage shortcut placed under the tweet is a clickbait trap by the system.

Figure 4.1

FANDC System Example of Clickbait Query Result

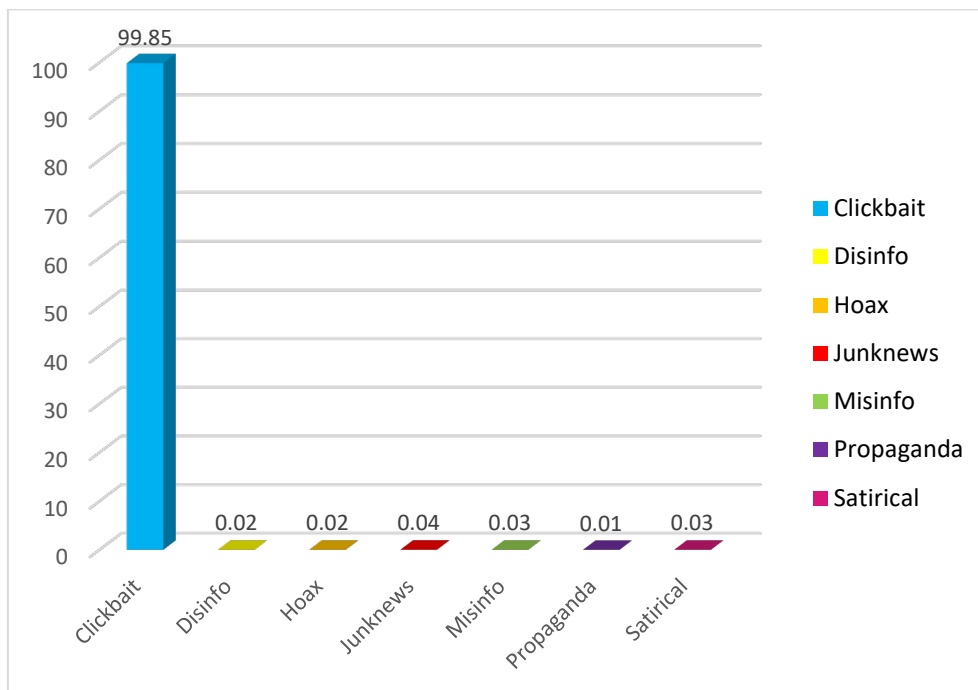


Figure 4.2 shows an example of the disinformation query results. The tweet text is “*Delighted to be part of this [@UoYSociology](#) event on July 26. We're looking for proposals from any discipline on the themes of 'Myth, Rumor & Misinformation'. 250 words max, deadline Fri 10 Jun. See all the details here: <http://bit.ly/folklore-to-fa...> [#myth](#) [#misinfo](#)”*. When the content of a tweet is examined, the use of a word’s myth and rumor together with misinformation leads to its perception as disinformation.

Figure 4.2

FANDC System Example of Disinformation Query Result

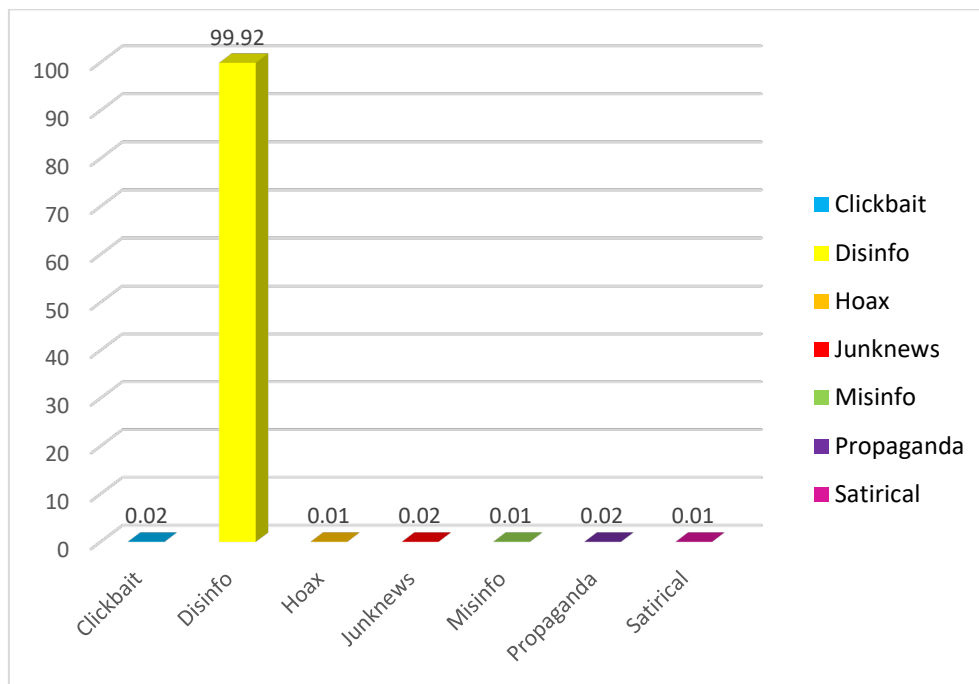


Figure 4.3 shows an example of the Hoax query result. Tweet text is “*Freshman Christopher Phillips CALLS OUT Brian Stelter and CNN for being a “purveyor of disinformation” purveyor of disinformation. He points to the Russian collusion hoax Jussie Smollett, the smears of Justice Kavanaugh and Nick Sandmann, and their dismissal of Hunter Biden’s laptop*”. Although word disinformation is used within the scope of the word hoax in the content of the tweet, it is essentially a hoax.

Figure 4.3

FANDC System Example of Hoax Query Result

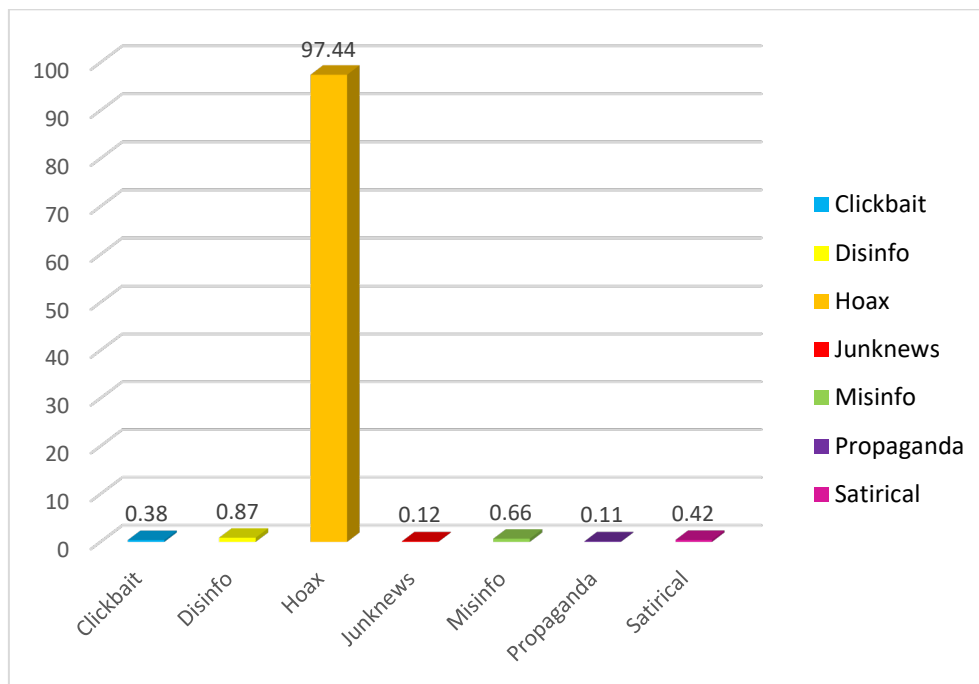


Figure 4.4 shows an example of a junk news query. “A Russian soldier from a chemical, biological, and nuclear protection unit picked up a source of cobalt-60 at one waste site with his bare hands, exposing himself to so much radiation in a few seconds that it went off the scales of a Geiger counter”.

Figure 4.4

FANDC System Example of Junk News Query Result

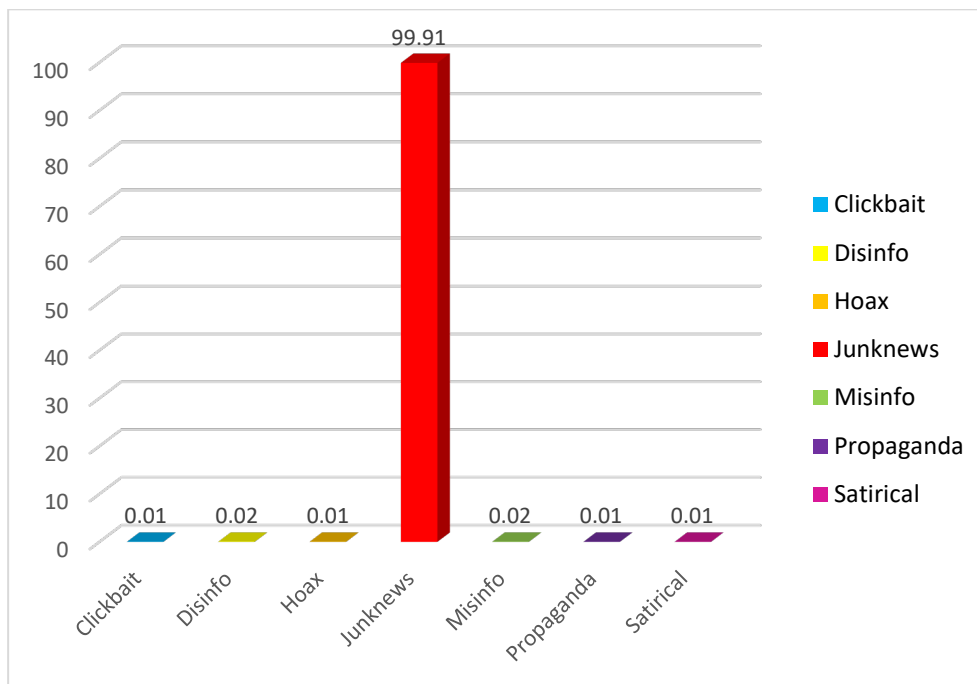


Figure 4.5 shows an example of a misinformation query result. Tweet text is “NC/VA - If you are not angry about this, you are not paying attention! #WatchTCenergy #Disinformation Internal emails show gas pipeline firms providing NC and Virginia leaders draft letters and points to praise their own projects. https://huffpost.com/entry/williams-tc-energy-pipeline-projects-influence-virginia-north-carolina_n_6261e382e4b0dc52f494659e?utm_campaign=share_twitter&ncid=engmodushp mg00000004... via @HuffPostPol”.

Figure 4.5

FANDC System Example of Misinformation Query Result

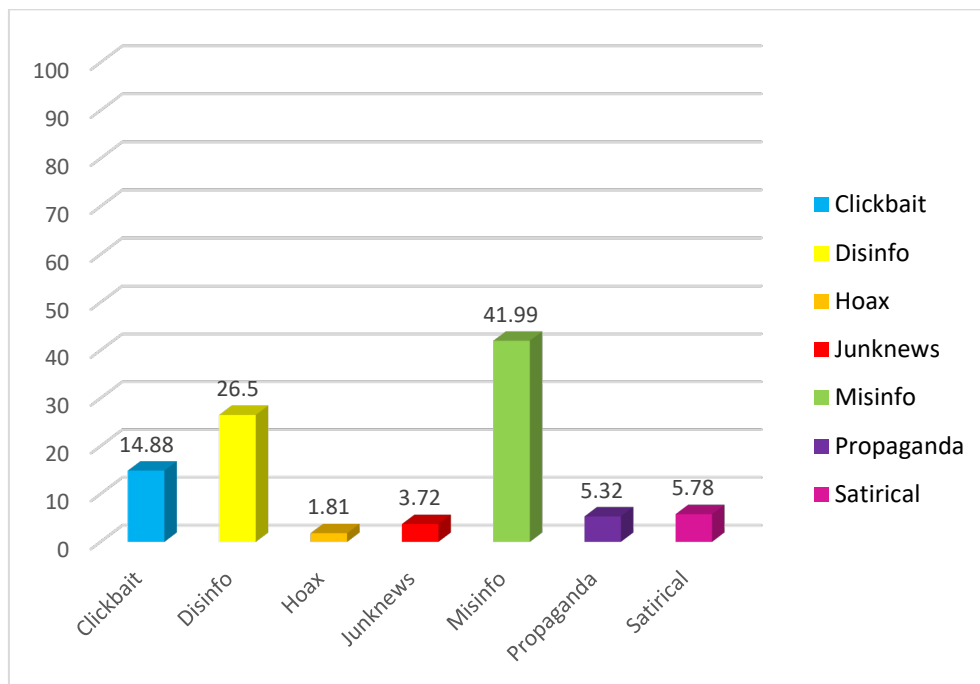


Figure 4.6 shows an example of propaganda query results. The text is “*Ontario Doctor accused of ‘disgraceful’ #COVID19 conduct has been suspended. Patrick Phillips spread the pandemic #misinformation and prescribed the debunked treatment #ivermectin at @lexharvs <https://thestar.com/news/canada/2022/05/03/ontario-doctor-accused-of-disgraceful-covid-conduct-gets-suspended.html>. utm_source=Twitter... via @torontostar #cdnhealth #infodemic*”. In this tweet, the propaganda activities of doctors were classified as having a high success rate.

Figure 4.6

FANDC System Example of Propaganda Query Result

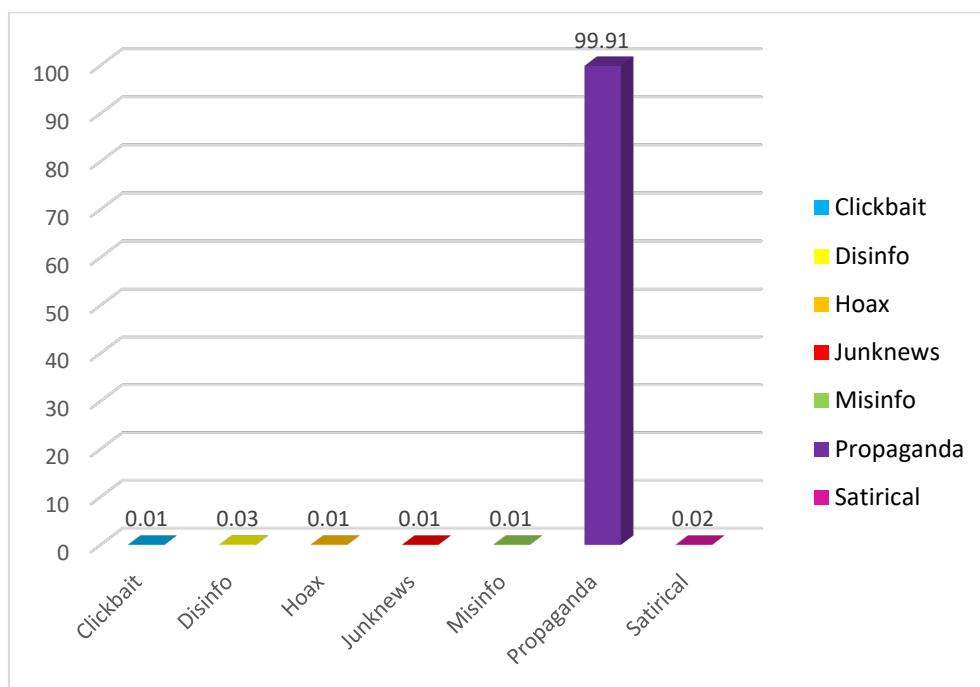
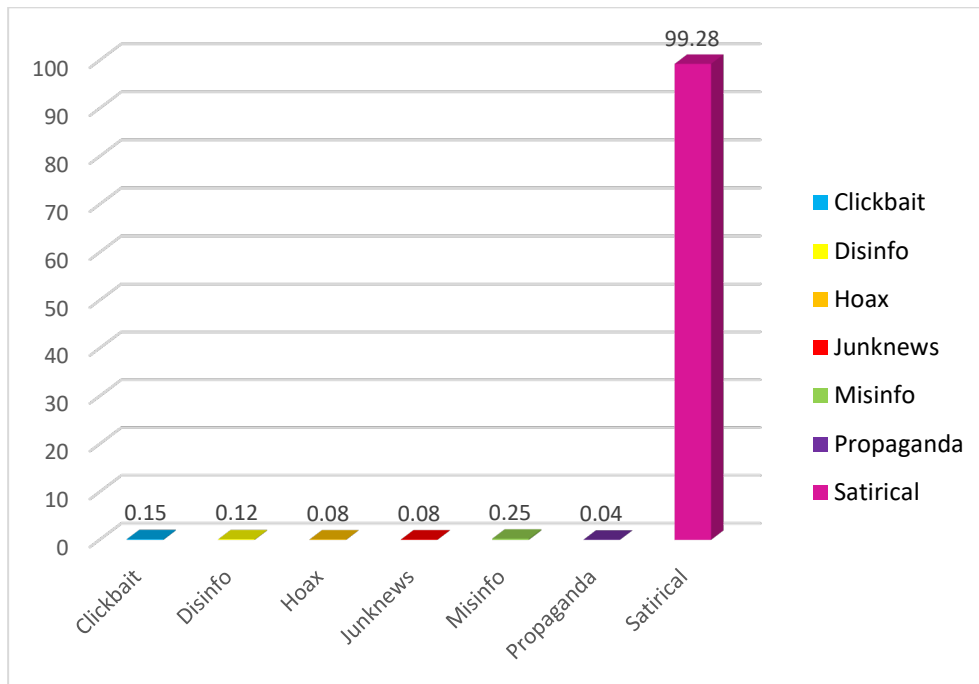


Figure 4.7 shows an example of a satisfactory query result. *The information that the [#Vatican](#) bought Ruble for the [#Russian](#) gas is based on a [#Satirical](#) post*". Finally, when we look at the tweets analyzed in Figure 5.7, it is determined that they are satirical in terms of content and are classified in this category.

Figure 4.7

FANDC System Example of Satirical Query Result



CHAPTER 5

DISCUSSION

In this section, the results obtained based on the research methodology adopted in this study are discussed comparatively with studies in the literature.

5.1 Discussion

Although fake news is often viral in OSNs, users are often unprotected and helpless. Many studies have been conducted on the detection of fake news in OSNs, particularly, given their recent popularity. To deceive OSN users, clickbait is embedded in a news story that contains fake information. Although Rajapaksha et al. (2021) detailed a study to detect click-bait traps by focusing on a learning model, when the results were examined, it was observed that the success rates were low despite the use of the BERT algorithm and its derivatives. The dataset used in this study consists of a labeled dataset. Again, as stated in the conclusion, the dataset used is insufficient in terms of volume and veracity. In this context, it is seen that the best result achieved is at the level of 90%. Although the extra-weighted method was used in the algorithms in a study by Hadi et al., (2021) the results did not reach 80%. Compared with the results of the FANDC system, which yielded results with 99.85% accuracy, as shown in Figure 4.1, the click-bait detections from other studies were at a very low level. What makes this study valuable is the volume of the dataset and meticulous preprocessing of the data.

Disinformation is an important concept that leaves a mark on the age at which we live, with an abundance of information. The diversification and widespread use of OSNs for different preferences is undoubtedly the leading cause of information pollution (Serrano-Puche, 2021). Elhadad et al. (2020) achieved a 99% success rate for a system developed to detect misleading information. However, the study was limited by modeling within the framework of the data collected in the field of health. For analyses outside of this area, it is necessary to remodel the system and modify the database. The *FANDC* system gathers a large volume and a variety of data. This produced more meaningful results within the framework of the fact that many people started to use OSNs intensively during the Covid-19 period. As shown in Figure 4.2, the data in the database are quite veracity and valuable, achieving 99.92% performance.

Hoax is among the most common types of fake news in an OSNs. Many studies have been conducted on the hoax. When these studies are examined Henry and Stattner (2019)

focused on the early detection of the spread of hoaxes in their study. They achieved an accuracy rate of up to 90% in the early detection of hoax spread in OSNs within approximately 20 minutes. Amrullah et al. (2022) proposed a linguistic approach that could be used as the first approach for detecting hoaxes. In this approach, the speaker's attitudes and behaviors were the focus, and the success rate could reach only 40%. Unlike other studies, Kencana et al. (2020) attempted to detect hoaxes using feed-forward and backpropagation neural-network classification methods. The study was conducted using an artificial neural network learning methodology based on deep learning algorithms. However, a success rate of 78.76% was achieved. Linge and Wicaksono (2022) conducted research on negative content on Twitter to detect hoaxes during the Covid-19 period. Classical ML algorithms were applied using the *CRISP-DM* methodology. The SMOTE technique was used in this study because unbalanced datasets were used. Consequently, the success rate of the algorithms was in the range 95-99%. Della Vedova et al. (2018c) Facebook posts, one of the OSNs in detecting hoaxes, making fun of fake news, hoaxes, etc., used datasets obtained from websites that were published for such purposes. The use of limited datasets attracted the attention of this study. In addition, the study works through a chatbot such as Facebook's messenger. The measurement results were in the range of 80-90%. Patel (2021a) used deep learning models for hoax detection. He also created a dataset by using Facebook posts. As stated in the Conclusion, the data were trained using a 10-fold cross-validation technique because they were studied using an insufficient dataset. The performance of the models was measured using the Friedman test, because the data were not normally distributed. It was observed that the study achieved an accuracy of approximately 70%. On the other hand, Putri et al. (2019) in their study, they used a data set they created with news articles. The most striking factor in this study was the inadequacy of the dataset. In total, 251 news articles were included in this study. After the data were labeled as hoax and non-hoax, they were trained using five different ML algorithms. From the results, it was observed that values in the range 67-74% were obtained. It was concluded that this study was conducted only at an experimental level. On the other hand, Yuliani et al. (2019) seems to have established a framework for hoax detection by collecting data from many websites and OSNs. Therefore, in future studies, we plan to use a dataset created for hoax detection.

A tweet, which is evaluated in terms of its content, is classified as junk news because it is far from context. Junk News is a genre that is viral in OSNs, categorized under the umbrella of fake news, and aims to create a sensation (Venturini, 2019b). It is usually based on trivial stories, cheap to produce, and profitable. Liotsiou et al. (2019) defined junk news as

various forms of propaganda: ideologically extreme, extreme partisan, or conspiratorial political news and information. For example, news that the disease was caused by the consumption of bat and dog meat at the beginning of the Covid-19 epidemic suddenly became viral. However, with the emergence of scientific facts, they disappeared from OSNs and became unimportant news (Duda-Chodak et al., 2020). As a result of research conducted on the detection of unimportant news, an understanding focusing on search engines or websites (as news sources) is encountered. It is naturally found on many search engines and websites with unimportant news. Savolainen et al. (2020) conducted a study on Facebook, a commonly used OSNs platform. In this study, junk news was identified by associating it with sentiment analysis within the scope of bipartisan or extremist ideas. Marchal et al. (2020) in their study on Twitter, measured the rate of junk news among all news and analyzed the results according to sentiment analysis. They found that less than 2% of the junk news was shared. The results of these studies indicate that junk news has not been examined extensively. For this reason, it was observed that the FANDC system has achieved a unique result in this category in the field of 99.91% of the results, as shown in Figure 4.4. This is because the FANDC system responds to the requests and needs of OSN users real-time and in a redundant structure to protect against cyberattacks on the cloud computing.

Misinformation shared without the purpose of harm, defined as the spreading process, is another type of fake news that spreads through an OSNs. Misinformation detection is often difficult. For this reason, the success of the system was only approximately 40% because of the insufficient level of the database in the training dataset and its complex relationship with the disinformation. Mulahuwaish et al. (2023) obtained 92.2% accuracy with a deep learning model in their studies by collecting Twitter data. It is remarkable that the datasets are sufficiently large and that they achieve success because of ten-fold training. Liu et al. (2019) on the other hand, created a data set by collecting data from WeChat and Weibo, a local microblogging site like Twitter used in China. They trained this dataset with 80% training and 20% testing using a tenfold cross-validation technique. The score obtained by applying classical ML algorithms was approximately 83%. This score indicates a low level of experimental success, because it has not been studied with sufficiently large data. Hayawi et al. (2022) created a new Twitter dataset to detect misinformation regarding the Covid-19 vaccine. They managed to create a very successful dataset with many tweets exceeding 15M and modeled the system with 75% training and 25% testing. The results obtained using three different algorithms and different iterations reached 99% in the BERT algorithm, 84% in XGBoost in other algorithms, and approximately 99% in LSTM. This study also achieved

better results than those of the FANC system. Al-Rakhami and Al-Amri (2020) collected approximately 400 K tweets on Twitter and created a dataset for their study. In their study, using six classical ML algorithms, they achieved a 97% success rate using a ten-fold cross-validation technique.

Propaganda is one of the most widely used types of fake news. For this type of fake news, it is important to reach many people in order to influence the public. In this context, Dewantara and Budi (2020) detected propaganda in online news articles by training the data in two layers, 80% training and 20% testing, using deep learning algorithms. They achieved an accuracy of 93%. However, it is noteworthy that online news sites are used instead of OSN. Compared with the *FANDC* system, as shown in Figure 4.6, our system once again came to the forefront in the fake news detection stage, providing results with 99.91% accuracy. Polonijo *et al.* (2021) applied a dataset created by collecting data from online news sites using RapidMiner software, a ready-made data-mining tool that uses deep-learning algorithms. In this study, although the extent to which the dataset was separated into training and test data was not specified, a ten-fold deep learning method was used. However, results were obtained with an accuracy of up to 95%. When compared with the *FANDC* system, considering that our system works real-time and, on the cloud, it was evaluated that 99.9% accuracy responds to OSN users with confidence in detecting propaganda. When the study by Khanday *et al.* (2021) was examined, it was observed that they created a dataset with approximately 5 K tweets on Twitter and used classical ML algorithms. The dataset was divided into two groups: 70% for training and 30% for testing. Although the results of the study with a limited number of datasets appear satisfactory (98%), the disadvantage is that they remain at the experimental level and do not appeal to OSN users.

Razali *et al.* (2022) study include 32k articles trained with deep learning algorithms and collected from online news sites. The dataset was divided into 80% training data and 20% testing data. The data obtained at the end of the training were evaluated by classification using ML algorithms. Accordingly, scores between 86 and 94% were obtained. Compared to the *FANDC* system, our system is at a very good level, with 99.28% accuracy, considering that it runs real-time and on the cloud. Ionescu & Chifu (2021) in their study, they used CamemBERT (Martin *et al.*, 2019), a state-of-the-art language model for French, with the data set they created from French online news sites for the French language. They used kernel ridge regression, which is resistant to overfitting, and achieved 97.4% success in news articles. Although the system does not operate online or real-time, it remains in the experimental stage. In the *FANDC* system, the rate is 99.28%, as shown in Figure 4.7.

In the framework of the above results, a comparative summary of the performance of FANDC and other studies is shown in Table 5.1. Accordingly, the results of FANDC are very good. Users can check any tweet that they suspect and want to check on Twitter by copying its shortcut from the system control bar and getting a response within a maximum of 5-10 seconds.

The two most important factors that make the system different from other fake news detection systems are that it is online, and it works in the cloud. In the future, data will be collected from other social networks and testing and evaluation of my site will continue. As a result, it is concluded that successful and real-time detection of fake news spread on OSNs is possible. Nevertheless, it is thought that the system can be improved further with more usage and user feedback in the future. At this stage, the evaluation results have been considered successful. Thus, users will be able to analyze as much as they want, whenever and wherever they want. Also, is planned to create another system trained with OpenAI's GPT-3 algorithm which is a revolutionary AI tool.

Table 5. 1*Comparison of the success rates of FANDC and other studies*

Categorization	Data Source	Success Rate Comparison	
Click Bait	Kaggle	Rajapaksha et al. (2021) 90%	FANDC
	Mendeley	Hadi et al. (2021) 80%	99.85%
Disinformation	WHO, UNICEF and UN	Elhadad et al. (2020) 99%	FANDC 99.92%
Hoax	Twitter	Henry & Stattner (2019) 90%,	FANDC 97.44%
	Local Web News Site	Amrullah et al. (2022) 40%	
	Twitter	Kencana et al. (2020) 78.76%	
	Twitter	Linge & Wicaksono (2022) 95-99%	
	Mixed source	Della Vedova et al. (2018) 80-90%	
	Facebook	Patel, (2021) 70%	
Junk News	Facebook	Marchal et al. (2020) 98%	FANDC
	Twitter	Mulahuwaish et al. (2023) 92.2%	99.92%
Misinformation	Chinees OSNs	Liu et al. (2019) 83%	FANDC 41.99%
	Twitter	Hayawi et al. (2022) 84-99%	
	Twitter	Al-Rakhami & Al-Amri (2020) 97%	
	Twitter	Dewantara & Budi (2020) 93%	
	Local web News Site	Polonijo et al. (2021) 95%	
Propaganda	Twitter	Khanday et al. (2021)98%	FANDC 99.91%
Satirical	CNN and The Onion	Razali et al. (2022) 86-94%	FANDC
	Local Web News Site	Ionescu & Chifu (2021) 97.4%	99.28%

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

This is the last chapter of the thesis and it concludes the research work with summarized findings, and recommendations for future studies.

6.1 Conclusion

Undoubtedly, OSNs are no longer just social networks, but as mobile phones become smarter and take the place of computers, they stand before us as a response to almost all our needs. Many government agencies now turn to OSNs to determine a person's delinquency or social status. Likewise, when you apply for a job in any institution, they want to browse your profile in your social network accounts and try to have information about you. However, as in the research of this thesis, the presence of inaccurate and misleading content in the profile created by the user or in the shares he/she makes has become the biggest problem of today's OSNs. Due to the increasing amount of data in OSNs, fake news is increasing both by malicious users and by well-intentioned but unaware users. Most of the time, users share the content they think is right, but they remain insensitive to the possible problems that it may cause. Sometimes it is even difficult to discern the exact truth. Therefore, this complex situation in OSNs has divided the fake news detection problem into seven categories as the subject of this thesis. Because each problem has been handled separately in the literature and focused more on system success, not fake news detection in OSNs. The system named FANDC, which was created to solve this problem, offers an implementation of a model that adopts a hybrid approach and provides almost 100% accuracy in terms of the results obtained. With this system we have created, fake news in OSNs can be detected in real time by user query and offers the user results in seven different categories. After the declaration of the Pandemic by the WHO, the tweets published on the subject from Twitter were carefully collected within the framework of the increasing use of OSN, and then these collected data were passed through a detailed pre-processing stage and the corpus was created to be used. Thus, the success of the system has emerged as subject-specific and target-oriented, not by the collection of random data. With the FANDC system introduced in this thesis, it has also been demonstrated that fake news can be detected in real time in OSNs and while doing this, it can be protected by avoiding cyber threats by making use of cloud computing.

The system was first tested by installing it on a local server. With the results obtained here, it was moved to cloud computing in order to avoid cyber threats, one of the most important problems of today. However, it was not possible to use the advantages of cloud computing in the first place. Of course, it took time for some connection issues and the system to run in the cloud with all its features. However, after ensuring the compatibility of the system, a system that is backed up in the form of containers and that can operate 24/7 over the other backup system has been revealed even if it is exposed to any cyber-attack with its distributed structure. In addition to avoiding cyber-attacks, using cloud computing brings with its internet connection and connection speed problems. However, besides its advantages, it is considered that this disadvantage can be ignored.

Another important factor that increases the success of the system is Google's BERT algorithm. It has contributed to the stable operation of the system with its high accuracy and success rate, as it is a revolution in the field of natural language processing by processing words and word groups in both directions. As a result, in order to protect OSN users from the fake news epidemic they are exposed to on these platforms, a system that has not yet been found in the literature and takes it from the experimental level to the operational level has emerged. With this system, it is thought that OSN users can easily solve the fake news detection problem in any situation they suspect and instantly.

6.2 Recommendations

The fact that the problem of detecting fake news in OSNs has become a research topic not only in computer engineering sciences, but also in artificial intelligence sciences such as NLP, as well as computational social sciences, necessitates an interdisciplinary approach to this problem. Of course, it is an undeniable fact that communication faculties are also in the field of interest in the last decade. It reveals how complex this problem is, especially with the introduction of concepts such as digital journalism and data journalism into the literature. First of all, suggestions will be presented to researchers in order to shed light on the studies expected to be carried out in the field with their reasons and results. In this content;

6.2.1 Recommendations For Researchers

Language models created for the detection of fake news in the field of Computer Science are limited to some languages, and this is one of the areas that should be studied first. In addition to its general acceptance in academia, the widespread use of the English language shows how narrowly the subject is addressed. There are very few studies conducted outside of

the English language, and it is considered that there is a clear need to develop and mature the literature and increase studies on the subject. A similar situation arises in the creation of algorithms and their use in real life. Examining these patterns with the unique structure of each language is important for natural language processing researchers. Again, studies on this subject cannot go beyond classical ML algorithms. Although there are some optimization studies, it is considered that these studies are not sufficient. Another research topic is that cloud computing and cyber security researchers work together to create a safer, more accessible and more sterile environment. Because, considering the problems that fake news will cause, it will take a long time to repair the damage it will cause to individuals, institutions and states. This can lead to people losing their lives and states not being able to fulfill their responsibilities towards their citizens in any crisis, such as the earthquake in Turkey in February 2023. In this context, it is recommended to ensure that all kinds of news published on OSNs can be easily controlled with this and a similar application developed, and to include it in the literature and disseminate it as the most important task.

6.2.2 Recommendations For OSN User

The increase in the use of OSN day by day, accordingly, the increasing desire of human beings to access information and news has affected OSN users both positively and negatively. Fake news spread on OSNs is the most obvious example of this. OSN users share every news or information they encounter on these platforms because they believe it is true. However, this shared news is very important not only for individuals but also for societies, organizations, institutions and even states. It is important to increase the awareness of users in this area, using information pollution as the purpose of disinformation and propaganda. It is recommended that an inquiring OSN user prevent the spread of such news by using the fake news detection system or different detection systems introduced in line with this thesis. In addition, OSN users are recommended to act sensitively by reporting fake news to the relevant state institutions and to contribute positively to the solution of the problem in question as a participant and responsible citizen.

6.2.3 Recommendations For Policy Maker

Of course, any news that spreads rapidly thanks to OSNs is important for the security of states. In the post-truth era, where the masses are manipulated through OSNs, it is among the primary duties of states to ensure that their citizens have access to real news. In this context, it is recommended to strictly supervise OSNs with relevant institutions and

organizations, to ensure that the journalism institution makes news within the framework of ethical principles, and of course to implement online systems such as the fake news detection systems introduced in this study in order to protect the individual users of OSNs. In addition, if fake news spread on OSNs is detected, it is recommended that states expose them and impose sanctions on the networks in question as another option. On the other hand, it is recommended to guide academia and researchers, non-governmental organizations as well as individuals who will work in these fields, through encouraging meetings, symposiums and competitions.

REFERENCES

- ABC News (n.d.). Retrieved May., 25, 2020 from <https://hollywoodgazette.com/abcnews-com-co/>.
- Aborisade, O., & Anwar, M. (2018, July 6-9). *Classification for authorship of tweets by comparing logistic regression and naive bayes classifiers*. In IEEE International Conference on Information Reuse and Integration (IRI). Salt Lake City, UT, USA.
- Affelt, A. (2019). How to spot fake news. *Emerald Publishing Limited, Leeds*, pp. 57-84. <https://doi.org/10.1108/978-1-78973-361-720191005>
- Ahmad, T., Aliaga Lazarte, E. A., & Mirjalili, S. (2022). A systematic literature review on fake news in the covid-19 pandemic: can ai propose a solution?. *Applied Sciences*, *12*(24), 12727. <https://doi.org/10.3390/app122412727>
- Ahmed, A. A. A., Aljabouh, A., Donepudi, P. K., & Choi, M. S. (2021). Detecting fake news using machine learning: A systematic literature review. *arXiv preprint arXiv:2102.04458*. <https://doi.org/10.48550/arXiv.2102.04458>
- Akyön, F. Ç., Alp, Y. K., Gök, G., & Arıkan, O. (2018, May 2-5). *Deep learning in electronic warfare systems: automatic intra-pulse modulation recognition*. In 26th Signal Processing and Communications Applications Conference (SIU). IEEE. Izmir, Türkiye.
- Alam, F., Cresci, S., Chakraborty, T., Silvestri, F., Dimitrov, D., Martino, G. D. S., ... & Nakov, P. (2021). A survey on multimodal disinformation detection. *arXiv preprint arXiv:2103.12541*. <https://doi.org/10.48550/arXiv.2103.12541>
- Al-Asadi, M. A., & Tasdemir, S. (2022). Using artificial intelligence against the phenomenon of fake news: a systematic literature review. *Combating Fake News with Computational Intelligence Techniques*, pp. 39-54. https://doi.org/10.1007/978-3-030-90087-8_2
- Aldwairi, M., & Alwahedi, A., (2018, November 5-8). *Detecting fake news in social network networks*. The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks. Leuven, Belgium.

- Alkhodair, S. A., Ding, S. H., Fung, B. C., & Liu, J. (2020). Detecting breaking news rumors of emerging topics in social media. *Information Processing & Management*, 57(2), 102018. <https://doi.org/10.1016/j.ipm.2019.02.016>
- Allen, J., Martel, C., & Rand, D. G. (2022, April 29-May 5). *Birds of a feather don't fact-check each other: partisanship and the evaluation of news in twitter's birdwatch crowdsourced fact-checking program*. In Proceedings of the CHI Conference on Human Factors in Computing Systems. New Orleans, LA, USA.
- Allyn, B. (2020, May 20). *Researchers: nearly half of accounts tweeting about coronavirus are likely bots*. Retrieved May., 25, 2020 from <https://www.npr.org/sections/coronavirus-live-updates/2020/05/20/859814085/researchers-nearly-half-of-accounts-tweeting-about-coronavirus-are-likely-bots>.
- Alom, Z., Carminati, B., & Ferrari, E. (2018, August 28-31). *Detecting spam accounts on Twitter*. In IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Barcelona, Spain.
- Al-Rakhami, M. S., & Al-Amri, A. M. (2020). Lies kill, facts save: detecting covid-19 misinformation in Twitter. *IEEE Access*, 8, 155961-155970. <https://doi.org/10.1109/ACCESS.2020.3019600>
- Al-Garadi, M. A., Yang, Y. C., & Sarker, A. (2022). The role of natural language processing during the covid-19 pandemic: health applications, opportunities, and challenges. *Healthcare*, Vol. 10, No. 11, p. 2270. <https://doi.org/10.3390/healthcare10112270>
- Alghamdi, J., Luo, S., & Lin, Y. (2024). A comprehensive survey on machine learning approaches for fake news detection. *Multimedia Tools and Applications*, 83(17), 51009-51067. <https://doi.org/10.1007/s11042-023-17470-8>
- Altheneyan, A., & Alhadlaq, A. (2023). Big data ML-based fake news detection using distributed learning. *IEEE Access*, 11, 29447-29463. <https://doi.org/10.1109/ACCESS.2023.3260763>
- American News (n.d.). Retrieved May., 25, 2020 from <https://www.politifact.com/personalities/americannewscom/>.
- Amrullah, F., Gusnawaty, G., & Yassi, A. H. (2022, April 27). *Hoax detection through analysis of modality: a systemic-functional linguistics study*.

- In 9th Asbam International Conference (Archeology, History, & Culture In The Nature of Malay) (ASBAM 2021). Malaysia.
- Aphiwongsophon, S., & Chongstitvatana, P. (2018, July 18-21). *Detecting fake news with machine learning method*. In 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). Chiang Rai, Thailand.
- Apuke, O. D., & Omar, B. (2021). Fake news and COVID-19: modelling the predictors of fake news sharing among social media users. *Telematics and Informatics*, 56, 101475. <https://doi.org/10.1016/j.tele.2020.101475>
- Aridor, G., Goncalves, D., & Sikdar, S. (2020, September 22-26). *Deconstructing the filter bubble: user decision-making and recommender systems*. In Proceedings of the 14th ACM Conference on Recommender Systems. Brazil.
- Atodiresei, C. S., Tănăselea, A., & Iftene, A. (2018). Identifying fake news and fake users on Twitter. *Procedia Computer Science*, 126, 451-461. <https://doi.org/10.1016/j.procs.2018.07.279>
- Bastick, Z. (2021). Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation. *Computers in human behavior*, 116, 106633. <https://doi.org/10.1016/j.chb.2020.106633>
- BBC, (2018, December 18). *France protests: The voices of the “gilets jaunes”*. Retrieved May., 05, 2022 from <https://www.bbc.com/news/world-europe-46480867>.
- Bimber, B. (2014). Digital media in the Obama campaigns of 2008 and 2012: Adaptation to the personalized political communication environment. *Journal of information technology & politics*, 11(2), 130-150. <https://doi.org/10.1080/19331681.2014.895691>
- Burkov, A. (2020). *Machine learning engineering* (Vol. 1). Montreal, QC, Canada: True Positive Incorporated.
- Capuano, N., Fenza, G., Loia, V., & Nota, F. D. (2023). Content-based fake news detection with machine and deep learning: a systematic review. *Neurocomputing*, 530, 91-103. <https://doi.org/10.1016/j.neucom.2023.02.005>
- Cardoso Durier da Silva, F., Vieira, R., & Garcia, A. C. (2019, January 8-11). *Can machines learn to detect fake news? a survey focused on social*

- media*. Proceedings of the 52nd Hawaii International Conference on System Sciences. Grand Wailea, Hawaii.
- Castells, M. (2016). İletişim Gücü, (Çev. Ebru Kılıç). *İstanbul: Bilgi Üniversitesi Yayınları*.
- Centers for Disease Control and Prevention (2022 May., 05). Retrieved May., 10, 2022) from <https://www.cdc.gov/vaccines/covid-19/clinical-considerations/interim-considerations-us.html>.
- Chaudhari, D. D., & Pawar, A. V. (2021). Propaganda analysis in social media: a bibliometric review. *Information Discovery and Delivery*, 49(1), 57-70. <https://doi.org/10.1108/IDD-06-2020-0065>
- Chen, E., Lerman, K., & Ferrara, E. (2020). Tracking social media discourse about the covid-19 pandemic: Development of a public coronavirus twitter data set. *JMIR public health and surveillance*, 6(2), e19273. <https://doi.org/10.2196/19273>
- Choudhary, A., & Arora, A. (2021). Linguistic feature based learning model for fake news detection and classification. *Expert Systems with Applications*, 169, 114171. <https://doi.org/10.1016/j.eswa.2020.114171>
- Ciampaglia, G. L., Shiralkar, P., Rocha, L. M., Bollen, J., Menczer, F., & Flammini, A. (2015). Computational fact checking from knowledge networks. *PloS one*, 10(6), e0128193. <https://doi.org/10.1371/journal.pone.0128193>
- Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. <https://doi.org/10.1073/pnas.2023301118>
- Çetin, V., & Yildiz, O. (2022). A comprehensive review on data preprocessing techniques in data analysis. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 28(2), 299-312. <https://doi.org/10.5505/pajes.2021.62687>
- De Beer, D., & Matthee, M. (2021). Approaches to identify fake news: a systematic literature review. *Integrated Science in Digital Age*, 2020, 13-22. https://doi.org/10.1007/978-3-030-49264-9_2

- De Magistris, G., Russo, S., Roma, P., Starczewski, J. T., & Napoli, C. (2022). An explainable fake news detector based on named entity recognition and stance classification applied to covid-19. *Information*, 13(3), 137. <https://doi.org/10.3390/info13030137>
- Della Vedova, M. L., Tacchini, E., Moret, S., Ballarin, G., DiPierro, M., & De Alfaro, L. (2018, May 15-18). *Automatic online fake news detection combining content and social signals*. 2018 22nd Conference of Open Innovations Association (FRUCT). Jyväskylä, Finland.
- Department for Digital, Culture, Media & Sport, United Kingdom Government. (2020, May 6). *5G and coronavirus (COVID-19)*. Retrieved Jun., 25, 2020 from <https://www.gov.uk/guidance/5g-and-coronavirus-covid-19>.
- Derhab, A., Alawwad, R., Dehwah, K., Tariq, N., Khan, F. A., & Al-Muhtadi, J. (2021). Tweet-based bot detection using big data analytics. *IEEE Access*, 9, 65988-66005. <https://doi.org/10.1109/ACCESS.2021.3074953>
- Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*.
- Dewantara, D. S., & Budi, I. (2020, November 3-4). Combination of lstm and cnn for article-level propaganda detection in news articles. 2020 Fifth International Conference on Informatics and Computing (ICIC). Gorontalo, Indonesia
- Dharani, M., & Sivachitra, M. (2017, March 17-18). *Motor imagery signal classification using semi supervised and unsupervised extreme learning machines*. 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). Coimbatore, India.
- Dixon, S. (2024, May 22). *Number of social network users in selected countries in 2023 and 2029*. Retrieved Oct., 10, 2024 from <https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/>.
- Dixon, S. (2024, July 10) *Most popular social networks worldwide as of April 2024, by number of monthly active users*. Retrieved Oct., 10, 2024 from <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.

- Duda-Chodak, A., Lukasiewicz, M., Zięć, G., Florkiewicz, A., & Filipiak-Florkiewicz, A. (2020). Covid-19 pandemic and food: Present knowledge, risks, consumers fears and safety. *Trends in Food Science & Technology*, *105*, 145-160. <https://doi.org/10.1016/j.tifs.2020.08.020>
- Duff, A. S. (2023). Castells versus Bell: a comparison of two grand theorists of the information age. *European Journal of Social Theory*, *26*(1), 90-108. <https://doi.org/10.1177/13684310221099695>
- Elhadad, M. K., Li, K. F., & Gebali, F. (2020). Detecting misleading information on COVID-19. *IEEE Access*, *8*, 165201-165215. <https://doi.org/10.1109/ACCESS.2020.3022867>
- Ersöz, B. (2020). Yeni nesil web paradigması-web 4.0. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *1*(2), 58-65.
- Facebook (n.d.) Retrieved May., 25, 2020 from <https://www.facebook.com/>.
- Ferrara, E., Chang, H., Chen, E., Muric, G., & Patel, J. (2020). Characterizing social media manipulation in the 2020 U.S. presidential election. *First Monday*, *25*(11). <https://doi.org/10.5210/fm.v25i11.11431>
- Figueira, Á., & Oliveira, L. (2017). The current state of fake news: challenges and opportunities. *Procedia computer science*, *121*, 817-825. <https://doi.org/10.1016/j.procs.2017.11.106>
- Freelon, D., Bossetta, M., Wells, C., Lukito, J., Xia, Y., & Adams, K. (2022). Black trolls matter: Racial and ideological asymmetries in social media disinformation. *Social Science Computer Review*, *40*(3), 560-578. <https://doi.org/10.1177/0894439320914853>
- Gilda, S. (2017, December 13-14). *Evaluating machine learning algorithms for fake news detection*. 2017 IEEE 15th Student Conference on Research and Development (SCORED). Wilayah Persekutuan Putrajaya, Malaysia.
- Girgis, S., Amer, E., & Gadallah, M. (2018, December 18-19). *Deep learning algorithms for detecting fake news in online text*. 2018 13th International Conference on Computer Engineering and Systems (ICCES). Cairo, Egypt.
- Goksu, M., & Cavus, N. (2023). Knowledge Management in the Covid-19 Period: Misinformation and Disinformation. *IU Press, Pandemic and the Critical Role of Knowledge Management*. <https://doi.org/10.26650/B/ET07.2023.004.16>

- Goksu, M., Cavus, N., Cavus, A., & Karagozlu, D. (2020). Fake news detection on social networks with cloud computing: Advantages and disadvantages. *Int. J. Adv. Sci. Technol*, 29(7), 2137-2150.
- Goksu, M., & Cavus, N. (2019, August 27-28). *Fake news detection on social networks with artificial intelligence tools: systematic literature review*. 10th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions - ICSCCW-2019. Prague, Czech Republic. https://doi.org/10.1007/978-3-030-35249-3_5
- Granik, M., & Mesyura, V. (2017, May 29-June 2). *Fake news detection using naive Bayes classifier*. 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON). Kyiv, Ukraine.
- Gupta, S., Thirukovalluru, R., Sinha, M., & Mannarswamy, S. (2018, August 28-31). *CIMTDetect: a community infused matrix-tensor coupled factorization-based method for fake news detection*. 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Barcelona, Spain.
- Hadi, P. S., Fanani, A. Z., Shidik, G. F., & Alzami, F. (2021, September 18-19). *Using extra weight in machine learning algorithms for clickbait detection of Indonesia online news headlines*. 2021 International Seminar on Application for Technology of Information and Communication (iSemantic). Semarangin, Indonesia.
- Hakak, S., Alazab, M., Khan, S., Gadekallu, T. R., Maddikunta, P. K. R., & Khan, W. Z. (2021). An ensemble machine learning approach through effective feature extraction to classify fake news. *Future Generation Computer Systems*, 117, 47-58. <https://doi.org/10.1016/j.future.2020.11.022>
- Hall, W., Tinati, R., & Jennings, W. (2018). From Brexit to Trump: Social media's role in democracy. *Computer*, 51(1), 18-27. <https://doi.org/10.1109/MC.2018.1151005>
- Hayawi, K., Shahriar, S., Serhani, M. A., Taleb, I., & Mathew, S. S. (2022). ANTi-Vax: a novel Twitter dataset for COVID-19 vaccine misinformation detection. *Public health*, 203, 23-30. <https://doi.org/10.1016/j.puhe.2021.11.022>
- Helmstetter, S., & Paulheim, H. (2018, August 28-31). *Weakly supervised learning for fake news detection on Twitter*. 2018 IEEE/ACM International

- Conference on Advances in Social Networks Analysis and Mining (ASONAM). Barcelona, Spain.
- Henry, D., & Stattner, E. (2019, November 08-11). *Predictive models for early detection of hoax spread in Twitter*. 2019 International Conference on Data Mining Workshops (ICDMW). Beijing, China.
- Herrero-Diz, P., Conde-Jiménez, J., & Reyes de Cózar, S. (2020). Teens' motivations to spread fake news on WhatsApp. *Social Media+ Society*, 6(3), 2056305120942879. <https://doi.org/10.1177/2056305120942879>
- Hickman, L., Thapa, S., Tay, L., Cao, M., & Srinivasan, P. (2022). Text preprocessing for text mining in organizational research: Review and recommendations. *Organizational Research Methods*, 25(1), 114-146. <https://doi.org/10.1177/1094428120971683>
- Huang, B., & Carley, K. M. (2020). Disinformation and misinformation on twitter during the novel coronavirus outbreak. *arXiv preprint arXiv:2006.04278*. <https://doi.org/10.48550/arXiv.2006.04278>
- Huang, Y. F., & Chen, P. H. (2020). Fake news detection using an ensemble learning model based on self-adaptive harmony search algorithms. *Expert Systems with Applications*, 159, 113584. <https://doi.org/10.1016/j.eswa.2020.113584>
- Huber, S., Wiemer, H., Schneider, D., & Ihlenfeldt, S. (2019). DMME: Data mining methodology for engineering applications—a holistic extension to the CRISP-DM model. *Procedia Cirp*, 79, 403-408. <https://doi.org/10.1016/j.procir.2019.02.106>
- Instagram (n.d.) Retrieved May., 25, 2020 from <https://www.instagram.com/>.
- Ionescu, R. T., & Chifu, A. G. (2021, July 18-22). *Fresada: a french satire data set for cross-domain satire detection*. 2021 International Joint Conference on Neural Networks (IJCNN). Shenzhen, China.
- Iosifidis, P., & Nicoli, N. (2020). The battle to end fake news: A qualitative content analysis of Facebook announcements on how it combats disinformation. *International Communication Gazette*, 82(1), 60-81. <https://doi.org/10.1177/1748048519880729>
- Işık, M., & Dağ, H. (2020). The impact of text preprocessing on the prediction of review ratings. *Turkish Journal of Electrical Engineering and Computer Sciences*, 28(3), 1405-1421. <https://doi.org/10.3906/elk-1907-46>

- Jain, A., & Kasbe, A. (2018, February 24-25). Fake News Detection. *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*. Bhopal, India.
- Jeong, Y., Kim, S., & Yoon, B. (2018, August 19-23). *An algorithm for supporting decision making in stock investment through opinion mining and machine learning*. 2018 Portland International Conference on Management of Engineering and Technology (PICMET). Honolulu, HI, USA.
- Jeremiah, S. S., Miyakawa, K., Morita, T., Yamaoka, Y., & Ryo, A. (2020). Potent antiviral effect of silver nanoparticles on SARS-CoV-2. *Biochemical and biophysical research communications*, *533*(1), 195-200. <https://doi.org/10.1016/j.bbrc.2020.09.018>
- Jiang, S., & Wilson, C. (2018). Linguistic signals under misinformation and fact-checking: Evidence from user comments on social media. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-23. <https://doi.org/10.1145/3274351>
- Jiang, T. A. O., Li, J. P., Haq, A. U., Saboor, A., & Ali, A. (2021). A novel stacking approach for accurate detection of fake news. *IEEE Access*, *9*, 22626-22639. <https://doi.org/10.1109/ACCESS.2021.3056079>
- Kachalsky, I., Zakirzyanov, I., & Ulyantsev, V. (2017, December 18-21). *Applying reinforcement learning and supervised learning techniques to play hearthstone*. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). Cancun, Mexico.
- Kadhim, A. I. (2018). An evaluation of preprocessing techniques for text classification. *International Journal of Computer Science and Information Security (IJCSIS)*, *16*(6), 22-32.
- Kaliyar, R. K., Goswami, A., Narang, P., & Sinha, S. (2020). FNDNet—a deep convolutional neural network for fake news detection. *Cognitive Systems Research*, *61*, 32-44. <https://doi.org/10.1016/j.cogsys.2019.12.005>
- Kauffmann, E., Peral, J., Gil, D., Ferrández, A., Sellers, R., & Mora, H. (2020). A framework for big data analytics in commercial social networks: A case study on sentiment analysis and fake review detection for marketing decision-making. *Industrial Marketing Management*, *90*, 523-537. <https://doi.org/10.1016/j.indmarman.2019.08.003>

- Kemp, S. (2024, January 31). *Digital 2024: 5 billion social media users*. Retrieved Oct., 10, 2022 from <https://wearesocial.com/us/blog/2024/01/digital-2024-5-billion-social-media-users/>.
- Kemp, S. (2024, January 31). *Digital 2024: Global Overview Report*. Retrieved Oct., 10, 2024 from <https://datareportal.com/reports/digital-2024-global-overview-report>.
- Kencana, C. W., Setiawan, E. B., & Kurniawan, I. (2020). Hoax detection system on twitter using feed-forward and back-propagation neural networks classification method. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(4), 655-663. <https://doi.org/10.29207/resti.v4i4.2038>
- Khanday, A. M. U. D., Khan, Q. R., & Rabani, S. T. (2021). Identifying propaganda from online social networks during COVID-19 using machine learning techniques. *International Journal of Information Technology*, 13, 115-122. <https://doi.org/10.1007/s41870-020-00550-5>
- Kotteti, C. M. M., Dong, X., Li, N., & Qian, L. (2018, August 12-15). *Fake news detection enhancement with data imputation*. In IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) pp. 187-192. IEEE. Athens, Greece. <https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00042>
- Kristoffersen, E., Aremu, O. O., Blomsma, F., Mikalef, P., & Li, J. (2019, September 18-20). *Exploring the relationship between data science and circular economy: an enhanced CRISP-DM process model*. 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019. Trondheim, Norway.
- Lahby, M., Aqil, S., Yafooz, W. M., & Abakarim, Y. (2022). Online fake news detection using machine learning techniques: A systematic mapping study. *Combating Fake News with Computational Intelligence Techniques*, 3-37. https://doi.org/10.1007/978-3-030-90087-8_1
- Li, D., Guo, H., Wang, Z., & Zheng, Z. (2021). Unsupervised fake news detection based on autoencoder. *IEEE access*, 9, 29356-29365.

- Liao, Q., Chai, H., Han, H., Zhang, X., Wang, X., Xia, W., & Ding, Y. (2021). An integrated multi-task model for fake news detection. *IEEE Transactions on Knowledge and Data Engineering*, 34(11), 5154-5165. <https://doi.org/10.1109/TKDE.2021.3054993>
- Linge, P. T., & Wicaksono, A. F. (2022). Detection of negative content (hoax) on microblog data that contains covid-19 information. *Syntax Literate; Jurnal Ilmiah Indonesia*, 7(6), 8820-8830. <https://doi.org/10.36418/syntax-literate.v7i6.8279>
- LinkedIn (n.d.) Retrieved May., 25, 2020 from <https://www.linkedin.com/>.
- Liotsiou, D., Kollanyi, B., & Howard, P. N. (2019). The junk news aggregator: Examining junk news posted on Facebook, starting with the 2018 US midterm elections. *arXiv preprint arXiv:1901.07920*. <https://doi.org/10.48550/arXiv.1901.07920>
- Liu, Y., Yu, K., Wu, X., Qing, L., & Peng, Y. (2019). Analysis and detection of health-related misinformation on Chinese social media. *IEEE Access*, 7, 154480-154489. <https://doi.org/10.1109/ACCESS.2019.2946624>
- Lutkevich, B. (n.d.). *BERT language model*. Retrieved Jul., 05, 2023 from <https://www.techtarget.com/searchenterpriseai/definition/BERT-language-model#:~:text=BERT%20is%20designed%20to%20help,with%20question%20and%20answer%20datasets.>
- Madani, Y., Erritali, M., & Bouikhalene, B. (2021). Using artificial intelligence techniques for detecting Covid-19 epidemic fake news in Moroccan tweets. *Results in Physics*, 25, 104266. <https://doi.org/10.1016/j.rinp.2021.104266>
- Mahyoob, M., Al-Garaady, J., & Alrahaili, M. (2020). Linguistic-based detection of fake news in social media. *Forthcoming, International Journal of English Linguistics*, 11(1). <https://doi.org/10.5539/ijel.v11n1p99>
- Malumatfurus (n.d.) Retrieved May., 25, 2020 from <https://www.malumatfurus.org/>.
- Marchal, N., Kollanyi, B., Neudert, L. M., Au, H., & Howard, P. N. (2020). Junk news & information sharing during the 2019 UK general election. *arXiv preprint arXiv:2002.12069*. <https://doi.org/10.48550/arXiv.2002.12069>

- Marlow, T., Miller, S., & Roberts, J. T. (2021). Bots and online climate discourses: Twitter discourse on President Trump's announcement of US withdrawal from the Paris Agreement. *Climate Policy*, 21(6), 765-777. <https://doi.org/10.1080/14693062.2020.1870098>
- Martin, L., Muller, B., Suárez, P. J. O., Dupont, Y., Romary, L., de La Clergerie, É. V., ... & Sagot, B. (2019). CamemBERT: a tasty French language model. *arXiv preprint arXiv:1911.03894*. <https://doi.org/10.18653/v1/2020.acl-main.645>
- Martínez-Plumed, F., Contreras-Ochando, L., Ferri, C., Hernández-Orallo, J., Kull, M., Lachiche, N., ... & Flach, P. (2019). CRISP-DM twenty years later: From data mining processes to data science trajectories. *IEEE Transactions on Knowledge and Data Engineering*, 33(8), 3048-3061. <https://doi.org/10.1109/TKDE.2019.2962680>
- Mathews, E. Z., & Preethi, N. (2022, January 25-27). *Fake news detection: an effective content-based approach using machine learning techniques*. 2022 International Conference on Computer Communication and Informatics (ICCCI). Coimbatore, India.
- Mazza, M., Avvenuti, M., Cresci, S., & Tesconi, M. (2022). Investigating the difference between trolls, social bots, and humans on Twitter. *Computer Communications*, 196, 23-36. <https://doi.org/10.1016/j.comcom.2022.09.022>
- Meel, P., & Vishwakarma, D. K. (2020). Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. *Expert Systems with Applications*, 153, 112986. <https://doi.org/10.1016/j.eswa.2019.112986>
- Milani, A. (2010, October 6). *The Green Movement*. Retrieved May., 05, 2022 from <https://iranprimer.usip.org/resource/green-movement>.
- Mir, A. A., Rathinam, S., & Gul, S. (2022). Public perception of COVID-19 vaccines from the digital footprints left on Twitter: analyzing positive, neutral and negative sentiments of Twitterati. *Library Hi Tech*, 40(2), 340-356. <https://doi.org/10.1108/LHT-08-2021-0261>
- Mu, Y., & Aletras, N. (2020). Identifying Twitter users who repost unreliable news sources with linguistic information. *PeerJ Computer Science*, 6, e325. <https://doi.org/10.7717/peerj-cs.325>

- Mukhopadhyay, S., Tilak, O., & Chakrabarti, S. (2018, December 17-20). *Reinforcement learning algorithms for uncertain, dynamic, zero-sum games*. 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). Orlando, FL, USA.
- Mulahuwaish, A., Osti, M., Gyorick, K., Maabreh, M., Gupta, A., & Qolomany, B. (2023 October 20-22). *CovidMis20: covid-19 misinformation detection system on Twitter tweets using deep learning models*. 14th International Conference, IHCI 2022. Tashkent, Uzbekistan.
- Nasir, J. A., Khan, O. S., & Varlamis, I. (2021). Fake news detection: A hybrid CNN-RNN based deep learning approach. *International Journal of Information Management Data Insights*, 1(1), 100007. <https://doi.org/10.1016/j.jjime.2020.100007>
- News Busters (n.d.) Retrieved May., 25, 2020 from <https://www.newsbusters.org/>.
- Newman, N. (2022, February 4). *Digital New Report 2022*. Retrieved Jul., 15, 2022 from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf.
- Newyorker (n.d.) Retrieved May., 25, 2020 from <https://www.newyorker.com/>.
- Nijhawan, R., Srivastava, I., & Shukla, P. (2017, June 2-3). *Land cover classification using super-vised and unsupervised learning techniques*. 2017 International Conference on Computational Intelligence in Data Science (ICCIDS). Chennai, India.
- Onan, A., & Toçoğlu, M. A. (2020). Satire identification in Turkish news articles based on ensemble of classifiers. *Turkish Journal of Electrical Engineering and Computer Sciences*, 28(2), <https://doi.org/1086-1106.10.3906/elk-1907-11>
- Ongsulee, P. (2017, November 22-24). *Artificial intelligence, machine learning and deep learning*. 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE). Bangkok, Thailand.
- Orabi, M., Mouheb, D., Al Aghbari, Z., & Kamel, I. (2020). Detection of bots in social media: a systematic review. *Information Processing & Management*, 57(4), 102250. <https://doi.org/10.1016/j.ipm.2020.102250>

- Ozbay, F. A., & Alatas, B. (2020). Fake news detection within online social media using supervised artificial intelligence algorithms. *Physica A: statistical mechanics and its applications*, 540, 123174. <https://doi.org/10.1016/j.physa.2019.123174>
- Pal, A., & Pradhan, M. (2023). Survey of fake news detection using machine intelligence approach. *Data & Knowledge Engineering*, 144, 102118. <https://doi.org/10.1016/j.datak.2022.102118>
- Patel, K. (2021). *Automatic Hoax Detection on Social Media Using Deep Learning*. [Master of Science Thesis]. Faculty of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden.
- Peng, S., Zhou, Y., Cao, L., Yu, S., Niu, J., & Jia, W. (2018). Influence analysis in social networks: A survey. *Journal of Network and Computer Applications*, 106, 17-32. <https://doi.org/10.1016/j.jnca.2018.01.005>
- Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, 64(6), 763-774. <https://doi.org/10.1016/j.bushor.2021.07.012>
- Petrosyan, A. (2024, November 5). *Number of internet and social media users worldwide as of January 2024*. Retrieved Oct., 15, 2024 from <https://www.statista.com/statistics/617136/digital-population-worldwide/>.
- Politifact (n.d.). Retrieved May., 25, 2020 from <https://www.politifact.com/>.
- Polonijo, B., Šuman, S., & Šimac, I. (2021, September27-October 1). *Propaganda Detection Using Sentiment Aware Ensemble Deep Learning*. In 44th International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 199-204). Opatija, Croatia.
- Pulido, C. M., Villarejo-Carballido, B., Redondo-Sama, G., & Gómez, A. (2020). COVID-19 infodemic: More retweets for science-based information on coronavirus than for false information. *International sociology*, 35(4), 377-392. <https://doi.org/10.1177/0268580920914755>
- Purbasari, A., Rinawan, F. R., Zulianto, A., Susanti, A. I., & Komara, H. (2021, September 29-30). *CRISP-DM for data quality improvement to support machine learning of stunting prediction in infants and toddlers*. 2021 8th International Conference on Advanced Informatics: Concepts, Theory and Applications (ICAICTA). Bandung, Indonesia.

- Putri, T. T., Sitepu, I. Y., Sihombing, M., & Silvi, S. (2019). Analysis and detection of hoax contents in Indonesian news based on machine learning. *Journal of Informatic Pelita Nusantara*, 4(1).
- Qureshi, K. A., Malick, R. A. S., Sabih, M., & Cherifi, H. (2021). Complex network and source inspired COVID-19 fake news classification on Twitter. *IEEE Access*, 9, 139636-139656. <https://doi.org/10.1109/ACCESS.2021.3119404>
- Rajapaksha, P., Farahbakhsh, R., & Crespi, N. (2021). Bert, xlnet or roberta: The best transfer learning model to detect clickbaits. *IEEE Access*, 9, 154704-154716. <https://doi.org/10.1109/ACCESS.2021.3128742>
- Ramaciotti Morales, P., Cointet, J. P., & Froio, C. (2022). Posters and protesters: The networked interplay between onsite participation and Facebook activity in the Yellow Vests movement in France. *Journal of Computational Social Science*, 1-29. <https://doi.org/10.1007/s42001-022-00163-x>
- Rawat, G., Pandey, T., Singh, T., Yadav, S., & Aggarwal, P. K. (2023, January 27-29). *Fake news detection using machine learning*. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). Greater Noida, India.
- Razali, M. S., Halin, A. A., Chow, Y. W., Norowi, N. M., & Doraisamy, S. (2022). Context-driven satire detection with deep learning. *IEEE Access*, 10, 78780-78787. <https://doi.org/10.1109/ACCESS.2022.3194119>
- Rhodes, S. C. (2022). Filter bubbles, echo chambers, and fake news: How social media conditions individuals to be less critical of political misinformation. *Political Communication*, 39(1), 1-22. <https://doi.org/10.1080/10584609.2021.1910887>
- Rogers, A., Kovaleva, O., & Rumshisky, A. (2021). A primer in BERTology: What we know about how BERT works. *Transactions of the Association for Computational Linguistics*, 8, 842-866. https://doi.org/10.1162/tacl_a_00349
- Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10, 65703-65727. <https://doi.org/10.1109/ACCESS.2022.3183083>
- Saltz, J. S. (2021, December 15-18). *CRISP-DM for data science: strengths, weaknesses and potential next steps*. 2021 IEEE International Conference on Big Data (Big Data). Orlando, FL, USA.

- Saquete, E., Tomás, D., Moreda, P., Martínez-Barco, P., & Palomar, M. (2020). Fighting post-truth using natural language processing: A review and open challenges. *Expert systems with applications*, *141*, 112943. <https://doi.org/10.1016/j.eswa.2019.112943>
- Sasahara, K., Chen, W., Peng, H., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2021). Social influence and unfollowing accelerate the emergence of echo chambers. *Journal of Computational Social Science*, *4*(1), 381-402. <https://doi.org/10.1007/s42001-020-00084-7>
- Savolainen, L., Trilling, D., & Liotsiou, D. (2020). Delighting and detesting engagement: Emotional politics of junk news. *Social Media+ Society*, *6*(4), 2056305120972037. <https://doi.org/10.1177/2056305120972037>
- Schröer, C., Kruse, F., & Gómez, J. M. (2021). A systematic literature review on applying CRISP-DM process model. *Procedia Computer Science*, *181*, 526-534. <https://doi.org/10.1016/j.procs.2021.01.199>
- Seattle Municipal Archives (n.d.). *World Trade Organization Protests in Seattle*. Retrieved _____ May., 05, 2022 from <https://www.seattle.gov/cityarchives/exhibits-and-education/digital-document-libraries/world-trade-organization-protests-in-seattle>.
- Seddari, N., Derhab, A., Belaoued, M., Halboob, W., Al-Muhtadi, J., & Bouras, A. (2022). A hybrid linguistic and knowledge-based analysis approach for fake news detection on social media. *IEEE Access*, *10*, 62097-62109. <https://doi.org/10.1109/ACCESS.2022.3181184>
- Seo, Y., Seo, D., & Jeong, C. S. (2018, October 28-31). *FaNDeR: fake news detection model using media reliability*. TENCON 2018 - 2018 IEEE Region 10 Conference. Jeju, Korea (South).
- Serrano-Puche, J. (2021). Digital disinformation and emotions: exploring the social risks of affective polarization. *International Review of Sociology*, *31*(2), 231-245. <https://doi.org/10.1080/03906701.2021.1947953>
- Shabani, S., & Sokhn, M. (2018, October 18-20). *Hybrid machine-crowd approach for fake news detection*. 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). Philadelphia, PA, USA.
- Shah, H. (2011, April 4-7). *Turing's misunderstood imitation game and IBM's Watson success*. In Keynote in 2nd Towards a Comprehensive Intelligence test (TCIT) symposium at AISB. York, UK.

- Shishah, W. (2022). JointBert for detecting Arabic fake news. *IEEE Access*, *10*, 71951-71960. <https://doi.org/10.1109/ACCESS.2022.3185083>
- Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2020). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(6), e1385. <https://doi.org/10.1002/widm.1385>
- Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake news detection on social media: A data mining perspective. *ACM SIGKDD Explorations Newsletter*, *19*(1), 22-36. <https://doi.org/10.1145/3137597.3137600>
- Silverman, C. (2016, November 17). *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook*. Retrieved May., 05, 2022 from <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.
- Simko, J., Racsko, P., Tomlein, M., Hanakova, M., Moro, R., & Bielikova, M. (2021). A study of fake news reading and annotating in social media context. *New Review of Hypermedia and Multimedia*, *27*(1-2), 97-127. <https://doi.org/10.1080/13614568.2021.1889691>
- Stahl, K. (2018). Fake news detection in social media. *California State University Stanislaus*, *6*, 4-15.
- Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics—Challenges in topic discovery, data collection, and data preparation. *International journal of information management*, *39*, 156-168. <https://doi.org/10.1016/j.ijinfomgt.2017.12.002>
- Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). Defining “fake news” A typology of scholarly definitions. *Digital journalism*, *6*(2), 137-153. <https://doi.org/10.1080/21670811.2017.1360143>
- Tavana, M., Shaabani, A., Raeesi Vanani, I., & Kumar Gangadhari, R. (2022). A review of digital transformation on supply chain process management using text mining. *Processes*, *10*(5), 842. <https://doi.org/10.3390/pr10050842>
- Thang, P. C., & Trang, T. T. N. (2023). The application of artificial intelligence technologies in social media to detect fake news: A systematic review. *Micro-Electronics and Telecommunication Engineering: Proceedings of 6th ICMETE 2022*, 251-261. https://doi.org/10.1007/978-981-19-9512-5_23

- Theonion (n.d.). Retrieved May., 25, 2020 from <https://www.theonion.com/>.
- Teyit (n.d.). Retrieved May., 25, 2020 from <https://teyit.org/>.
- Teyitet (n.d.). Retrieved May., 25, 2020 from <http://teyitet.net/>.
- Teyitet (2020, March 11). Retrieved Agu., 12, 2023 from <http://teyitet.azurewebsites.net/>.
- Toffler, A. (2022). *The third wave: The classic study of tomorrow*. Bantam.
- Tomaiuolo, M., Lombardo, G., Mordonini, M., Cagnoni, S., & Poggi, A. (2020). A survey on troll detection. *Future internet*, 12(2), 31. <https://doi.org/10.3390/fi12020031>
- Traylor, T., Straub, J., & Snell, N. (2019, January 30-February 1). *Classifying fake news articles using natural language processing to identify in-article attribution as a supervised learning estimator*. 2019 IEEE 13th International Conference on Semantic Computing (ICSC). Newport Beach, CA, USA.
- Tsao, S. F., Chen, H., Tisseverasinghe, T., Yang, Y., Li, L., & Butt, Z. A. (2021). What social media told us in the time of COVID-19: A scoping review. *The Lancet Digital Health*, 3(3), e175-e194. [https://doi.org/10.1016/S2589-7500\(20\)30315-0](https://doi.org/10.1016/S2589-7500(20)30315-0)
- Tsfati, Y., Boomgaarden, H. G., Strömbäck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. (2020). Causes and consequences of mainstream media dissemination of fake news: literature review and synthesis. *Annals of the International Communication Association*, 44(2), 157-173. <https://doi.org/10.1080/23808985.2020.1759443>
- Twitter (n.d.). Retrieved May., 25, 2020 from <https://twitter.com/> (x.com).
- Twitter API (2019, December 9). *@goksum1 user name*. Retrieved Nov., 15, 2020 from <https://developer.twitter.com/en/portal/products>.
- Unver, A. (2020). Fact-checkers and fact-checking in Turkey. *EDAM Research Reports*.
- Umer, M., Imtiaz, Z., Ullah, S., Mehmood, A., Choi, G. S., & On, B. W. (2020). Fake news stance detection using deep learning architecture (CNN-LSTM). *IEEE Access*, 8, 156695-156706. <https://doi.org/10.1109/ACCESS.2020.3019735>
- Van Dijk, J. (2016). *Ağ toplumu*. Epsilon Yayincilik Ltd. Sti.
- Venturini, T. (2019). From fake to junk news: The data politics of online virality. *Data Politics*, 123-144.

- Verma, P. K., Agrawal, P., Amorim, I., & Prodan, R. (2021). WELFake: word embedding over linguistic features for fake news detection. *IEEE Transactions on Computational Social Systems*, 8(4), 881-893. <https://doi.org/10.1109/TCSS.2021.3068519>
- Vijayan, R., & Mohler, G. (2018, October 1-3). *Forecasting retweet count during elections using graph convolution neural networks*. 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA). Turin, Italy.
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151. <https://doi.org/10.1126/science.aap9559>
- Walter, A., & Andersen Tuttle, K. (2023). All the president's media: How the traditional press responded to new communications technology adopted by US presidents. *American Journalism*, 40(1), 4-25. <https://doi.org/10.1080/08821127.2023.2165576>
- Walther, J. B., & Whitty, M. T. (2021). Language, psychology, and new new media: The hyperpersonal model of mediated communication at twenty-five years. *Journal of Language and Social Psychology*, 40(1), 120-135. <https://doi.org/10.1177/0261927X20967703>
- Wei, P., Wu, F., Sun, Y., Zhou, H., & Jing, X. Y. (2022). Modality and event adversarial networks for multi-modal fake news detection. *IEEE Signal Processing Letters*, 29, 1382-1386. <https://doi.org/10.1109/LSP.2022.3181893>
- Werner de Vargas, V., Schneider Aranda, J. A., dos Santos Costa, R., da Silva Pereira, P. R., & Victória Barbosa, J. L. (2023). Imbalanced data preprocessing techniques for machine learning: A systematic mapping study. *Knowledge and Information Systems*, 65(1), 31-57. <https://doi.org/10.1007/s10115-022-01772-8>
- WhatsApp (n.d.). Retrieved May., 25, 2020 from <https://web.whatsapp.com/>.
- Wirth, R., & Hipp, J. (2000, April 11-13). *CRISP-DM: Towards a standard process model for data mining*. Fourth International Conference on the Practical Application of Knowledge Discovery and Data Mining. Manchester, UK.

- Wolfsfeld, G., Segev, E., & Sheaffer, T. (2013). Social media and the Arab spring: Politics comes first. *The International Journal of Press/Politics*, 18(2), 115-137. <https://doi.org/10.1177/1940161212471716>
- Wordhippo (n.d.). Retrieved Dec., 15, 2019 from <https://www.wordhippo.com/>.
- World Health Organization (n.d.). *WHO Coronavirus (COVID-19) Dashboard*. Retrieved Apr., 10, 2020 from <https://covid19.who.int/>.
- World Health Organization (n.d.). *12 myths about COVID-19*. Retrieved Jun., 18, 2021 from [12myths-final099bfbf976c54d5fa3407a65b6d9fa9d.pdf](https://www.who.int/publications/m/item/12myths-final099bfbf976c54d5fa3407a65b6d9fa9d.pdf) (who.int).
- World Health Organization (n.d.). *Disinformation and public health*. Retrieved Feb., 06, 2024 from <https://www.who.int/news-room/questions-and-answers/item/disinformation-and-public-health>.
- Wu, L., Morstatter, F., Carley, K. M., & Liu, H. (2019). Misinformation in social media: definition, manipulation, and detection. *ACM SIGKDD explorations newsletter*, 21(2), 80-90. <https://doi.org/10.1145/3373464.3373475>
- Wu, W. T., Li, Y. J., Feng, A. Z., Li, L., Huang, T., Xu, A. D., & Lyu, J. (2021). Data mining in clinical big data: the frequently used databases, steps, and methodological models. *Military Medical Research*, 8, 1-12. <https://doi.org/10.1186/s40779-021-00338-z>
- Wu, Y., Fang, Y., Shang, S., Jin, J., Wei, L., & Wang, H. (2021). A novel framework for detecting social bots with deep neural networks and active learning. *Knowledge-Based Systems*, 211, 106525. <https://doi.org/10.1016/j.knsys.2020.106525>
- Wu, Z., Chen, Y., Kao, B., & Liu, Q. (2020). Perturbed masking: Parameter-free probing for analyzing and interpreting BERT. *arXiv preprint arXiv:2004.14786*. <https://doi.org/10.48550/arXiv.2004.14786>
- Xia, Z., Liu, C., Gong, N. Z., Li, Q., Cui, Y., & Song, D. (2019, August 4-8). *Characterizing and detecting malicious accounts in privacy-centric mobile social networks: a case study*. KDD '19: The 25th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Anchorage, AK, USA.

- Yang, X. (2021). Potential consequences of COVID-19 for sustainable meat consumption: the role of food safety concerns and responsibility attributions. *British food journal*, 123(2), 455-474. <https://doi.org/10.1108/BFJ-04-2020-0332>
- Yuan, J., & Yu, J. (2016, December 18-20). *Semi-supervised learning with bidirectional adaptive pairwise encoding*. 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). Anaheim, CA, USA.
- Yuliani, S. Y., Abdollah, M. F. B., Sahib, S., & Wijaya, Y. S. (2019). A framework for hoax news detection and analyzer used rule-based methods. *International Journal of Advanced Computer Science and Applications*, 10(10). <https://doi.org/10.14569/ijacsa.2019.0101055>
- Zhang, J., Li, Z., Pu, Z., & Xu, C. (2018). Comparing prediction performance for crash injury severity among various machine learning and statistical methods. *IEEE Access*, 6, 60079-60087. <https://doi.org/10.1109/ACCESS.2018.2874979>
- Zhang, X., & Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, 57(2), 102025. <https://doi.org/10.1016/j.ipm.2019.03.004>
- Zhou, X., & Zafarani, R. (2019). Network-based fake news detection: A pattern-driven approach. *ACM SIGKDD Explorations Newsletter*, 21(2), 48-60. <https://doi.org/10.1145/3373464.3373473>
- Zhou, Y. (2017). Clickbait detection in tweets using self-attentive network. *arXiv preprint arXiv:1710.05364*. <https://doi.org/10.48550/arXiv.1710.05364>
- Zinderen, İ. E. (2020). Yeni medya ekolojisi ekseninde YouTube: Türkiye örneği. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 24(1), 215-232.

APPENDICES**APPENDIX I: ETHICS APPROVAL**

13.04.2022

Dear Murat GÖKSU

Your application titled **“Detecting Fake News with Artificial Intelligence Tools based on Cloud Computing Systems with Text Mining in Online Social Networks”** with the application number NEU/AS/2022/155 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

Assoc. Prof. Dr. Direnç Kanol

Rapporteur of the Scientific Research Ethics Committee



Note: If you need to provide an official letter to an institution with the signature of the Head of NEU Scientific Research Ethics Committee, please apply to the secretariat of the ethics committee by showing this document.

APPENDIX II: SIMILARITY REPORT

AFTER DEFENCE			
ORIGINALITY REPORT			
19%	15%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	link.springer.com Internet Source	6%	
2	cdn.istanbul.edu.tr Internet Source	3%	
3	docs.neu.edu.tr Internet Source	1%	
4	www.researchgate.net Internet Source	1%	
5	Submitted to Sabanci Universitesi Student Paper	1%	
6	Patrick Ferrucci, Toby Hopp. "Let's intervene: How platforms can combine media literacy and self-efficacy to fight fake news", Communication and the Public, 2023 Publication	<1%	
7	Deepak P, Tanmoy Chakraborty, Cheng Long, Santhosh Kumar G. "Data Science for Fake News", Springer Science and Business Media LLC, 2021 Publication	<1%	

8	www.fsfv.ni.ac.rs Internet Source	<1 %
9	www.groundai.com Internet Source	<1 %
10	www.jatit.org Internet Source	<1 %
11	Submitted to Middle East Technical University Student Paper	<1 %
12	deepai.org Internet Source	<1 %
13	Submitted to Uczelnia Łazarskiego Student Paper	<1 %
14	Larisa Ismailova, Viacheslav Wolfengagen, Sergey Kosikov, Mikhail Maslov, Juliane Dohrn. "Semantic models to indicate post- truth with fake news channels", Procedia Computer Science, 2020 Publication	<1 %
15	Submitted to Istanbul Bilgi University Student Paper	<1 %
16	www.asjp.cerist.dz Internet Source	<1 %
17	idpr.org.uk Internet Source	<1 %
towardsdatascience.com		

18	Internet Source	<1 %
19	www.warse.org Internet Source	<1 %
20	Submitted to Teaching and Learning with Technology Student Paper	<1 %
21	Submitted to The University of Manchester Student Paper	<1 %
22	coek.info Internet Source	<1 %
23	Submitted to Flinders University Student Paper	<1 %
24	Hadad, Moshe םוֹסֶה הַדָּד, םוֹסֶה. "From Network Traffic Data to Event Log", University of Haifa (Israel), 2023 Publication	<1 %
25	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Student Paper	<1 %
26	www.pivony.com Internet Source	<1 %
27	eprints.bournemouth.ac.uk Internet Source	<1 %

28	Kai Shu, Huan Liu. "Detecting Fake News on Social Media", Springer Science and Business Media LLC, 2019 Publication	<1 %
29	Pires, Inês Tomás. "Customer Churn Prediction in Portuguese Banking Sector: Using a Machine Learning Approach", Universidade NOVA de Lisboa (Portugal), 2024 Publication	<1 %
30	Submitted to The Robert Gordon University Student Paper	<1 %
31	Submitted to Yakin Doğu Üniversitesi Student Paper	<1 %
32	Noureddine Seddari, Abdelouahid Derhab, Mohamed Belaoued, Waleed Halboob, Jalal Al-Muhtadi, Abdelghani Bouras. "A Hybrid Linguistic and Knowledge-Based Analysis Approach for Fake News Detection on Social Media", IEEE Access, 2022 Publication	<1 %
33	www.techtarget.com Internet Source	<1 %
34	Submitted to Liverpool John Moores University Student Paper	<1 %

35	"Advances in Multimedia Information Processing – PCM 2018", Springer Science and Business Media LLC, 2018	<1 %
Publication		
36	arifakyuz.com	<1 %
Internet Source		
37	Gülsüm KAYABAŞI KORU, Doç.Dr.Çelebi ULUYOL. "Fake News Detection in Turkish Using Machine Learning Algorithms and Fasttext With Word Embedding", Research Square Platform LLC, 2022	<1 %
Publication		
38	Submitted to University of Lugano	<1 %
Student Paper		
39	Submitted to University of Southampton	<1 %
Student Paper		
40	Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, Huan Liu. "Fake News Detection on Social Media", ACM SIGKDD Explorations Newsletter, 2017	<1 %
Publication		
41	Submitted to University of Alabama at Birmingham	<1 %
Student Paper		
42	ebin.pub	<1 %
Internet Source		

43	Alzahrani, Amani. "Misinformation Detection in the Social Media Era", Howard University, 2024 Publication	<1 %
44	mythdetector.ge Internet Source	<1 %
45	www.mdpi.com Internet Source	<1 %
46	Lingfei Qian, Ruipeng Xu, Zhipeng Zhou. "MRDCA: a multimodal approach for fine-grained fake news detection through integration of RoBERTa and DenseNet based upon fusion mechanism of co-attention", Annals of Operations Research, 2022 Publication	<1 %
47	Sonay Duman, Yagmur Aydin, Petek Bilim, Mehmet Ali Aktas. "Analysis of the Effects of Smoking Desire and Self-Efficacy on Nicotine Use Levels During the Covid-19 Pandemic Period Using Machine Learning Techniques", 2021 Innovations in Intelligent Systems and Applications Conference (ASYU), 2021 Publication	<1 %
48	cris.unibo.it Internet Source	<1 %
49	"Natural Language Processing and Chinese Computing", Springer Science and Business	<1 %

	Media LLC, 2019 Publication	
50	Submitted to University of Central Oklahoma Student Paper	<1 %
51	Submitted to Universität Liechtenstein Student Paper	<1 %
52	Yanis Labrak, Adrien Bazoge, Richard Dufour, Mickael Rouvier, Emmanuel Morin, Béatrice Daille, Pierre-Antoine Gourraud. "DrBERT: A Robust Pre-trained Model in French for Biomedical and Clinical domains", Cold Spring Harbor Laboratory, 2023 Publication	<1 %
53	www.aimspress.com Internet Source	<1 %
54	Biliaminu, Karamot Kehinde. "Using Multiple Instance Learning Techniques to Rank Maize Ears According to Their Traits", Universidade do Porto (Portugal), 2024 Publication	<1 %
55	Diptendu Sinha Roy, Mir Wajahat Hussain, K. Hemant Kumar Reddy, Deepak Gupta. "Healthcare-Driven Intelligent Computing Paradigms to Secure Futuristic Smart Cities", CRC Press, 2024 Publication	<1 %

- | | | |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| 56 | Lerina Aversano, Mario Luca Bernardi, Marta Cimitile, Martina Iammarino, Debora Montano. "Forecasting technical debt evolution in software systems: an empirical study", <i>Frontiers of Computer Science</i> , 2022
Publication | <1 % |
| 57 | Submitted to Istanbul Aydin University
Student Paper | <1 % |
| 58 | Submitted to University of Northumbria at Newcastle
Student Paper | <1 % |
| 59 | "Linking and Mining Heterogeneous and Multi-view Data", Springer Science and Business Media LLC, 2019
Publication | <1 % |
| 60 | Esma Aïmeur, Sabrine Amri, Gilles Brassard. "Fake news, disinformation and misinformation in social media: a review", <i>Social Network Analysis and Mining</i> , 2023
Publication | <1 % |
| 61 | Feyza Altunbey Ozbay, Bilal Alatas. "Fake news detection within online social media using supervised artificial intelligence algorithms", <i>Physica A: Statistical Mechanics and its Applications</i> , 2020
Publication | <1 % |
| 62 | Submitted to Istanbul Medeniyet Üniversitesi | |

	Student Paper	<1 %
63	Submitted to Lingnan University Student Paper	<1 %
64	Submitted to University of New Haven Student Paper	<1 %
65	Varalakshmi Konagala, Shahana Bano. "chapter 11 Fake News Detection Using Deep Learning", IGI Global, 2020 Publication	<1 %
66	www.coursehero.com Internet Source	<1 %
67	www.rankwise.net Internet Source	<1 %
68	Submitted to Cambridge Education Group Student Paper	<1 %
69	cse.iitkgp.ac.in Internet Source	<1 %
70	Submitted to Corvinus University of Budapest Student Paper	<1 %
71	Hawamdah, Luma M.. "From Hooks to Clicks: A Data-Driven Approach to Understanding Language Trends in Phishing Schemes Across Different Attack Vectors", The George Washington University, 2023 Publication	<1 %

72	"Computing and Network Sustainability", Springer Science and Business Media LLC, 2019 Publication	<1 %
73	Gc, Sunil. "Integrating High-Throughput Phenotyping, Robotic, and Artificial Intelligence Technologies in Weed Species Identification", North Dakota State University, 2023 Publication	<1 %
74	Submitted to University of North Texas Student Paper	<1 %
75	Submitted to University of Wales Institute, Cardiff Student Paper	<1 %
76	a.pr-cy.ru Internet Source	<1 %
77	docplayer.net Internet Source	<1 %
78	iacis.org Internet Source	<1 %
79	xteam.jaw.cz Internet Source	<1 %
80	"Disinformation, Misinformation, and Fake News in Social Media", Springer Science and Business Media LLC, 2020	<1 %

Publication		
81	Anat Toder Alon, Ilan Daniels Rahimi, Hila Tahar. "Fighting fake news on social media: a comparative evaluation of digital literacy interventions", <i>Current Psychology</i> , 2024 Publication	<1 %
82	Djaha Fodja, Christel Herlin. "The Effectiveness of Machine Learning Techniques in the Detection of Multi-Intrusion Attacks", <i>The George Washington University</i> , 2023 Publication	<1 %
83	Ferreira, Pedro Daniel Fernandes. "Improving Image Captioning Through Segmentation", <i>Universidade do Porto (Portugal)</i> , 2024 Publication	<1 %
84	Kweku-Muata Osei-Bryson, Corlane Barclay. "Knowledge Discovery Process and Methods to Enhance Organizational Performance", <i>Auerbach Publications</i> , 2019 Publication	<1 %
85	Rainer Greifeneder, Mariela E. Jaffé, Eryn J. Newman, Norbert Schwarz. "The Psychology of Fake News - Accepting, Sharing, and Correcting Misinformation", <i>Routledge</i> , 2020 Publication	<1 %
86	Saqib Hakak, Wajiha Shahid, Bahman Jamshidi, Wazir Zada Khan, Muhammad Khurram Khan, Haruna Isah. "Detecting and	<1 %

Mitigating the Dissemination of Fake News: Challenges and Future Research Opportunities", Institute of Electrical and Electronics Engineers (IEEE), 2022

Publication

87 Sarith Imaduwege, P.P.N.V. Kumara, W.J. Samaraweera. "Capturing Credibility of Users for an Efficient Propagation Network Based Fake News Detection", 2022 2nd International Conference on Computer, Control and Robotics (ICCCR), 2022

<1 %

Publication

88 Yin-Fu Huang, Po-Hong Chen. "Fake News Detection Using an Ensemble Learning Model Based on Self-adaptive Harmony Search Algorithms", Expert Systems with Applications, 2020

<1 %

Publication

89 detrterritorialinvestigations.files.wordpress.com

Internet Source

<1 %

90 discovery.ucl.ac.uk

Internet Source

<1 %

91 essay.utwente.nl

Internet Source

<1 %

92 ijsret.com

Internet Source

<1 %

libweb.kpfu.ru

93	Internet Source	<1 %
94	papyrus.bib.umontreal.ca Internet Source	<1 %
95	patents.justia.com Internet Source	<1 %
96	repository.tcu.edu Internet Source	<1 %
97	trepo.tuni.fi Internet Source	<1 %
98	turcomat.org Internet Source	<1 %
99	Debasish Patra, Biswapati Jana, Sourav Mandal, Arif Ahamed Sekh. "Chapter 21 Understanding Fake News Detection on Social Media: A Survey on Methodologies and Datasets", Springer Science and Business Media LLC, 2022 Publication	<1 %
100	Linda K. Cummins, Katharine V. Byers, Laura Pedrick. "Policy Practice for Social Workers - An Ethic of Care Approach", Routledge, 2023 Publication	<1 %
101	Barsha Pattanaik, Sourav Mandal, Rudra M. Tripathy. "A survey on rumor detection and prevention in social media using deep	<1 %

learning", Knowledge and Information Systems, 2023

Publication

-
- | | | |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 102 | Clemens, Erik. "Transfer Learning, Model Interpretation, and Dataset Bias Analysis for Automated Violence Detection from Video", Marquette University, 2023 | <1 % |
| <hr/> | | |
| 103 | Gulshan Shrivastava, Prabhat Kumar, Rudra Pratap Ojha, Pramod Kumar Srivastava, Senthilkumar Mohan, Gautam Srivastava. "Defensive Modeling of Fake News Through Online Social Networks", IEEE Transactions on Computational Social Systems, 2020 | <1 % |
| <hr/> | | |
| 104 | Sarthak Arora, Vallari Agrawal, Deepika Kumar, Sarvesh Arora, Sumit Kumar Banshal. "Sentimental impact of fake news on social media using an integrated ensemble framework", Social Network Analysis and Mining, 2024 | <1 % |
| <hr/> | | |
| 105 | Submitted to University of Houston System | <1 % |
-

Exclude quotes

On

Exclude matches

< 5 words

Publication

105 Submitted to University of Houston System <1 %
Student Paper

Exclude quotes On Exclude matches < 5 words

Exclude bibliography On

APPENDIX III: CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name : Goksu, Murat
 Nationality : Republic of Turkey
 Date and Place of Birth : 07 July 1974, Eskişehir
 Marital Status : Married
 Phone : +90 553 370 91 91
 e-mail : muratgoksu26@gmail.com
 ORCID İD : <https://orcid.org/my-orcid?orcid=0000-0002-9918-5732>
 ResearchGate : <https://www.researchgate.net/profile/Murat-Goeksu>
 Academia : <https://neu-tr.academia.edu/muratgoksu>
 GoogleScholar: <https://scholar.google.com/citations?user=pKoRAOQAAAAJ&hl=tr>
 DegiParkAkademik : https://dergipark.org.tr/tr/pub/@kara_murat
 TR Dizin : <https://yonetim.trdizin.gov.tr/#/author/detail/946692>
 Researcher ID : <https://www.webofscience.com/wos/author/record/HIR-7097-2022>



EDUCATION

Degree	Institution	Year of Graduation
Ph.D.	Near East University, Department of Computer Information Systems	2024
M.Sc.	Ahmet Yesevi University, Department of Management Information Systems	2014
B.Sc.	Anadolu University, Department of Economy, Economy	2007

WORK EXPERIENCE

Year	Place	Enrollment
September, 2023- March 2024	Bosnia and Herzegovina Turkish Representative Delegation Presidency, Liaison and Observation Team (LOT), Zenica/ Bosnia and Herzegovina	LOT Deputy Commander
October, 2022- January, 2023	3 rd NATO Rapid Deployable Corps Istanbul/Türkiye and NATO Joint Force Training Centre Bydgoszcz/Poland	Intelligence Plan Officer
2022-2024	CIS School and Training Center, CIS Training Regiment, Ankara/ TÜRKİYE	Chief of Operations, Training and Intelligence
2021-2022	Land Forces Logistics Command, Department of Operations and Administrative Management, Ankara/ TÜRKİYE	Executive-NCO
2020-2021	National Defence Ministry of Turkish Republic, Department of Communication and Information Systems (CIS), Digital Transformation (DTO) and Project Management Office (PMO), Ankara/ TÜRKİYE	DTO Expert and PMO Coordinator
2018-2020	TRNC Peace Corps, CIS Company, Girne/KKTC	CIS Centre Commander

2014-2018	Land Forces Command, Department of Communications Electronics and Information Systems (CEIS), Ankara/TÜRKİYE	CIS Analysis and Plan NCO
2009 -2014	Land Forces Command, CIS Battalion, Ankara/ TÜRKİYE	SatCom Team Leader
2007-2009	2 nd Motorized Infantry Brigade, CIS Company, Lice/Diyarbakır/ TÜRKİYE	RadCom Team Leader
2005-2007	66 th Mechanized Infantry Brigade (Peace Forces of NATO Rapid Forces), CIS Company, Topkule/Istanbul/ TÜRKİYE	RadCom Team Leader
1998-2005	102 nd Artillery Regiment, Keşan/Edirne	Meteo. Platoon Leader
1996-1998	9 th Infantry Division, 28 th Infantry Regiment, Sarıkamış/Kars/ TÜRKİYE	CIS Platoon Leader
1992-1996	172 nd Armored Brigade, Signal Company, Kahramanmaraş/ TÜRKİYE	CIS Platoon Leader

FOREIGN LANGUAGES

- Yökdil-Fen:76,25 (out of 100) (2024)
- YDS:72.5 (out of 100) (2023)

HONORS AND AWARDS

- *Honor, M.Sc.* (2014) – Ahmet Yesevi University, Faculty of Information Technologies and Engineering, Ankara (TURTEP), CGPA: 3.09 (out of 4.00).

- *ESDP Operation Althea Medal* – European Union Force in BiH, Bosan & Herzegovina. (Instituted in 2004, the European Security and Defence Policy (ESDP) Service Medal is awarded to military and civilian personnel involved in military operations or missions endorsed by the European Union.)

PUBLICATIONS IN INTERNATIONAL REFEREED JOURNALS (IN COVERAGE OF SSCI/SCI-EXPANDED, AHCI AND ESCI):

- Cavus, N., Goksu, M., and Oktekin, B. (2024). [Real-Time Fake News Detection in Online Social Networks: FANDC Cloud-Based system](https://doi.org/10.1038/s41598-024-76102-9), *Sci Rep* **14**, 25954 (2024). <https://doi.org/10.1038/s41598-024-76102-9>
- Goksu, M., Cavus, N., Cavus, A. & Karagozlu, D. (2020). [Fake News Detection on Social Networks with Cloud Computing: Advantages and Disadvantages](#). *International Journal of Advanced Science and Technology*, Vol. 29, No. 7, (2020), pp. 2137-2150, ISSN: 2005-4238 IJAST.

PUBLICATIONS IN INTERNATIONAL REFEREED JOURNALS (IN COVERAGE OF British Education Index, ERIC, Science Direct, Scopus, IEEE):

- Goksu, M. & Cavus, N. (2023). [Knowledge Management in the COVID-19 Period: Misinformation and Disinformation](https://doi.org/10.26650/B/ET07.2023.004.16). *Pandemics and the Critical Role of Knowledge Management*, İstanbul University Press, 14.02.2023. <https://doi.org/10.26650/B/ET07.2023.004.16>
- Goksu, M. & Cavus, N. (2020). [Fake News Detection on Social Networks with Artificial Intelligence Tools: Systematic Literature Review](#). In: Aliev R., Kacprzyk J., Pedrycz W., Jamshidi M., Babanli M., Sadikoglu F. (Eds) 10th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions- ICSCCW-2019. ICSCCW 2019. *Advances in Intelligent Systems and Computing* (vol. 1095, pp. 47-53). Springer, Cham. https://doi.org/10.1007/978-3-030-35249-3_5
- Goksu, M. & Cavus, N. (2019). [New technological trends in English language learning](#). In *the Proceedings of the 11th Annual International Conference on Education and New Learning Technologies (EDULEARN2019)* (pp. 6134-6139), 1-3 July, 2019,

Palma De Mallorca, Spain, <https://doi.org/10.21125/edulearn.2019.1477> (The paper indexed by Web of Science)

- Goksu, M. & Cavus, N. (2019). [The future of learning management systems in the context of Industry 4.0](#). *In the Proceedings of the 13th Annual International Technology, Education and Development Conference (INTED2019)* (pp. 5599-5605), 11-13 March, 2019, Valencia, Spain. <https://doi.org/10.21125/inted.2019.1376> (The paper indexed by Web of Science)

THESES

Ph.D.

- Goksu, M. (2024). *Real-Time Fake News Detection in Online Social Networks: FANDC Cloud-Based system*, Dissertation, Near East University, Graduate School of Applied Sciences, Department of Computer Information Systems, Nicosia, Cyprus.

Master

- Goksu, M. (2014). [Bilişsel Radyoların \(BR\) Bilişim Sistemleriyle Birlikte Kullanılması ve Karar Destek Sistemlerine Etkileri](#). (*Using Cognitive Radios (CR) with Information Systems and Effects on Decision Support Systems.*) Unpublished Master Thesis, Ahmet Yesevi University, Department of Management Information Systems, Ankara (TURTEP).

HOBBIES

- Reading, Swimming, Fitness, Running and Cooking.

OTHER INTERESTS

- Big Data, Data Science, Data Mining, Business Intelligence and Data Analytics, Text Mining, Social Networks, Cloud Computing, Machine Learning, Artificial Intelligence, Natural Language Processing, Large Language Models, Electronics and Communication, Knowledge Management and Knowledge Sociology.