Chapter 6
Social Media Privacy and Security:
Stacking and Boosting for Misinformation Detection

Sanaa Ashiq
https://orcid.org/0009-0008-0070-9403
National University of Modern Languages, Rawalpindi, Pakistan

Sehrish Ferdous
https://orcid.org/0009-0004-6495-9939
National University of Modern Languages, Rawalpindi, Pakistan

Muhammad Adnan
https://orcid.org/0009-0004-2537-0398
National University of Computer and Emerging Sciences (FAST), Islamabad, Pakistan

Wajahat Sultan
https://orcid.org/0009-0007-6271-7268
National University of Sciences and Technology, Pakistan

Hasan Tahir
https://orcid.org/0000-0002-0966-0721
National University of Sciences and Technology, Pakistan

Bilal Ahmed
https://orcid.org/0009-0006-8664-7463
National University of Sciences and Technology, Pakistan

Qamar Yasmeen
Niazi Medical and Dental College, Sargodha, Pakistan

Madeeha Saqib
https://orcid.org/0000-0003-4856-8095
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

ABSTRACT

Despite being a modern means of communication, social media is one of the biggest risks to privacy and security because of the misinformation that it perpetuates. This chapter proposes a new ensemble model that uses stacking and boosting techniques

DOI: 10.4018/979-8-3373-3171-3.ch006

for misinformation detection with identity protection. The developed framework combines machine learning and deep learning algorithms to improve detection accuracy while reducing the threat of fake news, identity fraud, and cyber terrorism. The chapter covers the implementation of natural language processing for feature extraction and model evaluation with real life datasets containing misinformation. It also addresses the policy and ethical consequences of automating misinformation detection from the perspective of safety, privacy, and freedom of speech. The resulting system encourages safety in a digital space by increasing privacy and surveillance of information among individuals and organizations, thus fostering trust in online content.

INTRODUCTION

Cybersecurity and privacy are key challenges of digital age and this chapter introduces the background, motivation, and significance of detecting misinformation in terms of social media privacy and security (Saeed, 2023, Saeed 2023a, Saeed, 2025). In the contemporary digital age, the internet has become the main medium whereby people receive news and information. Social media applications like Facebook, Twitter, Instagram, and YouTube have been central to this evolution. With increasingly busy lifestyles, consumers rely on online news and social media for quick and convenient sources of information. These websites are no longer limited to informal communication; instead, they play vital functions in areas like education, healthcare, business, and politics. For example, platforms like Facebook and Twitter are widely visited for numerous reasons like consumption of information, entertainment, e-commerce, and exchange of opinions (Ledford, 2020).

Despite the communication platforms, there are some other platforms to be popularly used as alternative search engines. For a lot of users, it is easier to navigate trending news or content of specific topics using social media instead of traditional search engines (Monti et al., 2019). Due to this, people are becoming more concerned about whether the information shared on social media is true and reliable. Misinformation simply defined as a false, misleading, or manipulated content, which can be spread either by mistake or on purpose. Sometimes misinformation can be spread on purpose to harm someone's reputation, influence elections, make money, or mislead the public (Garcia et al., 2020), (Brummette et al., 2018). Others might spread false information without knowing it, because of their personal opinions, lack of knowledge, or strong beliefs. The famous example is the 2016 US presidential election, where false information was shared on purpose to influence voters and change public opinion (Hakak et al., 2021).