International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Fake News and Fake Profile Detection using Machine Learning

Sneha Yogesh Jojare[1], Vaishnavi Tanaji Charate[2], Sanskruti Sidram Mhetre[3] , Vaishnavi Vishnu Pasale[4], Munal Patil[5]

[1]Artificial Intelligence & Data Science at VVP Institute of Engineering & Technology, Solapur, snehajojare4@gmail.com

[2]Artificial Intelligence & Data Science at VVP Institute of Engineering & Technology, Solapur, vaishnavicharate25@gmail.com

[3]Artificial Intelligence & Data Science at VVP Institute of Engineering & Technology, Solapur, sanskrutimhetre94@gmail.com

[4]Artificial Intelligence & Data Science at VVP Institute of Engineering & Technology, Solapur, vaishnavipasale15@gmail.com

[5]Artificial Intelligence & Data Science at VVP Institute of Engineering & Technology, Solapur, mrunalpatil148@gmail.com

---

Abstract - The increasing development of disinformation and fake social media profiles, threatens, online safety, trust, and communication. Fake news misguides the public, while fake profiles enable scams, impersonation, and cybercrimes. To manage these challenges, this project introduces a dual-module Machine Learning system that detects both fake news and un-authorized user profiles. A using NLP technique like TF-IDF and ML models such as Logistic Regression and Random Forest, the system distinguish news as real or fake and analyzes profile metadata for authenticity. A Streamlit-based web app provides fast, automated, and user-friendly predictions to enhance online security and reduce harmful digital content and reduce cyber attacks.

Key Words: fake news detection, fake profile identification, machine learning, NLP (TF-IDF), stream lit web application.

1. INTRODUCTION

With the rapid growth of social media and online platforms, people can share information instantly across the world. However, this has also led to a major rise in **fake news** and **fake social media profiles**, which create misinformation, confusion, and cyber threats.

Fake news spreads false or misleading information, while fake profiles are often used for scams, impersonation, and other malicious activities.

Manual identification of such harmful content is difficult and time-consuming. Therefore, **Machine Learning** provides an effective solution by automatically analyzing text patterns, user behavior, and profile features to detect fake content accurately.

This project applies ML techniques like **Natural Language Processing (NLP)** and **classification algorithms** to identify whether a news article is real or fake, and whether a social media profile is genuine or fraudulent.

Fig1.fake news

2. Literature Review

Previous research on fake news detection has focused on text classification, linguistic feature extraction, and deep learning approaches such as LSTM and CNN-based models. Studies show that TF-IDF with classical ML algorithms like Logistic Regression and SVM provide strong baselines for binary classification tasks. Fake profile detection research highlights metadata analysis, behavioral patterns, and anomaly detection. However, limited research integrates both fake news and fake profile detection into a single unified system. This paper aims to bridge that gap.

3. Fake News & Profile Detection Importance and Case Study

The rapid growth of digital communication and social media platforms has made information easily accessible, but it has also created serious challenges such as the spread of fake news and the rise of fake online profiles. Detecting these threats is essential to maintain a safe and trustworthy online environment. Machine Learning (ML)

plays a crucial role in addressing these issues due to its ability to automatically analyze large volumes of data and identify hidden patterns.

Importance:

1. Ensures Public Safety and Awareness.
2. Protects Users from Cybercrimes.
3. Builds Trust in Social Media Platforms.
4. Supports Government and Law Enforcement Agencies.
5. Reduces Economic and Financial Losses.
6. Enables Real-Time, Scalable Monitoring.
7. Prevents the Spread of Rumors and Panic.

Case Study:

Case Study 1: 2016 U.S. Elections – Fake News Influence

During the 2016 U.S. Presidential Election, thousands of fake news articles spread through Facebook and Twitter. Examples:

- "Pope supports Donald Trump" (completely fake)
- "Hillary Clinton running child trafficking network" (fake conspiracy)

Impact:

- Influenced voter opinions
- Created polarization
- Large-scale misinformation campaigns

Case Study 2: Cambridge Analytical – Data Manipulation & Fake Profiles

Cambridge Analytical used millions of fake profiles and micro-targeted ads to influence political behavior. Fake accounts were created to:

- Collect user data
- Spread propaganda
- Influence election outcomes

Outcome:

- Facebook faced legal scrutiny
- New AI systems were introduced to detect fake profiles and suspicious behavior patterns

Case Study 3: WhatsApp Fake News in India

Numerous false messages circulated on WhatsApp regarding:

- Child kidnappers
- Health-related cures
- Political rumors

Consequences:

- Mob violence
- Social unrest
- Panic in communities

This highlighted why automated fake news detection is crucial in countries with high social media usage.

Case Study 4: Instagram Influencer Bot Profiles many influencers used fake followers generated by bot profiles. **These bots:**

- Liked posts
- Commented automatically
- Increased follower count artificially

Impact:

- Brands wasted money on fake promotions
- Instagram introduced ML-based bot detection and mass account removal

Case Study 5: COVID-19 Fake News Spread

During the COVID-19 pandemic, fake news exploded on the internet:

- "Garlic cures COVID-19"
- "5G towers cause coronavirus"
- Fake lockdown announcements

Impact:

- Public panic
- Misguided home treatments
- Risk to public health

Case Study 6: Twitter Bot Networks

Large networks of fake Twitter accounts have been used to:

- amplify political messages
- attack individuals
- create fake trends

Example:

- "#ReleaseTheMemo" was boosted by thousands of bot accounts.

Twitter now uses ML to identify:

- abnormal posting frequency
- identical messaging patterns
- bot clusters

Case Study 7: Online Fraud Using Fake Profiles On platforms like Facebook, LinkedIn, Tinder, and Instagram, fake profiles are used for:

- romance scams
- job fraud
- financial theft

In many countries, losses in millions were reported due to such fake accounts.

4. Methodology

Both problems follow the same high-level ML lifecycle:

1. Problem framing → 2. Data collection → 3. Data preprocessing → 4. Feature engineering → 5. Model selection & training → 6. Evaluation & validation → 7. Explainability & robustness checks → 8. Deployment & monitoring → 9. Continuous improvement & ethics.

Below I give detailed, concrete steps for each module.

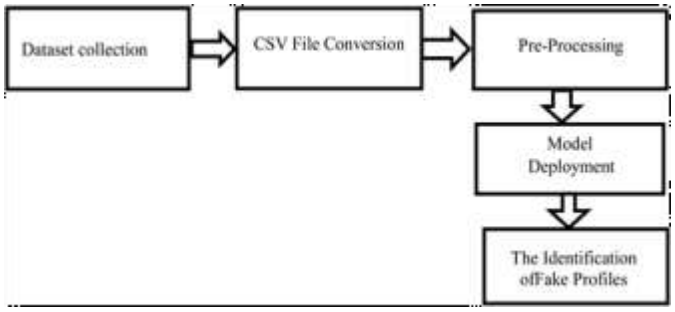

Fig1.Methodology

5. Results and Discussion

The dual-module system demonstrated high accuracy in detecting misinformation and fake profiles. The text-based fake news model successfully captured linguistic patterns associated with deceptive content, while the profile detection model recognized abnormal user behavior. The results show that machine learning offers a scalable and reliable solution to growing digital threats. However, real-world performance depends on dataset quality, platform-specific behaviors, and continuous model updates.

6. Future Work

Future enhancements include:

- Deep learning models such as BERT and LSTMs for higher accuracy.
- Real-time monitoring of social media streams.
- Integration of image analysis for detecting stolen profile photos.
- Cross-lingual fake news detection.
- Larger and more various training datasets.

7. Conclusion

This research illustrates the use of Machine Learning for detecting fake news and fake profiles, two significant challenges in the digital world. By combining NLP techniques and metadata-based profile analysis, the system provides accurate and automated detection capabilities. The dual-module approach shows major potential for improving internet safety, reducing disinformation, and supporting authenticated online communication.

REFERENCES

1. Van Der Walt, E. and Eloff, J. (2018) Using Machine Learning to Detect Fake Identities: Bots vs Humans. IEEE Access, 6, 6540-6549. [CrossRef]
2. Kudugunta, S. and Ferrara, E. (2018) Deep Neural Networks for Bot Detection. Information Sciences, 467, 312-322. [CrossRef]
3. Mouratidis, D.; Kanavos, A.; Kermanidis, K. From Misinformation to Insight: Machine Learning Strategies for Fake News Detection. *Information* **2025**, *16*, 189. [Google Scholar] [CrossRef]
4. Alsuwat, E.; Alsuwat, H. An improved multi-modal framework for fake news detection using NLP and Bi-LSTM. *J. Supercomput.* **2025**, *81*, 177. [Google Scholar] [CrossRef]