

# Sentiment Analysis for Detecting Scammer on Social Media: A Review

Nur Huda Jaafar<sup>1\*</sup>, Zuriati Ismail<sup>1</sup>, Mazlyda Abd Rahman<sup>1</sup>, Rashidah Mokhtar<sup>1</sup>

<sup>1</sup> College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Johor Branch, Segamat Campus, Malaysia

\*Corresponding Author: [nurhu378@uitm.edu.my](mailto:nurhu378@uitm.edu.my)

Received: 25 August 2023 | Accepted: 5 October 2023 | Published: 31 October 2023

DOI: <https://doi.org/10.55057/ijbtm.2023.5.3.57>

---

**Abstract:** *Nowadays, social media become a part of human daily routine. It is a common routine for people to share their activities, feelings and information using social media. They feel it is easy to connect using social media. This trend has become a daily routine for many people. This situation attracts scammers to find their victims on social media. Sentiment analysis is one method that can prevent scammers' activities by analysing text contents such as social media posts, reviews and comments. A few techniques can be considered for developing sentiment analysis. The data, environment and situation are elements that developers should study before deciding the techniques to be used for developing sentiment analysis.*

**Keywords:** Sentiment analysis, Scammers, Fraud, Scam, Social media

---

## 1. Introduction

Nowadays, social media platforms have become an integral part of our lives. Initially, social media was just a place for connecting with friends and family. However, when most people adopt activities on social media as a part of their lives, social media nowadays also become an advertising platform.

The growth of features in social media attracts scammers to use this platform to find their victims. They use various techniques, such as manipulating human emotions and leveraging psychological vulnerabilities to deceive their victims. Their actions cause their victims to experience various difficulties, such as loss of money and personal information.

Sentiment analysis is a technique in machine learning and natural language processing (NLP) that can be used to detect scammers on social media. It is the process of compiling and examining people's opinions, ideas, and impressions regarding various issues, goods, and services (Wankhade, Rao, & Kulkarni, 2022). By analysing the sentiments expressed in social media posts, comments, and messages, it is plausible for machine learning algorithms to detect dubious patterns. This detection mechanism encompasses the identification of accounts and content that embody characteristics consistent with those of a scammer. One study by Yue, Chen, Li, Zuo and Yin (2019) shows the effectiveness of sentiment analysis in detecting scams or fake information on social media platforms. For example, from a commercial perspective, sentiment analysis can assist customers and merchants in analysing products and services online.

However, the techniques for developing sentiment analysis should be studied to ensure that the sentiment analysis will work correctly. So, in this paper, we will show a few techniques used by developers for developing sentiment analysis on social media. This paper will also discuss the reason social media has become a target medium among scammers and the uses of sentiment analysis on social media.

## **2. Social Media as Target Medium of Scammer**

Most people nowadays have at least one account on social media. Socialising on social media can be considered a part of a human daily routine. This lifestyle is one of the reasons why social media become a target medium for scammers (Tambe Ebot, Siponen, & Topalli, 2023). The expansive scope of users and the interrelated structure of these platforms furnish fraudsters with abundant prospects to manipulate unassuming individuals. Scammers leverage the innate susceptibilities that social media interactions present, utilising diverse stratagems to mislead and trick their targets.

A study from Bharne and Bhaladhare (2023) found that the increasing reliance on social media among their users, whether for communication, information sharing, and online transactions, has been attractive for scammers to use social media as their target medium. These platforms offer a sense of anonymity and distance, making it easier for scammers to hide their true identities and intentions. Moreover, the proliferation of social media and the open nature of social media characteristics have provided scammers with many potential victims.

The scammers expert in manipulating human emotions, use psychological vulnerabilities to gain trust and deceive their victims (Hussain, Siddiqui, & Islam, 2023). They often create fake profiles, impersonating trusted individuals or organisations to deceive victims. Whether the victims are deceived through impersonation, phishing, or fraudulent schemes, the scammers' activities cause the victims to face financial loss, emotional distress and erode trust in online interactions.

To combat this issue, proactive actions must be taken to avoid the increasing number of victims. The capability of sentiment analysis techniques can be used as a one strategy to combat this issue. By analysing the sentiments expressed in social media posts, comments and messages, machine learning algorithms can identify suspicious patterns and flag accounts and content that exhibit characteristics consistent with scammer behaviour.

## **3. Sentiment Analysis and its Roles in Social Media**

Sentiment analysis is a potent strategy utilised to analyse and extract subjective data from textual information, encompassing social media posts, comments, reviews, and messages (Nandwani & Verma, 2021). Its primary objective is to identify the sentiment or emotional tone behind a given text, be it positive, negative, or neutral. With the fast growth of social media platforms and the sheer abundance of user-generated content, sentiment analysis has increasingly accrued value in comprehending the public's opinions, attitudes, and trends.

One of the foremost applications of sentiment analysis in social media concerns monitoring brands and managing reputation (Sheng, Amankwah-Amoah, Wang, & Khan, 2019). Corporations and organisations can employ sentiment analysis to evaluate the perceptions surrounding their brand, products, or services. By analysing content generated by social media users, such as tweets, Facebook posts, and online reviews, commercial entities can acquire

valuable insights into customer satisfaction, identify potential issues or concerns, and make informed decisions to improve their brand image and customer experience.

Sentiment analysis plays a pivotal role in monitoring social media for public opinion analysis (Sainger, 2021). Political campaigns, public figures, and governments use sentiment analysis to evaluate public sentiment and gauge sentiment trends regarding particular topics, policies, or events. The acquisition of such information can enhance comprehension of public sentiment, facilitate the prediction of shifts in public opinion, and ultimately influence communication strategies.

The sentiment analysis is not only limited to analysing public opinion and brands. It is also used widely for service sectors such as hotels, healthcare, education and tourism ((Akkaya & İlhan, 2021; AL-Bakri, Yonan, Sadiq, & Abid, 2021; Pham et al., 2020). Using sentiment analysis in various sectors shows that this technique brings many benefits to social media users. The open nature of social media that attracts irresponsible people to activities such as spreading fake information and online scams can be identified using sentiment analysis.

#### 4. Techniques of Sentiment Analysis to Identify Scammers

Sentiment analysis is well-known as a technique to analyse subjective data from textual information such as social media posts, comments, and reviews. A few techniques may be needed to develop sentiment analysis for detecting scammers. Table 1 shows a few techniques used by researchers to develop sentiment analysis in their study.

**Table 1: A Few techniques Used by Researcher for Developing Sentiment Analysis**

Researcher	Research Topic	Technique
Habib, 2021	Sentiment analysis of user tweet	Deep learning, Long-Short Term Memory
Alghamdi & Alharby, 2019	Detecting online recruitment fraud	Random Forest, Support Vector Machine
Sadi, Pk, & Zeki, 2021	Detecting scams on social media	Naïve Bayes, Support Vector Machine
Sureshbhai, Bhattacharya, & Tanwar, 2020	A blockchain-based sentiment analysis framework for fraud cryptocurrency schemes	Classification Scores, Long-Short Term Memory
Li, 2022	E-Commerce fraud detection model	Big Data Mining, Information Fusion Technology, Support Vector Machine, Logistic Regression Model
Pillai, 2023	Detecting fake job posting	Bidirectional Long-Short Term Memory

Habib (2021) in his study proposes a hybrid deep-learning model for sentiment analysis of user tweets. This study applies Long-Short Term Memory (LSTM) with various word embedding strategies to detect positive or negative sentences. The deep learning algorithms were trained using training data and then evaluated on the test data of the existing Kaggle dataset previously released for sentiment analysis.

Alghamdi and Alharby (2019) develop an intelligent model for online recruitment fraud detection. They used Random Forest and Support Vector Machine in their study. The model

uses the Support Vector Machine method for feature selection and Random Forest for classification and detection. The Employment Scam Aegean Dataset is used in this study. The main features and important factors in detection include a company profile feature, a company logo feature, and an industry feature, which were also considered during this project's development.

Sadi et al. (2021) developed a machine-learning model for detecting scams on Twitter. They use Naïve Bayes and Support Vector Machine in their study. The implementation of these techniques achieved a high accuracy rate in detecting tweet scam threats.

Sureshbhai et al. (2020) propose a decentralised framework called KaRuNa, a blockchain-based sentiment analysis framework for fraud cryptocurrency schemes. This framework operates on a public blockchain with three phases of trust modelling among stakeholders. In the first phase, transactions on the blockchain offer trust, auditability, and transparency among stakeholders. In the second phase, sentiment analysis (SA) of cryptocurrencies is proposed based on a novel algorithm of hash addresses to generate classification scores (CS). Parameters like social trends, rise/fall in cryptocurrency price, measured standard deviation, peak and low are selected to be fed to the proposed novel Long-short term memory (LSTM) classifier to generate recommendations based on CS.

Li (2022) apply big data mining, information fusion technology and Support Vector Machine to develop an e-commerce fraud detection model. The samples have been divided into nonfraud and fraud based on fraud attributes. He also uses the logistic regression (LR) model to find risk factors for particular situations, predict the probability of certain conditions under different independent variables, and judge.

Pillai (2023) propose a methodology for detecting fake job posting using Bidirectional Long-Short Term Memory. The authors employed a Bidirectional Long Short-Term Memory (Bi-LSTM) model to identify fake job advertisements. The model considers numeric and text features, effectively capturing the underlying patterns and relationships within the data.

## 5. Conclusion

Social media is a famous platform for people to connect. People easily share their feelings, activities, and information through social media. The open nature of social media attracts scammers to find their victims on social media. The scammers' activities should be prevented to prevent the number of victims from increasing. Sentiment analysis is a technique that can help people detect scammers on social media. However, knowing the techniques to develop efficient sentiment analysis is crucial. The environment, situation, and data are examples of elements that should be considered when determining the techniques that should be applied for developing sentiment analysis.

## References

- Akkaya, A., & İlhan, N. (2021). Sentiment Analysis of the Coronavirus Vaccine on Social Media. 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 295–299. <https://doi.org/10.1109/ISMSIT52890.2021.9604753>
- AL-Bakri, N. F., Yonan, J. F., Sadiq, A. T., & Abid, A. S. (2021). Tourism Companies Assessment via Social Media Using Sentiment Analysis. *Baghdad Science Journal*,

- 19(2), 422–429. <https://doi.org/http://dx.doi.org/10.21123/bsj.2022.19.2.0422>
- Alghamdi, B., & Alharby, F. (2019). Journal of Information Security. *Journal of Information Security*, 10, 155–176. <https://doi.org/https://doi.org/10.4236/jis.2019.103009>
- Bharne, S., & Bhaladhare, P. (2023). *Comprehensive Analysis of Online Social Network Frauds BT - Advances in Data-Driven Computing and Intelligent Systems* (S. Das, S. Saha, C. A. Coello Coello, & J. C. Bansal, eds.). Singapore: Springer Nature Singapore.
- Habib, M. A. (2021). Tweet Sentiment Analysis using Deep Learning Technique. *International Journal of Information Technology and Electrical Engineering*, 10(5), 27–36.
- Hussain, M., Siddiqui, S., & Islam, N. (2023). Social Engineering and Data Privacy. In A. Naim, P. K. Malik, & F. A. Zaidi (Eds.), *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses* (pp. 225–248). <https://doi.org/10.4018/978-1-6684-6581-3>
- Li, J. (2022). E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining. *Computational Intelligence and Neuroscience*, 1–9. <https://doi.org/https://doi.org/10.1155/2022/8783783>
- Nandwani, P., & Verma, R. (2021). A review on sentiment analysis and emotion detection from text. *Social Network Analysis and Mining*, 11(1), 81. <https://doi.org/10.1007/s13278-021-00776-6>
- Pham, T. D., Vo, D., Li, F., Baker, K., Han, B., Lindsay, L., ... Rowley, R. (2020). Natural Language Processing for Analysis of Student Online Sentiment in a Postgraduate Program. *Pacific Journal of Technology Enhanced Learning*, 2(2), 15–30. <https://doi.org/10.24135/pjtel.v2i2.4>
- Pillai, A. S. (2023). Detecting Fake Job Postings Using Bidirectional LSTM. *International Research Journal of Modernization in Engineering Technology and Science*, 5(3), 3883–3890. <https://doi.org/https://www.doi.org/10.56726/IRJMETS35202>
- Sadi, S. H., Pk, M. R. H., & Zeki, A. M. (2021). Threat Detector for Social Media Using Text Analysis. *International Journal on Perceptive and Cognitive Computing*, 7(1), 113–117.
- Sainger, G. (2021). Sentiment Analysis-An Assessment of Online Public Opinion: A Conceptual Review. *Turkish Journal of Computer and Mathematics Education*, 12(5), 1881–1887.
- Sheng, J., Amankwah-Amoah, J., Wang, X., & Khan, Z. (2019). Managerial Responses to Online Reviews: A Text Analytics Approach. *British Journal of Management*, 30(2), 315–327. <https://doi.org/https://doi.org/10.1111/1467-8551.12329>
- Sureshbhai, P. N., Bhattacharya, P., & Tanwar, S. (2020). KaRuNa: A Blockchain-Based Sentiment Analysis Framework for Fraud Cryptocurrency Schemes. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–6. <https://doi.org/10.1109/ICCWorkshops49005.2020.9145151>
- Tambe Ebot, A. C., Siponen, M., & Topalli, V. (2023). Towards a cybercontextual transmission model for online scamming. *European Journal of Information Systems*, 1–26. <https://doi.org/10.1080/0960085X.2023.2210772>
- Wankhade, M., Rao, A. C. S., & Kulkarni, C. (2022). A survey on sentiment analysis methods, applications, and challenges. *Artificial Intelligence Review*, 55(7), 5731–5780. <https://doi.org/10.1007/s10462-022-10144-1>
- Yue, L., Chen, W., Li, X., Zuo, W., & Yin, M. (2019). A survey of sentiment analysis in social media. *Knowledge and Information Systems*, 60(2), 617–663. <https://doi.org/10.1007/s10115-018-1236-4>