International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Social Media Fraud: Identifying Fake Engagement and its Impact on Digital Marketing

Diptika Raju Shripad[1], Mr. S.S. Bhide[2]

[1]PG Student, MCA Department, PES's Modern College of Engineering, Pune, Maharashtra, India
[2]Assistant Professor, MCA Department, PES's Modern College of Engineering, Pune, Maharashtra, India

Abstract
Social media has transformed digital marketing by enabling businesses to engage with audiences in real time. However, the rise of fake engagement fraud, including artificially inflated likes, followers, and comments, has created significant challenges for brands, advertisers, and consumers. Social Media Marketing (SMM) panels offer fraudulent services that manipulate engagement metrics, leading to misleading marketing insights and financial losses. This paper explores various social media fraud techniques, such as phishing, cloned accounts, investment fraud, cyberbullying, cyberstalking, dating scams, online shopping fraud, and spamming, highlighting their impact on brand credibility and user trust. Additionally, the study examines machine learning-based fraud detection techniques, including supervised and unsupervised models for identifying fake interactions. By understanding these fraudulent activities and developing robust detection mechanisms, businesses can safeguard their marketing investments and ensure authentic audience engagement.

Keywords: Fake engagement, Influencer Fraud, Digital Marketing, Social Media Bots, ROI Loss, Brand Fraud Detection.

1. Introduction

With the increasing dependence on social media for business growth and brand promotion, platforms such as Instagram, YouTube, and Facebook have become primary targets for fake engagement fraud. Fraudulent activities, including purchased likes, fake followers, and manipulated views, distort key marketing metrics, leading to misleading performance evaluations and inefficient ad spending. The widespread availability of SMM panels has further enabled businesses, influencers, and scammers to exploit engagement metrics for personal and financial gains.

This paper explores the different types of social media fraud and their impact on digital marketing. It also investigates machine learning-based fraud detection methods used to counter these deceptive practices. By analyzing fraudulent engagement trends and detection techniques, this research aims to provide insights into protecting brands from manipulation, ensuring data integrity, and promoting authentic user interactions on social media platforms.

2. Literature Survey

The literature survey focuses on documented fake engagement fraud and its impact on brands. In these real-world instances, social media metrics were abused, and brands became victims of deception by influ-

encers who provided tampered engagement figures.

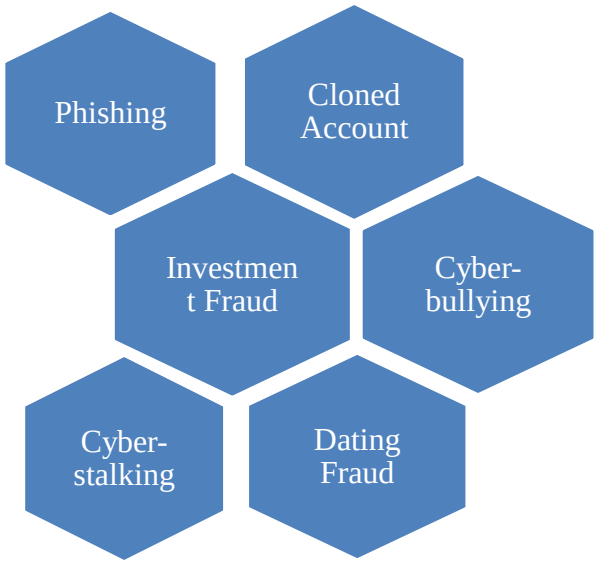
2.1 Social Media Frauds

Social media has become an essential part of our daily lives, helping people stay connected with loved ones, especially those living overseas. It allows us to make new friends, shop for products, share information, and so much more. However, along with these benefits come significant risks. The rapid expansion of social networking sites has also created opportunities for criminals and cybercriminals to carry out illegal activities.

One major concern is the presence of fake accounts and the spread of misinformation. Many fraudulent profiles are created for various purposes, such as manipulating public opinion, influencing financial markets, or spreading false rumours that can impact society on a large scale. As social media continues to grow, tackling these issues becomes increasingly important to ensure a safer online environment for everyone. [2][3]

2.1.1 Types of Fraud

Figure 1 Different Types of Fraud



1. Phishing: Phishing is a form of social engineering attack in which cybercriminals steal and misuse individuals' confidential information. This type of fraud often results in serious consequences like identity theft, email spoofing, and financial loss. Online Social Networks (OSNs) have become a common platform for phishing activities, creating major risks to users' financial safety and digital trust. Research shows that approximately 22% of phishing scams are targeted specifically at Facebook users. Cyber attackers employ several methods to conduct phishing, including the use of social media platforms, SMS (Short Message Service), instant messaging apps, and blogs. Common phishing techniques involve crafting fake URLs, disguising malicious links as trustworthy ones, and creating fraudulent user profiles to trick victims. To defend against phishing, various technical solutions have been introduced, such as machine learning-based URL detection, search engine content filtering, and similarity analysis tools designed to identify and block deceptive activities.[4][5][6]

2. Cloned Accounts: A cloned account attack occurs when an individual replicates an existing user's profile on the same or a different social media platform. The attacker uses this duplicate profile to send friend requests to the original user's contacts, gaining their trust. Once connected, the attacker may exploit

this trust to engage in activities such as cyberbullying, cyberstalking, or blackmail. By accessing private details from the victim's contacts, they can manipulate or misuse sensitive information. This fraudulent profile is typically created using the real user's photos and publicly available personal details.[7][8][9]

3. Investment Fraud: Investment fraud occurs when scammers promote seemingly lucrative opportunities, often using fabricated news articles and advertisements to appear credible. Common types of fraud on online social networks (OSN) include cryptocurrency scams, fake investment offers, and fraudulent celebrity endorsements. In these schemes, fraudsters pose as financial experts or stock traders, reaching out to individuals through OSN to offer deceptive financial advice. To enhance their credibility, they may also impersonate well-known investment firms or financial institutions.[15][16]

4. Cyberbullying: Cyberbullying is a form of online harassment that instils fear and emotional distress in victims through deceptive, harmful, or unwanted interactions on digital platforms. It often involves public shaming, malicious intent, and threats. Perpetrators may send threatening messages, make inappropriate or offensive remarks, spread false rumours, or share embarrassing photos or videos without consent. In some cases, they may even expose personal and humiliating information about the victim to harm their reputation. One of the challenges with cyberbullying is that it is difficult to interpret the sender's tone through text messages, emails, or instant messages. However, repeated patterns of harmful messages, social media comments, or emails are rarely accidental, making it clear that cyberbullying is an intentional act of harassment.[7][9][10]

5. Cyberstalking: Cyberstalking refers to the act of tracking or keeping an eye on someone through the internet, emails, or other digital channels, often leading to fear and emotional distress. It violates an individual's privacy and can severely impact their sense of security. Fraudulent users may misuse publicly available information from genuine users' online profiles to intimidate or harass them. This form of digital harassment can cause victims to feel unsafe, anxious, and mentally disturbed. In many cases, individuals unknowingly share personal details such as phone numbers, home addresses, workplace information, or real-time locations on social media platforms. If not adequately protected, this data can be exploited by cyberstalks, increasing the risk of online harassment.[10][11]

6. Dating fraud: Dating fraud is a form of online deception that commonly occurs on dating websites and applications. It involves scammers creating fake identities to establish relationships with unsuspecting individuals, with the goal of gaining personal information or financial benefits. These fraudsters exploit emotions by pretending to form genuine connections, manipulating victims into trusting them. The rise of social networking platforms and dating apps has made it easier for such criminals to find and approach potential targets. Popular dating platforms like Facebook Dating, Tinder, Bumble, and OKCupid have millions of users, making them attractive targets for fraudsters. While financial loss is a frequent outcome of dating scams, the emotional damage suffered by victims is often even more distressing. In many cases, scammers create fake profiles with attractive images to lure users, and some schemes specifically target individuals based on their sexual orientation through misleading profiles.[12][13]

7. Online Shopping Fraud: Cybercriminals increasingly use social media platforms such as Facebook and Twitter to set up fake online stores. These fraudulent shops often sell counterfeit or low-quality versions of popular designer brands. Typically, these stores operate for a short time, making quick sales before shutting down and disappearing without a trace. Even when an online store is widely promoted or shared across social media networks, it does not guarantee its authenticity. To protect themselves from such scams, customers are advised to thoroughly research the store's reputation, especially by reviewing feedback and ratings from previous buyers before making any purchases.[17]

8. Spamming: Spam often includes misleading or irrelevant information designed to deceive people. On the internet, distinguishing between genuine and spam messages can be challenging. Cybercriminals commonly spread spam to reach a large audience, sometimes with the intent of stealing personal information. Since spam messages can closely resemble legitimate ones, identifying them requires caution.[14]

3. Methodology

This research follows a qualitative approach to study the problem of social media fraud and its effect on digital marketing. It is mainly based on reviewing and analyzing information that already exists in research papers, case studies, reports, and trusted online sources.

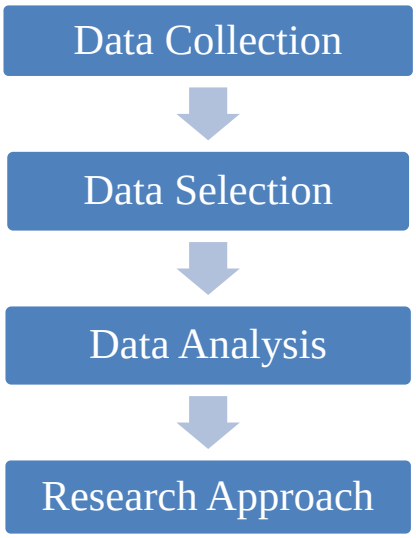


Figure 2 Methodology Process

1. Data Collection: This research relies entirely on secondary data sources. Information was gathered by reviewing academic journals, industry whitepapers, case analyses, and trusted web publications. Searches were conducted through academic databases such as Google Scholar, ResearchGate, and IEEE Xplore. Specific keywords like "social media fraud," "fake engagement," "influencer manipulation," and "fraud detection technologies" were used to locate credible and informative resources.

2. Data Selection: While gathering materials, careful selection criteria were applied to ensure that only authentic, up-to-date, and highly relevant sources were included. Preference was given to studies focusing on different forms of fake engagement, such as artificially inflated likes, followers, and comments. Particular attention was paid to research that examined how fake engagement impacts brand reputation, marketing effectiveness, and return on investment (ROI). Real-world case studies involving brands and influencers engaged in fraudulent practices were also reviewed to bring practical perspectives to the analysis.

3. Data Analysis: The collected data was systematically examined to identify recurring patterns, emerging challenges, and key trends associated with social media fraud. The analysis explored the mechanisms by which fraudulent engagement is created, the contribution of Social Media Marketing (SMM) panels to this issue, and the ways these activities damage digital marketing efforts. Furthermore, machine learning-based fraud detection techniques were assessed to understand their effectiveness in identifying fake engagement.

A comparative method was employed to distinguish between different types of fraudulent behavior and to evaluate various detection strategies.

4. Research Approach: A qualitative descriptive research approach was adopted for this study. Rather than relying on complex numerical or statistical analysis, the focus remained on understanding the behaviours, consequences, and underlying practices of social media fraud. The main goal was to provide a clear and comprehensive explanation of how fake engagement occurs, its effects on marketing campaigns and brand trust, and the strategies available to detect and combat such fraudulent activities.

4. Fraud Detection Methods based on Machine Learning

Several advanced machine learning algorithms are widely used to identify fake engagement in social media platforms. This section explores some of the most effective methods.

1. Iterative Attribute Clustering: This method helps to detect Cloned Accounts. Profile cloning detection in Online Social Networks (OSNs) can be effectively addressed using clustering algorithms such as the IAC (Iterative Attribute Clustering) algorithm. User profile information, including name, gender, education, location, active friends, page likers, and URLs, plays a crucial role in identifying cloned profiles. Research utilizing Facebook datasets [18] has demonstrated a three-component approach consisting of a profile verifier, profile hunter, and information distiller to detect and analyze cloned profiles. Similarly, studies leveraging LinkedIn datasets [20] have employed binary classifiers to detect profile cloning by analyzing profile similarities, friend lists, and friend request patterns. A synthetic dataset containing 2,000 user profiles [19] has also been used to evaluate the effectiveness of these detection methods. By combining profile similarity metrics with advanced clustering techniques, these approaches enhance the identification of fraudulent accounts, thereby improving the security of OSN platforms.

2. Bayes Trees and K-Nearest Neighbour (KNN): Spamming detection in Online Social Networks (OSNs) is effectively tackled using supervised, unsupervised, and semi-supervised machine learning algorithms. Various user profile features, including name, location, description, and content-based features such as user posts, comments, and likes, are analyzed to detect spam activity. Research utilizing Twitter datasets [14] has employed Support Vector Machines (SVM) and Random Forest classifiers, leveraging outlier standard scores and text content-based features for spam detection. Additionally, studies using both Twitter and Weibo datasets [22] have explored machine learning techniques such as Random Forest, Bayes Trees, and K-Nearest Neighbour (KNN) to enhance classification accuracy. Another approach involves analyzing user-based features, including account details, number of followers, number of followings, and number of lists, as demonstrated in research based on a Twitter dataset [23]. By integrating these machine learning techniques, OSN platforms can improve spam detection, ensuring a more secure and reliable user experience.

3. Random Forest, Support Vector Machines (SVM), and Logistic Regression: E-commerce fraud detection relies on advanced machine learning techniques such as Random Forest, Support Vector Machines (SVM), and Logistic Regression to identify fraudulent transactions. Key features used in fraud detection include transaction time, amount, and location, which help in distinguishing between legitimate and suspicious activities. Research utilizing the University of Brussels dataset [23] has demonstrated the effectiveness of these models in detecting anomalies in transaction patterns. Additionally, AdaBoost, when combined with multiple machine learning models, enhances fraud detection accuracy by leveraging a dataset with 28 numerical features, including user details, card information, transaction time, and amount. Kaggle [24] also provides extensive datasets for training and evaluating fraud detection models. By

integrating these machine learning approaches, e-commerce platforms can improve fraud detection mechanisms, reducing financial losses and ensuring secure transactions.

4. Random Forest, SVM, and Logistic Regression: Investment fraud detection employs machine learning techniques to recognize fraudulent activities and minimize financial risks. Supervised learning models, including Random Forest, Support Vector Machines (SVM), and Logistic Regression, examine key transactional attributes such as investment amounts, transaction patterns, and investor profiles to differentiate between genuine and fraudulent activities [25]. Unsupervised methods, such as Isolation Forest, identify irregularities in financial transactions without relying on labelled data [26]. Additionally, ensemble learning methods like AdaBoost and Gradient Boosting enhance fraud detection accuracy by integrating multiple classifiers [27]. These models utilize datasets such as the University of Brussels financial fraud dataset and the SEC fraud detection dataset [28]. By adopting these machine learning approaches, financial institutions can strengthen fraud detection mechanisms and provide better protection against fraudulent investment schemes.

5. CNN-LSTM: Phishing detection has been enhanced using the CNN-LSTM algorithm, which analyses various features such as URL characteristics, statistical webpage data, and webpage text content. This machine learning approach helps in accurately identifying fraudulent websites by distinguishing between legitimate and malicious URLs. The model has been trained using datasets from the PhishTank website, which provides a comprehensive collection of phishing data for improved detection accuracy [5].

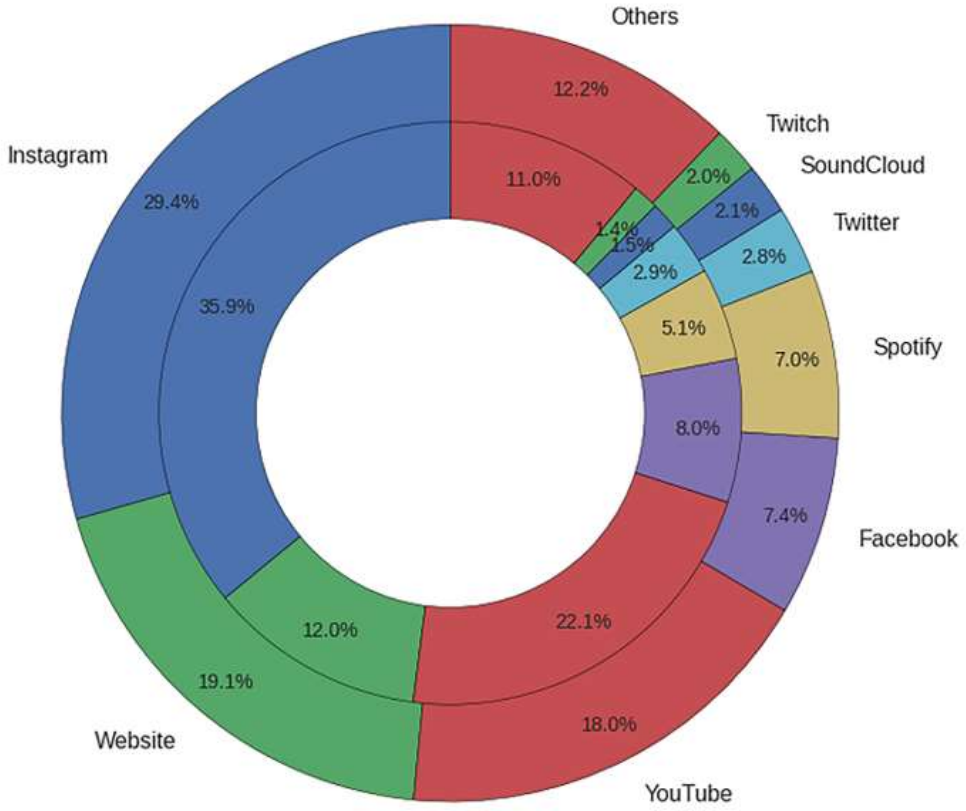
6. Deep neural network-based models: Cyberbullying detection has been advanced through deep neural network-based models that analyze text semantic features and initial word embeddings. These models are trained to recognize harmful language and patterns associated with cyberbullying, using datasets from platforms such as Formspring, a Q&A forum, and Wikipedia talk pages [29]. Additionally, transfer learning techniques utilizing deep neural networks have been employed to improve detection accuracy. These methods consider various factors, including post content, classification labels, text length, maximum word length, vocabulary size, and similar words. Extensive datasets, including 12,000 posts from Formspring, 16,000 posts from Twitter, and 100,000 posts from Wikipedia, have been used to enhance the effectiveness of cyberbullying detection models [30].

7. Naïve Bayes: Dating fraud detection utilizes machine learning techniques such as Naïve Bayes and Support Vector Machines (SVM) to identify fraudulent user profiles and suspicious activities on dating platforms. Key features for detecting fraud include user profile attributes, HTML text extraction, and text-based classification from web pages. Research based on datasets from dating sites [31] has demonstrated the effectiveness of SVM in distinguishing between genuine and fraudulent profiles. Additionally, an SVM ensemble classifier has been employed to improve detection accuracy by analyzing user demographics, including age, gender, marital status, and profile captions, along with other text-based features. A dataset from Datingmore.com [32] has been widely used for training and validating these models. By leveraging these techniques, dating platforms can enhance fraud detection, providing a safer and more trustworthy environment for users.

4.1 Impact of Fake Engagement on Different Social Media Platforms

Below is a visual representation of the impact of fake engagement across various social media platforms based on available research data.

Figure 3. Top 8 Targeted Platforms by Services in SMM(Social Media Marketing) Panels.[33]



The graph illustrates how platforms like Instagram, YouTube, and Facebook experience significantly higher levels of fake engagement compared to others.

- The inner ring represents the percentage of services offered by SMM panels (such as fake likes, followers, and views).
- The outer ring represents the percentage of daily entries these platforms receive, showing overall platform activity.

4.2 Top 20 Services in SMM Panels

Social Media Marketing (SMM) [33] panels offer a variety of services that artificially inflate engagement on social media platforms. The table below highlights the most frequently purchased services:

Table 1. Top 20 Services in SMM Panels[33]

Site	Product	Entries/day	Different variations	% Panels
Website traffic	4695	493	7066	72.4%
Instagram like	2677	235	8362	100.0%
YouTube view	2524	436	7836	98.3%
Instagram follower	1995	236	7390	100.0%
Instagram view	1084	70	2446	100.0%
Instagram comment	700	52	1622	94.8%
YouTube like	453	35	1151	96.6%
Facebook like	401	20	983	94.8%

Facebook page like	386	44	883	93.1%
YouTube share	441	145	1165	84.5%
YouTube comment	390	35	822	82.8%
YouTube ads view	351	88	940	63.8%
Instagram impression	326	20	654	91.4%
Instagram story view	311	19	704	91.4%
Facebook video view	316	49	657	94.8%
Facebook view	267	46	1272	70.7%
YouTube subscriber	267	47	1066	96.6%

In above table, SMM panels provide services that artificially boost social media engagement, affecting platform authenticity. The table highlights the most frequently purchased engagement services and their widespread use across various platforms.

Key Takeaways from the Data

- Instagram is the most targeted platform, with services like likes, followers, views, and comments being the most frequently purchased (100% coverage in multiple categories).
- YouTube is also heavily affected, with high demand for views, likes, shares, and subscribers, often used for fraudulent monetization.
- Facebook engagement is manipulated, with widespread purchases of page likes, video views, and general likes to enhance visibility.
- Website traffic manipulation (72.4%) indicates that brands and businesses inflate site visits to appear more credible.

This data reveals the large-scale issue of social media fraud, emphasizing the need for robust detection mechanisms to maintain authenticity and prevent financial losses for brands and advertisers. By understanding these fraudulent tactics, platforms can develop proactive measures to ensure genuine engagement and trustworthiness in digital marketing.

5. Conclusion

The growing issue of social media fraud, particularly the fabrication of engagement through fake likes, followers, and comments, has become a significant concern in digital marketing. Such deceptive activities damage brand reputation, mislead advertisers, and lead to financial setbacks. The availability of SMM panels has further enabled individuals and businesses to manipulate engagement metrics, making it easier to distort marketing performance. This study analyzed various social media fraud techniques, such as phishing, cloned accounts, investment fraud, cyberbullying, and online shopping scams, emphasizing their negative effects on consumer trust and digital authenticity.

To address these challenges, machine learning-based fraud detection strategies, including both supervised and unsupervised models, have been explored as potential solutions. By adopting effective fraud detection mechanisms, businesses can protect their marketing budgets, enhance data reliability, and encourage genuine user interactions. Establishing transparency and credibility in digital marketing is essential to sustaining consumer confidence and preserving brand integrity.

6. Future Scope

Future studies can focus on improving fraud detection techniques by leveraging advanced machine learning and artificial intelligence methods, such as deep learning and anomaly detection. Implementing blockchain technology may also enhance transparency in social media transactions, minimizing the risk of fraudulent interactions. Furthermore, stronger collaboration between social media platforms, regulatory authorities, and marketers can lead to the creation of more effective policies and sophisticated algorithms for detecting fraudulent activities. As social media continues to advance, ongoing evaluation and refinement of fraud detection strategies will be crucial to ensuring a secure and credible digital marketing environment.

7. References

1. Confessore, N. (2018). The Follower Factory. The New York Times. Retrieved from https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html
2. Chhabra, S., Solanki, A., Nayyar, A., & Narayan, Y. (2017). Online Social Network-Based Social Engineering: A Case Study of Fake Profile and Fake Identity Detection. IEEE. https://doi.org/10.1109/ICACCI.2017.8117694
3. Agrawal, S., Agrawal, J., & Singh, N. (2020). Fraud Detection on social media using Data Analytics. ResearchGate. https://www.researchgate.net/publication/341870341
4. Social Network Users Beware: 1 in 5 Phishing Scams Targets Facebook." Social Network Users Beware: 1 in 5 Phishing Scams Targets Facebook | Kaspersky Official Blog, www.kas persky.co.in, 23 June 2014, https://www.kaspersky.co.in/blog/1-in-5-phishing-attacks-targetsfacebook/3646/
5. Jain AK, Gupta BB (2022) A survey of phishing attack techniques, defense mechanisms and open research challenges. Enterprise Inf Syst 16(4):527–565
6. Security M (2022) 6 types of social engineering attacks. 6 types of social engineering attacks. www.mitnicksecurity.com, https://www.mitnicksecurity.com/blog/6-types-of-socialengineering-attacks. Accessed 28 May 2022
7. Kayes I, Iamnitchi A (2017) Privacy and security in online social networks: a survey. Online Social Network Media 3:1–21
8. Rathore S, Sharma PK, Loia V, Jeong Y-S, Park JH (2017) Social network security: Issues, challenges, threats, and solutions. Inf Sci 421:43–69
9. Jain AK, Sahoo SR, Kaubiyal J (2021) Online social networks security and privacy: comprehensive review and analysis. Complex Intell Syst 7(5):2157–2177
10. Guo Z, Cho J-H, Chen R, Sengupta S, Hong M, Mitra T (2020) Online social deception and its countermeasures: a survey. IEEE Access 9:1770–1806
11. Apte M, Palshikar GK, Baskaran S (2019) Frauds in online social networks: a review. SocNetw Surveill Soc, 1–18
12. Cross C (2020) Romance fraud. In: Holt T, Bossler A (eds) The Palgrave handbook of international cybercrime and cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/ 978-3-319-90307-1_41-1
13. Whitty MT (2015) Anatomy of the online dating romance scam. Secure J 28(4):443–455
14. Alom Z, Carminati B, Ferrari E (2020) A deep learning model for Twitter spam detection. Online SocNetw Media 18:100079
15. https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf

16. E5--Investment Scams | Scam watch. Australian Competition and Consumer Commission, www.scamwatch.gov.au, 19 Aug. 2021, https://www.scamwatch.gov.au/types-of-scams/investments/investment-scams
17. Online Shopping Scams | Scamwatch. Australian Competition and Consumer Commission, www.scamwatch.gov.au, 4 Jan. 2018, https://www.scamwatch.gov.au/types-of-scams/buyingorselling/online-shopping-scams
18. Zare M, Khasteh SH, Ghafouri S (2020) Automatic ICA detection in online social networks with PageRank. Peer-to-Peer Netw Appl 13(5):1297–1311
19. Kamhoua GA, Pissinou N, Iyengar SS, Beltran J, Kamhoua C, Hernandez BL, Njilla L, MakkiAP (2017) Preventing colluding identity clone attacks in online social networks. In: 2017 IEEE 37th international conference on distributed computing systems workshops (ICDCSW). IEEE, pp 187–192
20. Kontaxis G, Polakis I, Ioannidis S, Markatos E (2011) Detecting social network profile cloning. In: Proceedings of IEEE international conference on pervasive computing and communications, pp 295–300
21. Liu L, Lu Y, Luo Y, Zhang R, Itti L, Lu J (2016) Detecting "smart" spammers on social network: a topic model approach. arXiv preprint arXiv:1604.08504
22. Chen C, Zhang J, Xie Y, Xiang Y, Zhou W, Hassan MM, AlElaiwi A, Alrubaian M (2015) A performance evaluation of machine learning-based streaming spam tweets detection. IEEE Trans Comput Soc Syst 2(3):65–76
23. Jhangiani R, Bein D, Verma A (2019) Machine learning pipeline for fraud detection and prevention in e-commerce transactions. In: 2019 IEEE 10th annual ubiquitous computing, electronics and mobile communication conference (UEMCON). IEEE, pp 0135–0140
24. Ileberi E, Sun Y, Wang Z (2021) Performance evaluation of machine learning methods forced it card fraud detection using SMOTE and AdaBoost. IEEE Access 9:165286–216529
25. Kaggle. (n.d.). Credit card fraud detection. Retrieved from https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
26. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. 2008 Eighth IEEE International Conference on Data Mining, 413–422. https://doi.org/10.1109/ICDM.2008.17
27. Freund, Y., & Schapire, R. E. (1997). A decision-theoretic generalization of on-line learning and an application to boosting. Journal of Computer and System Sciences, 55(1), 119–139. https://doi.org/10.1006/jcss.1997.1504
28. U.S. Securities and Exchange Commission. (2022). Enforcement actions: FCPA cases. Retrieved from https://www.sec.gov/enforce/sec-enforcement-actions-fcpa-cases
29. Dadvar M, Eckert K (2020) Cyberbullying detection in social networks using deep learning-based models. In: International conference on big data analytics and knowledge discovery, pp 245–255. Springer, Cham
30. Agrawal S, Awekar A (2018) Deep learning for detecting cyberbullying across multiple social media platforms. In: European conference on information retrieval, pp 141–153. Springer, Cham
31. Jong K (2019) Detecting the online romance scam: recognizing images used in fraudulent dating profiles. Master's thesis, University of Twente
32. Suarez-Tangil G, Edwards M, Peersman C, Stringhini G, Rashid A, Whitty M (2019) Automatically dismantling online dating fraud. IEEE Trans Inf Forensics Secure 15:1128–1137

33. An analysis of fake social media engagement services. (2022). Nevado-Catalán, D., Pastrana, S., Vallina-Rodriguez, N., & Tapiador, J. Retrieved from https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/1677/1-s2.0-S0167404822004059-main.pdf?sequence=1