IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 1, January 2026

DOI: 10.17148/IARJSET.2026.13141

Identification of Fake Profiles on Social Media Networks: A Comprehensive Analysis

Ms Sumitra Menaria[1], Dr Viral H Borisagar[2]

Research Scholar, CSE/IT Engineering, GTU, Chandkheda, Ahmedabad, Gujarat, India[1]

Associate Professor, Computer Engineering Department, Vishwakarma Government Engineering College, Chandkheda, Ahmedabad, Gujarat, India[2]

Abstract: Social media sites such as Facebook, Instagram, blogs, and Twitter have become the most popular places for people of all ages to spend much of their time because they allow users to share information rapidly and broadly, which in turn attracts new users. The huge rise in daily visitors to these sites is increasing the risk of giving false information and becoming a victim of fraudulent accounts. A phoney account is frequently used to spread misleading information, send spam, forward phishing attack URLs, and steal contacts for personal benefit or the detriment of competitors. Therefore, Finding fraudulent users and spammers on online social networks (OSNs) is a popular research topic.

This study examined the effects of fake profiles and new methods for identifying them, including deep learning and machine learning algorithms like Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), and K-Nearest Neighbours (KNN). A comparison of different techniques for cross-platform profile verification or re-identification is also provided in order to mitigate the harm caused by fraudulent profiles.

Keywords: Cross-platform identification, online social media networks, profile cloning, fake profiles, and profile re-identification.

I. INTRODUCTION

In the past few years, social media connections have grown in popularity. People might look for pals who share their interests or missing connections through social networking. According to the Global Social Media Research Summary from August 2020, 3.81 billion people will be utilising online social media in 2020, with half of the world's population currently connected to the internet (4.77). According to Dean, this represents a 9.2% annual increase. The inventor of our world in data, Esteban Ortiz-Ospina, claims in his piece that Facebook is the biggest social media network globally. Users number 2.4 billion. YouTube and WhatsApp are two more social media sites with over one billion members apiece [1]. Fake profiles are more common on online social media because of their rapid growth. Profiles that have been created using false identities and images in an attempt to gain

Financial or personal advantages are known as fake profiles. Businesses can sell their products to a wide audience on social media platforms because so many people use them online. In order to gather information for research and other uses, many people use false identities. For OSN security and user privacy, identifying fraudulent profiles is therefore an important issue that must be resolved.

Fake profiles are made on OSNs for a variety of reasons, some of which include:

- Link farming is the practice of users trying to gain more followers or connections. It can be employed to target a large crowd for spreading false information or to influence people on a certain topic. Spammers use this link in their phishing campaigns. [5]– [2].

- Identity Theft: When a scammer assumes a false identity in an effort to get the victim's identity for personal or organizational benefit [4]–[7].
- Cyberbullying: Unauthorised individuals can send objectionable content or engage in cyberbullying by using fictitious personas. [8, 9]

- Stealing Personal Information: Phishing users can target real users and steal their personal information by engaging in extensive online discussions with friends [10], [11].

- Black marketing: It costs millions of dollars to sell accounts with a sizable following. Individuals develop enormous fan bases, which they subsequently provide to companies. Companies use them to advertise their products. [8, 11, 12]

There are numerous type of false profiles, some of the examples include:

- Sybil Account: In an attempt to compromise security and privacy, a hacker will manually create several accounts, according to Al-Qurishi et al. [1], Mateen et al. [8], and Mezhuyev et al. [10]. Businesses commonly utilise this type of attack to raise their ratings on e-commerce platforms or social media networks. When committing crimes, these profiles are usually used to get the greatest impact. Here, many accounts or identities—which seem to be genuinely distinct identities—can be created and managed on the same node.

- Sockpuppets: Kacchi and Deorankar [13], Krishnan et al. [7], Mateen et al. [8], and Singh et al. [14] claim that sockpuppets were created as fictitious online personas on purpose to trick others. Most often, a single commanding individual or group produces a large number of ockpuppets. They are usually used to evade blocks, make up public opinion, stack ballots, and engage in other related activities.

- Social Bots: According to Mateen et al. [8], Mezhuyev et al. [10], Narayanan et al. [15], and Xiao et al. [18], boats are software programs intended to carry out specific activities without the need for human involvement. They behave like people and keep users busy. Synthetic personas are commonly used by bots to communicate with humans and build less identifiable social networks. It can also be used to send friend invites, post comments, and influence others in online social networks.

The presented study has examined several methods for identifying the fraudulent account. Related work to detect fraudulent accounts has been covered in part II. A number of features and databases for false profile detection are presented in Section III. Section IV includes future activities.

II. RELATED WORK

Numerous in-depth studies have already been carried out to detect phoney profiles on OSNs using a range of methods. The first of three categories for identifying false accounts is the examination of phoney friend requests to stop fraudulent individuals from being added to our profiles [2]–[4], [6]. This type of approach is known as a pre-analysis approach. The second option is to detect fake profiles using machine learning techniques, like post analysis methods [5, 7, 8, 10, 12, 13]. The third technique, also known as profile re-identification, compares a person's profiles on multiple platforms to ascertain their authenticity.

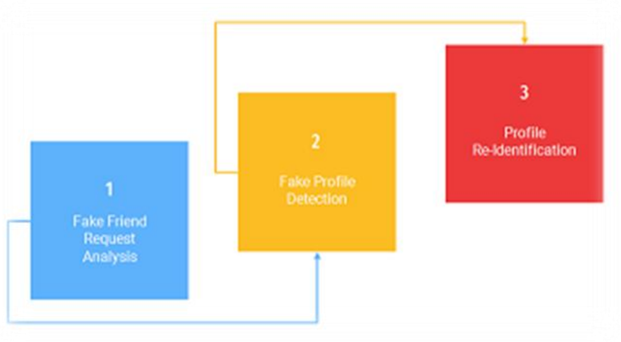

Figure 1. Types of Social Media Profile Analysis

A. Analysis technique for fake friend requests:

As an example, let's say that B sends a friend request to A. Begin by manually counting the number of friends you share. A found out that C and D had friends in common, thus A will trust B and accept B's friend request instead. Despite not knowing B personally, C accepted his friend request after recognising D, another friend they share. The indirect trust is used in this way to establish a connection with fraudulent users. In order to detect genuine friend requests, [2] has made an effort to build trust between different nodes. False friend requests can be detected using the methods provided.

DOI: 10.17148/IARJSET.2026.13141

Making system: Rahman et al. [12], Vitaliy, and Zakirul have proposed a method for reliable decision-making when deciding which "friend to be" to accept friend requests on social media networks. In this instance, the input data is a graph with user profiles at its vertices and friend requests at its edges. A three-stage approach is used in this investigation. The first stage is a simplified method of comparing the friend request's attributes with the user profile of the sender.

An improved approach, the second step examines the user's profile attributes, the profile of the person who sent the friend request, and the profiles of their friends. The third step analyses the attributes gathered in the first two processes to assess the buddy request's dependability.

Wang et al. have presented a semantic-based friend recommendation system [16]. Based on the user's lifestyle, a similarity matrix was generated using Freindbook as a data mining technique. A module that creates a buddy matching graph can illustrate how similar users' lifestyles are. However, the collection of data was the main weakness in the suggested system.

Kacchi and Deorankar [13] developed a friend recommendation system that is based on a number of parameters, including rating and elements such as blood type, proximity to one another, similar blood types, and related interests.

In order to support the Request Acceptance, Mezhuyev et al. [10] have created a reliable decision-making process. This study's author examined the characteristics of users, friend-to-bes, and friend-to-be friends. Various traits, such as liking and disliking, mutual friends, conduct, etc., were compared in order to improve buddy recommendations.

B. Identifying fraudulent profiles:

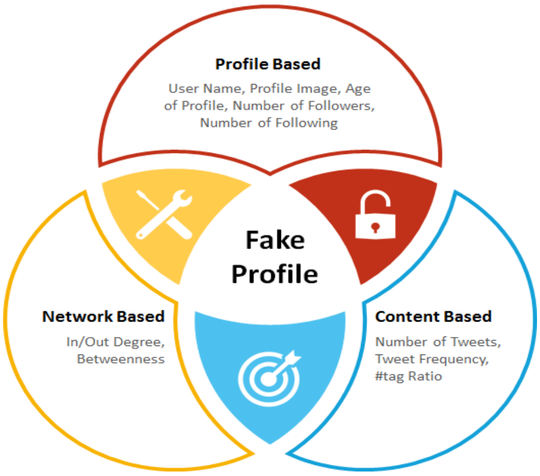
Profile Based
User Name, Profile Image, Age of Profile, Number of Followers, Number of Following
Fake Profile
Network Based
In/Out Degree, Betweenness
Content Based
Number of Tweets, Tweet Frequency, #tag Ratio

Figure 2. Techniques for identifying fraudulent profiles

Xiao et al. [3] devised a scalable approach to identify a sequence of fraudulent logins created by the same individual. The use of supervised machine learning techniques led to the classification of a group of accounts as malicious. The pattern encoding approach was developed to reduce user-generated data into a manageable space that could be used to calculate statistical features. The random forest technique, logistic regression, and support vector machines were used in this investigation. However, the system could not withstand hostile attacks and only supported alphabets in the English language.

Mateen et al. [8] developed a hybrid method that uses both content- and graph-based features to detect spammers on the Twitter network. J48, Decorate, and Nave Bayes classifiers are used to classify profiles as either spammers or authentic accounts. Using correlation, a number of the features used might be eliminated without changing the outcomes.

Three modules were proposed by Al-Qurishi et al. [1]: a deep regression module, a feature extraction approach, and a data gathering module. The data harvesting module separated Twitter users into three groups according on their networks, content, and profiles. Temporal, thematic, linguistic quality, and emotion-based categories were additional classifications for content-based data. The method's only drawback is that, despite its high accuracy, adequate data filtering is required.

Singh et al. [14] proposed a method that makes use of a neural network and a support vector machine. The retrieved profile traits were classified as real or fake using a machine learning technique. A significant amount of data from the 2013 election and fictitious projects was used for classification.

Narayanan et al. developed the machine learning-based browser extension IronSense [15]. The primary focus of their research was to distinguish between phoney and real users based on key attributes, like the number of friends, followers, and status updates. Machine learning methods such as logistic regression, random forest models, and support vector machines (SVM) were used. Still, there is potential for improvement in terms of forecast efficiency and accuracy.

Finite automata are the foundation of the false profile identifier introduced by Krishnan et al. [7]. A regular expression is built based on the persons' place of employment, educational institution, and location of birth. Regular expression was used to compare people who issued friend requests in order to look for login similarities. The regular expression that was produced, however, was much longer for the individual who had friends in more communities.

Wanda and Jie [17] developed a deep learning-based system with the WalkPool pooling function called DeepProfile. By analysing a profile's features, it employs supervised learning and a dynamic deep neural network to determine whether a profile is authentic or counterfeit. The identity of the account, its connections to other accounts, and its behaviour were the three categories of fabricated traits that this tactic exploited. Deviations in profile information and the use of defined attributes were used to identify malicious accounts.

C. Profile re-identification across platforms

The least amount of research has been done on cross-platform re-identification of individuals on online social media. It helps assess an individual's originality. The word "re-identification" comes from the fact that it provides confirmation as well.

Researchers have concentrated on fact-based, relationship-based, and model-based approaches for cross-platform user re-identification. The false negative ratio can be reduced with cross-platform identification. Any profile can be flagged as fraudulent by gathering supporting information during the re-identification procedure.

The four-step method developed by Hill and Nagle [18] was used to compare user behaviour on two distinct network entities during two time periods [5]. This framework's random graph approximation method enables estimation without comparison. This approach was resistant to missing links, although it was less noise-tolerant than other approaches.

User re-identification was carried out utilising both link and content information because Zafarani et al. [19] showed that cross identification based only on links is inadequate. Link information was used to determine correlations between different profiles on different SMNs and crossed-over friends on different networks of the same base node. An additional behavioural modelling technique was considered for systematic analysis. Because humans exhibit redundant behavioural patterns, the behavioural modelling technique to identification was successful. The three categories of behaviour patterns were "exogenous influences," "endogenous variables," and "pattern owing to human limitation."

Ahmad and Ali developed a hybrid approach based on personal data [20]. Re-identification was aided by the use of network and content features. The author used one content feature, cross-posting, network followers, and a network feature. The native approximation distance method was used to assess the comparability of two nodes on different networks. The seed user was penalised by crosslinks on other social media networks, and crawl lists of users from both networks that used cross link attributes were penalised as well. The Levenshtein distance between attributes was determined, and the seed user was identified by attributes with zero distance. In order to identify user commonalities across platforms, the seed user was then utilised as an input to collect relationships and followers.

The Hashimoto group [5] Various kinds of side data are connected to anonymised data through machine learning techniques. Side data was used for comparison, while the target data was the user's resume and social media accounts. An attempt was made by the author to solve the problems of data availability and the inappropriateness of side data. Since resumes may be found on any public platform, a machine learning technique was utilised to correlate side data with profile attributes, making data easier to retrieve.

Yadav S. et al. [11] developed a strategy to identify identical user logins on Twitter using the Jaro-winkler similarity algorithm. The three-layered approach, which used profile attributes to search people, content attributes to uncover similarities in postings, and network attributes to find mutual friends and link connections, was only useful for detecting duplicate logins on the same network.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2026

DOI: 10.17148/IARJSET.2026.13141

III. DATASET AND FEATURE FOR DETECTING FAKE PROFILE

Various strategies have been developed by numerous researchers to detect phoney profiles, false friend requests, and cross-platform profile re-identification. Researchers' features for each of the three categories are shown in this section. Table I lists the specific network characteristics, profile-based features, content-based features, and temporal features used by different research.

TABLE I Features for the Detection of Fake Profiles

Method’s	Feature Type’s	Feature’s	Reference’s
Analysis of False Friend Requests	Features for Users	Number of follower’s	[5], [8], [9], [12]
		Number of Following	
		Number of Replies	
		Number of Repost	
		Age of Account	
		Number of Replies	
	Features of the Content	Number of Retweets	
		Number of hash tags	
		Number of User Mentioned	
		Number of URL	
		Number of Retweets	
	Graph Features	In Degree	
		Out Degree	
		Between-ness	
	Temporal Characteristics	Time of tweet	
		Length of tweet	
		Tweet Frequency	
		Tweet sent in time interval	
		Ideal time in days	
Fake/False Profile	Features Based on Profiles	Verified account (Y/N)	
		#Char of Screen name	
		#Digits of Screen name	
		Time Zone	
		Default profile picture (Y/N)	
		Default profile cover (Y/N)	
		Account age	
		Has profile Description (Y/N)	
		Profile description length	
		Bio has URL (Y/N)	
		#URL in Bio	
		Contains social networks contacts	
	Features depending on content	Temporal Features	
		Topic-based Features	
		Quality-based Features	
		Emotion-based Features	
	Features based on networks	# Friends	
		# Followers	
		# Favorites	
		# Tweets	
		# Retweets	
		# Mentions	
		# replies	
		# Retweeted tweet	

		# Friends distribution	[1], [7], [9], [10], [13], [15]
		# Followers distribution	
		# Favorites distribution	
		#Replied by others	
		#Retweeted by others	
		#Mentioned by others	
		#Favorite by others	
Re-identifying a profile	Features of the profile	First name	[11], [19]–[21]
		Last name	
		Gender	
		Location	
		Education	
		Profession	
		Email	
		Language	
		Date of birth	
		Tag line	
		Profile URL	
		Location	
	Content attributes	Tweets	
		Video posts	
		Image posts	
		YouTube Links	
	Features of Networks	Friendships	
		Group membership	
		Fan page participations	
		Connections	
		Followings	
		Followers	

Ahmad and Ali [21] To create a data collection for the study, Tweeter was used to gather information that users had criticised about their other social media accounts. The user's screen name served as a distinctive characteristic to distinguish related elements. Token-based and character-based distance measure methods were employed to calculate the similarity between different social media profiles.

To identify bogus profiles, a variety of techniques use a wide range of datasets. In this section, information about the datasets is given. In essence, the Stanford Large Network Dataset, which Cao et al. [4] have worked on, is a collection of online social networks with interactions between users represented by the edges. With 4039 nodes and 88,234 edges between them, the dataset consists of information from Facebook and Twitter.

Zhang et al. [22] extended their study using the Facebook dataset. This dataset has 817,091 linkages and 63,731 individuals. The CREDBANK and PHEME Twitter datasets, which each included data on 38,000 individuals and their connections, were used as samples in Wang et al.'s study [9]. The Mateen et al. [8] data set, which includes 10256 individuals and 467480 tweets, is mostly helpful for content-based analysis and profile re-identification.

Research can also use Facebook datasets, which can be obtained from Twitter using the Twitter API. A social media dataset with 2820 nodes—1482 of which contained real user data and 1338 of which were fake—is also available in the Github repository. Because of confidentiality considerations, many research do not disclose the dataset they used.

The features provided in Table I are separated into three groups for the purpose of identifying phoney friend requests [9], [12], [14], [15], and [17]. Four different categories can be used to analyse fake friend requests, such as user profile-based features, which include an account's friends, followers, and activity. When comparing the number of followers and followings over a given time period, the account's age is another crucial consideration that can assist identify if an account is authentic or fraudulent. The number of tweets, retweets, and tags are examples of content characteristics that can be used to assess whether an account is authentic or fraudulent.

DOI: 10.17148/IARJSET.2026.13141

According to a graph feature that incorporates studies of in and out degree and between-ness, a friend request can be recognised as originating from a phoney account if it has submitted more friend requests than it has received in relation to other requests. By examining temporal characteristics, researchers might be able to identify whether a request is the product of a bot. By examining the timing and spacing between tweets, bot-sent content can be identified.

The detection of fraudulent profiles falls under the second category. When determining if a profile is authentic or fraudulent, screen names and profile names play a significant role. The next important determinant of whether an account is authentic or fraudulent, if the profile name is the same, is the profile picture.

The next important consideration is the profile's age. We can compare the ages of two profiles and identify the younger one as fraudulent if the name and photo match.

Content-based features make it easier to find a certain person's social media activity. The kind of content that profiles upload and distribute helps identify suspicious activities.

In order to identify bogus profiles, researchers used network-based features to track metrics such as the number of posts made from a particular account, the number of friend requests that are sent and received for that profile, the number of tweets or posts that are retweeted by friends in common, and other metrics. The technology is better able to identify phoney profiles thanks to all of the previously listed factors.

The third type of profile analysis on social media is profile re-identification [6, 19, 22]. Cross-checking an account using additional sources, including other social media accounts connected to the suspected account, is essential after identifying a suspicious account. Cross-verification can be done by looking at profile-based characteristics including name, date of birth, education, and qualifications.

Sharing the same post with similar-looking text, video, or image across many social media platforms enhances the accuracy of the detection algorithm and enables people to compare numerous accounts. One example of a network property is a similar buddy group across multiple social media networks. The quantity of connections, followers, and followers on various social media profiles is a crucial component in profile re-identification.

IV. CONCLUSION

Along with the datasets and analytical features, this study has examined the various techniques for identifying fraudulent profiles on social media networks. Our review of the literature showed that although many methods have been developed to detect false accounts, this is not enough. Techniques for alerting users to incoming phoney friend requests should be developed in order to stop users from associating with phoney profiles.

Although a lot of research has been done on identifying fraudulent accounts, we found that much of it concentrates on content-based techniques, with comparatively little effort being put into feature-, network-, or graph-based techniques. These two methods can improve the efficiency of identifying fraudulent accounts.

Methods that work with online data should be developed, as the majority of the work has only been done with offline data. A novel study in the field of collaboration and cross-platform analysis for re-identification of profiles can be carried out by using a variety of social networks and big data analysis for the detection of bogus accounts in social networks. We may further enhance the detection of fraudulent profiles by substituting unstructured behavioural data and sentiment analysis of user social activity for prepared tagged data.

REFERENCES

[1] M. Al-qurishi, M. Alrubaian, S. M. Rahman, and A. Alamri, “A Prediction System of Sybil Attack in Social Network using Deep-Regression Model,” *Futur. Gener. Comput. Syst.*, 2017, doi: 10.1016/j.future.2017.08.030.

[2] B. Dean, “Global social media growth rates.” .

[3] Q. Cao, M. Sirivianos, X. Yang, and K. Munagala, “Combating Friend Spam Using Social Rejections,” 2015, doi: 10.1109/ICDCS.2015.32.

[4] Dave Chaffey, “Global social media researchsummary.” .

[5] M. Ichino and H. Yoshiura, “A Re-Identification Strategy Using Machine Learning that Exploits Better Side Data,” *2019 IEEE 10th Int. Conf. Aware. Sci. Technol.*, pp. 1–8.

[6] D. M. Freeman and T. Hwa, “Detecting Clusters of Fake Accounts in Online Social Networks Categories and

DOI: 10.17148/IARJSET.2026.13141

Subject Descriptors," pp. 91–101.

[7] P. Krishnan and D. J. Aravindhar, "Finite Automata for Fake Profile Identification in Online Social Networks," no. Iciccs, pp. 1301–1305, 2020.

[8] M. Mateen and M. Aleem, "A Hybrid Approach for Spam Detection for Twitter," pp. 466–471, 2017.

[9] A. Zhibo Wang, Jilong Liao, Qing Cao, Hairong Qi and Z. Wang, "Friendbook: A semantic-based friend recommendation system for social networks," in *IEEE Transactions on Mobile Computing*, 2015, pp. 14(3):538–551, doi: doi: 10.1109/TMC.2014.2322373.

[10] V. Mezhuyev, Z. A. Bhuiyan, S. M. N. Sadat, S. Aishah, B. Zakaria, and N. Refat, "Reliable Decision Making of Accepting Friend Request on Online Social," vol. 4, no. c, 2018, doi: 10.1109/ACCESS.2018.2807783.

[11] S. Yadav, A. Sinha, and P. Kumar, "Multi - attribute identity resolution for online social network," *SN Appl. Sci.*, vol. 1, no. 12, pp. 1–15, 2019, doi: 10.1007/s42452-019-1701-z.

[12] V. Mezhuyev, S. Member, S. M. N. Sadat, and A. T. Asyhari, "Evaluation of the Likelihood of Friend Request Acceptance in Online Social Networks," *IEEE Access*, vol. 7, pp. 75318–75329, 2019, doi: 10.1109/ACCESS.2019.2921219.

[13] T. R. Kacchi and P. A. V Deorankar, "Friend Recommendation System based on Lifestyles of Users," 2016.

[14] N. Singh, T. Sharma, A. Thakral, and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning," *2018 Int. Conf. Adv. Comput. Commun. Eng.*, pp. 231–234, 2018.

[15] A. Narayanan, "IronSense : Towards the Identification of Fake User-Profiles on Twitter Using Machine Learning Department of Computer Science."

[16] J. Jia, B. Wang, and N. Z. Gong, "Random Walk based Fake Account Detection in Online Social Networks," 2017, doi: 10.1109/DSN.2017.55.

[17] P. Wanda and H. Jin, "Journal of Information Security and Applications DeepProfile : Finding fake profile in online social network using dynamic CNN," *J. Inf. Secur. Appl.*, vol. 52, p. 102465, 2020, doi: 10.1016/j.jisa.2020.102465.

[18] S. Hill, "Social Network Signatures : A Framework for Re-Identification in Networked Data and Experimental Results," 2009, doi: 10.1109/CASoN.2009.31.

[19] R. Zafarani, L. E. I. Tang, and H. Liu, "User Identification Across Social Media," vol. 10, no. 2, 2015.

[20] W. Ahmad and R. Ali, "A Framework for Seed User Identification across Multiple Online Social Networks," pp. 708–713, 2017.

[21] R. Ali, W. Ahmad, and R. Ali, "ScienceDirect ScienceDirect Social Account Matching in Online Social Media using Cross- Social Account Matching in Online Social Media using Cross- linked Posts linked Posts," *Procedia Comput. Sci.*, vol. 152, pp. 222–229, 2019, doi: 10.1016/j.procs.2019.05.046.

[22] Z. Zhang, S. Su, X. Liu, Y. Guo, and J. Zhang, "Efficient Multi-pair Active Friending in Online Social Networks," *2018 IEEE Glob. Commun. Conf.*, pp. 1–6, 2018.