International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 09 | Sep 2022 www.irjet.net p-ISSN: 2395-0072

Cyber Impact of Fake Instagram Business Account Identify Based on Sentiment Analysis

Umma Khatuna Jannat[1], Dr.M.Mohankumar[2], Syed Arif Islam[3]

[1]*First Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, 641021, India.*
[2]*Associate professor, Department of Computer Science, Karpagam Academy of Higher Education Coimbatore, 64102, India.*
[3]*Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, 641021, India.*

Abstract - *On-line social networks have grown in popularity, influencing people's social life and causing them to become involved with numerous social media sites. Cyber-attacks have become common in the last decade, posing a severe threat to the digital world. Individuals and corporations are increasingly concerned about cyber security as they utilise social media. Facebook, Instagram, and WhatsApp are just a few of the many social networking sites. A majority of people are unaware of the risks, and their lack of information contributes to an increase in cyber-crime. Instagram is one of the social media sites that have gained popularity. This platform is popular for sharing photographs and videos, and it has proven to be beneficial for celebrities, businesses, and anyone with a large following. Fake business accounts are one of the most common forms of malicious activity on Instagram. This research proposes an effective strategy for identifying Instagram fake business accounts.*

Key Words: Sentiment Analysis, Lexicon, Fake Instagram, Business Account, Detection

1. INTRODUCTION

The growth of technology has shown to be the most effective aspect for the current generation as a result of the increase of industrialisation in recent decades. The internet has extended to every corner of the globe thanks to significant technological developments, allowing all information to flow freely. To a significant extent, the internet invention has been a blessing that has had a dramatic impact on people daily lives. The birth of the internet, as well as the technical revolution, cleared the door for the development of many social networking websites. All of the websites are well-known and are visited by millions of people throughout the world. In practically every way, technology has made our lives easier. One of the benefits of technology is the ability to purchase online. Purchasing necessities has now become possible even without stepping out of the door. However, online fraud has made things more difficult and Instagram is a social networking service, many people utilise it to run their businesses online. People that run those internet businesses occasionally do not supply the exact goods that they advertised, or they do not send the thing at all after receiving payment. Fraud of this nature has been quite widespread in recent years. People trust in the internet marketplace is eroding as a result of the actions of a few. Other excellent businessmen are suffering. To determine which Instagram accounts are legitimate and which pages are false has become critical.

Over 16.7 million public were victims of online fakers worldwide in 2017 [1]. The entire amount of money taken by counterfeiters in 2016 was more than $7 billion US dollars, and it is predictable to reach about $31 billion in 2020 [2].

According to recent research from Grand View Research, Inc., With a CAGR of 15.4 percent throughout the projected period, the global fraud detection and prevention market is expected to reach USD 62.70 billion by 2028. Over the projected period, the rise in incidents of mobile payment frauds, phishing, and card frauds, as well as their impact on organisations and resulting financial losses, are expected to drive market expansion. As organisations modify how they connect with their customers, the term "digital transformation" has become the new buzzword. However, as organisations have become more digital, they have become more vulnerable to internet fraud and scams [3]. Every year, Instagram plays a role in the huge number of fakers. People like to buy products through Instagram because it allows them to communicate and negotiate prices before making a purchase. Even the seller's identification is crucial in this case. People impression a little better knowing who is selling the thing if they know who is selling it. However, there are still fakers Obtainable, and we haven't any answer for them.

2. LITERATURE REVIEW

The social media website is essentially a location that is monitored by businesses and can be safeguarded. Again, when it comes to being aware of hackers and cybercrime, which is common these days, it is primarily a fear component that has been observed by various researchers when researching incidents of privacy difficulties that people suffer while using these websites. Researchers all over the world are striving to detect various types of fakers, such as banking

fakers, credit card fakers, online purchase fakers, and so on, in order to ensure that the technology that was developed is not in the hands of bad individuals and is not being used to harm others. This study primarily focuses on social media faker account detection systems, and it also contains investigation of spam identification, fake account identification, dangerous website detection. Other relevant issues to guarantee that the proposed system's usability is as intended.

The internet has become an important instrument in people day-to-day activities, as well as a major source of pleasure. Social media sites have grown in popularity as a result of the entertainment support they provide in the form of music, movies, audios, and videos. The location-based networks that are displayed on smart phones and other similar devices are a feature, but they are also a problem for the general public. While researching privacy issues, social networking companies can help users be more careful of the content they publish. There are cyber footprints that are now being recognised as a big deception that catches an individual off guard. Detecting malicious accounts is a big issue on the Internet today. Online social media sites such as Facebook, LinkedIn, and Instagram offer both positive and bad services, such as opinions and comments, as well as rumors, spam, and other criminal behavior. All of this has opened the way for a plethora of well-known cybercrime cases. Cybercriminals have recently flocked to social networking platforms. Cybercriminals employ both social engineering and social engineering to meticulously exploit any personal information, and cybercrime has fast taken over all social networking networks. The difficulty of detecting fraudulent accounts in online social networks is investigated in this research. By developing a machine learning-based system and developing a model for a user's statistical and dynamic patterns. Using genuine data from online social networks, our system is capable of detecting rogue accounts with high accuracy [4].

In recent years, predicting the popularity of social media postings has been more essential, and numerous social networking tools offer. Solutions to improve and optimise the quality of published material as well as increase the attraction of businesses and organisations. In order to allow such technologies, scientific study has recently gone in this direction, utilising modern techniques such as machine learning, deep learning, natural language processing, and others. In light of the foregoing, this study approaches the task of predicting the popularity of a future Instagram post as a classification issue and proposes a novel method based on Gradient Boosting which encouraging testing results. For scalability and efficiency, the proposed solution uses big data technologies, and it may be extended to other social media platforms as well [5].

While reviewing recent studies on the detection of fake profiles on social media networks, the intention of this work is to give detecting false user profiles on Instagram based on certain traits utilising machine learning ideas. The logistic regression and random forest methods were employed in this research work [6].

For the Instagram platform, this research proposed a machine learning-based fraudulent account identification approach. To achieve the purpose of the suggested strategy, a dataset of authentic and fake Instagram accounts was established. Then, based on classification techniques and feature sets, numerous solutions for detecting bogus accounts were surveyed. The proposed method took into account the user's content and behavior characteristics and used a classifier algorithm for detecting fraudulent and real accounts [7].

In his research, compared the nave bayes classifier and SVM (Support Vector Machine) classification algorithms to examine sentiments toward candidates for Governor of DKI Jakarta. Using a dataset of 300 tweets in Indonesian with the keywords AHY, Ahok, and Anies, the maximum accuracy is obtained when using the Nave Bayes Classifier algorithm, which has an average value of 95 %. When employing the SVM (Support Vector Machine) approach, the greatest accuracy values are 90% [8].

This paper employed dynamic dictionaries and models to conduct real-time lexicon-based sentiment analysis experiments on Twitter constrained but relevant datasets in order to better understand the popularity of specific phrases and people perspectives on them. [9]. As a result, by examining the comment, sentiment analysis may be utilised to discover fake Instagram accounts. The proposed method is described in depth in this publication.

3. RESEARCH METHODOLOGY

This section explains the research approach that will be used. Figure 1 depicts the many procedures involved in detecting fakers using sentiment analysis. First and foremost, information from an Instagram group must be gathered to identify whether or not it is a fraudulent business account. The data will be collected in the form of a public post and the comments that accompany it. The data will be cleansed and all superfluous texts such as links, single-line comments, and so on will be eliminated during the preprocessing stage. Data that has been preprocessed is ready to be analyzed for sentiment. Different algorithms and even lexicon-based analysis will be used. Finally, based on the sentiment analysis, the processing system will determine whether or not the data should be transmitted for faker identification. The outcome will be reflected based on the detection report.

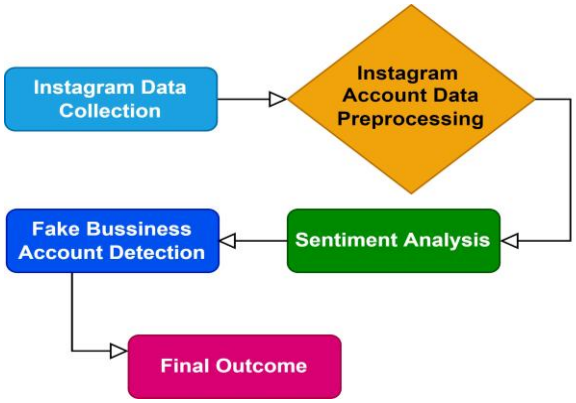

Fig -1: Proposed Diagram for Fake Instagram Identifying

In this research, a model for identifying deception via sentiment analysis is proposed. This will be accomplished by lexicon-based analysis. Customers remarks can be seen whenever a business account on Instagram engages in any form of deceit. Customers will give a positive review if the product is good since their sentiment is based on their satisfaction. As a result, sentiment analysis can be utilised to detect deception in Instagram company accounts.

3.1 Sentiment Analysis

Sentiment Analysis is used in a variety of sectors, including marketing to determine customer reaction to a new product or service, and by social media, users to determine public opinion on a topic that is currently trending. It can assist manufacturers in determining launch plans for new items based on responses to prior versions of that product in various geographic areas. It can also be used to detect heated debates in comments, as well as the usage of abusive language and spam. Sentimental Analysis can be phrase-based, which considers the sentiment of a single phrase, sentence-based, which considers the sentiment of the entire sentence, or document-based, which considers the aggregated sentiment of the entire document and categorises it as positive, negative, or neutral. The process of sentiment analysis is usually broken down into three parts. The subject toward which the sentiment is directed is first identified, then the sentiment's polarity is determined, and finally, the degree of polarity is assigned using a sentiment score that indicates the sentiment's intensity.

When the Instagram account data has been collected and is ready to be examined, the first step will be to do a sentiment analysis. Different algorithms, such as lexicon-based analysis, supervised machine learning can be used to conduct sentiment analysis and based on comments single sharing post polarity will be determine this is the study main goal. It refers to whether something is very positive, very negative, or neutral. When it comes to detecting Instagram account fraud, the polarity of the comments is always a factor. Because fakers cannot be detected on a page when the majority of customers are satisfied or have a favorable polarity. Positive polarity indicates that the page is nice and that the products are good. For very positive and very negative emotions, both algorithms will output a polarity chart. It will be regarded as an excellent page if and only if both charts contain at least 70 % positive comments.

The naive bayes method for sentiment analysis use its library, analysis model, and the result will be shown as a chart. In lexicon-based analysis, algorithm essential. As a result, we'll refer to a line's very positive score as L_{vp} and its very negative score as L_{vN}. It can be written as an equation to calculate the polarity of a line:

Line polarity,

$$L = L_{vP} - L_{vN} \quad (1)$$

If "L" is very positive, the comment will come very positive. Else, the comment will come very negative. Each comment will be give at least one point in either the positive or negative direction. This same calculation will be used for the next comment, and the score will increase according to positive and negative in proportion to the comments number and the polarity.

After analysing entirely shares post comments, the share post will be calculated based on the polarity of the comments.

Sentiment share post,

$$SSentiment = VP_L - VN_L \quad (2)$$

where VP_L represents the total score for the very positive line and VN_L represents the total score for the negative line. If the shares post sentiment is positive, it will receive one point on the positive side, and if the shares post sentiment is negative, it will receive one point on the negative side. Very positive share posts will be labelled Sv_P, while negative share posts will be labelled Sv_N.

Now we'll calculate the Instagram accounts very negative and very positive polarity in a percentage base. N_s is the total number of shares post on the account.

Instagram Account Positive Polarity,

$$IA_p = \frac{S_{vp}}{Ns} \times 100 = x\% \quad (3)$$

Instagram Account Negative Polarity,

$$IA_p = \frac{S_{VN}}{N_S} \times 100 = y\% \quad (4)$$

A chart will be constructed using the values of "y" and "x," but the data set will be forwarded for additional investigation of faker identification if negative score is > 30 %.

According to Figure. 2 does not need to screen for fakers because the majority of the sharing post have good ratings, with a score of 70% or higher. However, positive share posts

are fewer than 70 % in Fig. 3 resulting in a data set for faker identification analysis.

3.2 Fake Account Detection

If an account is fake will be decided by the overall percentage of fake based on share posts and comments (C1,C2…) with favorable or negative evaluations. In this section, all comments will be analysed for fraud analysis, and the output will be classified into Fake, Not Fake, and Neutral. A fake-related, positive, and negative word library will be created for this purpose. This library will be used to determine whether a remark is a fake business account. Now, the data set will consist just of comments from all of the postings. Table II, gives an example of the fake-related word library.

We'll acquire the data set for a fake account analysis after executing the sentiment analysis method and finding suspicious findings for the data set. Fake account analysis can be done using the comments in Table I.

They will receive one point for each faker, good, and negative word. As a result, each library was graded separately depending on each word. For example, the following remarks:

C1: Service is good. Fake things were given also the quality was lied about.

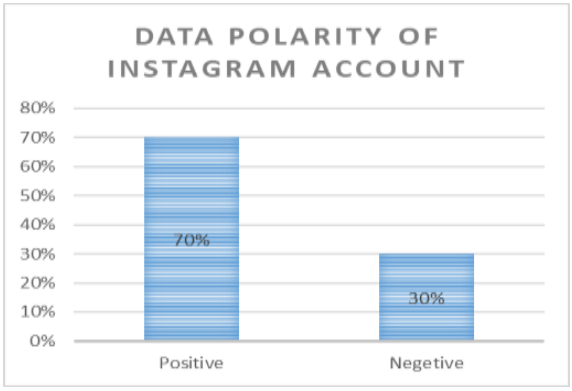

Fig -2: a Polarity for Account A

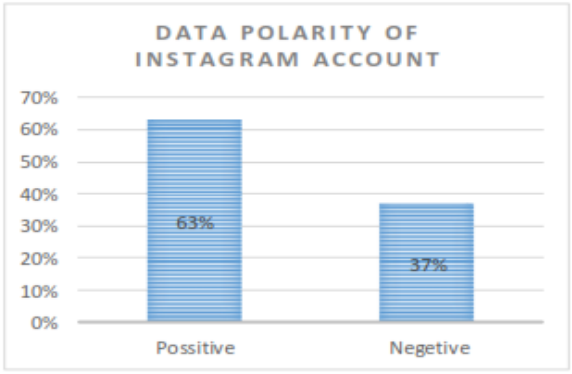

Fig -3: b Polarity for Account B

TABLE I: Fake Business Account Identify of Instagram Demo Data Set

Table II: Fake Account-Related and Negative Comments Library

Positive Comments	Trust, good, great, wished, joy, happy, proud, nice, thanks, sweet, best, smiled, light, fun enjoy, brilliant, promising, beautiful, etc.
Negative Comments	Tragically, dreadfully, shame shame, hate hate, damn damn, blamed, fearful, awfully. Adverse, Shocking, annoyed irritate hooked fail, defective, distress, weak alarming, untidy, damaged, etc.
Fake Comments	Cheat, deception, extortion, blackmail, scam, cheating, graft, hoax, narrator, duplicity, fraudulent, etc.

Table III: Library-Based Comment Scoring

	C1	**C2**
Fake Score Card	Fake =1 Score Card =1	Score Card =0
Positive Score Card	Good=1 Score Card=1	Beautiful=1 Satisfied=1 Score Card=1+1=2
Negative Score Card	Lied=1 Score Card=1	High-priced =1 Score Card=1

C2: Beautiful gown. Very satisfied with the product quality. However, it is a high-priced.

We derive the score shown in Table 3 based on C1 and C2.

As a result, the equation can be written as

$$Csc = VPsc - Fsc - VNsc \quad (5)$$

The score for the comment is Csc , the score for positive words is Ps, the score for fake words is Fsc, and the score for bad words is Ns. If the score is > 0, the comment is very positive (VPCsc), and if the score is < 0, the comment is a negative comment (VNCsc), which is regarded as fraudulent. A comment will be considered neutral if it receives the value 0 in some way. Table 3 shows that C1 has a fake score of 1, a negative score of 1, and a positive score of 1. C2 has a fake score of 0, a negative score of 1, and a positive score of 2.

As a result of Eq. (5), we receive as –1 for C1 and as 1 for C2. Now we may say that C1 is a fake identify and C2 is not. We'll get positive, negative, or neutral numbers after assessing all of the comments. As a result, the percentage of fraud/negative comments may now be determined.

As a result, the equation can be expressed as follows:

$$IFp \frac{VNC_{sc}}{Total\ Comments} \quad (6)$$

IFp is the Instagram fake percentage for all comments in Eq. 6. If the percentage is > 30% this account classified as a fake account.

4. EMPIRICAL ASSESSMENT

The goal of our proposed research is to assess the efficacy of a the security and social platform analytics domains. We also looked at how well the algorithm handled share posts and comments, such as Instagram reviews. Both data sets have been treated with the same terminology. We compared the following sentiment analysis algorithms in the experiment.

It represent Lvp and L_{vN} overall very positive and very negative in a line .The output sentiment value of Op/O_N and Lvp/LvN where Vp, V_N represent the very positive and very negative line. Instead of lowering or raising line sentiment values by 50% or 100%, where the ultimate negation is given by ON and S indicates a lexical sentiment value. The output sentiment function verifies the O_P/O_N and Lv_P/Lv_N values. It returns the sentiment or 0 reliant on whether the complete value of the sentiment is > 25 or the absolute value of the evidence is > 0.5. If the share post contains just positive lines, the ultimate sentiment value is determined solely by O_P and Lv_P. The same thing happens if the message only contains negative terms. When a message has both very positive and very negative terms, it is classified as either very positive or very negative, reliant on which of the two lines is stronger.

```
algorithm.cpp
IF(VN==0)
Return OutPutSentiment(Op,Lvp)
ElseIF(VP==0)
Return OutPutSentiment(ON,LvN)
Else{
IF(Op-ON >0.1)
Return OutPutSentiment(Op,Lvp)
Else IF(ON-Op >0.1)
Return OutPut Sentiment(ON,LvN)
Else{
IF(Op+ON>0)
Return OutPutSentiment (Op,Lvp)
ElseIF(Op+ON<0)
ReturnoutputSentiment(ON,LvN)
Else
Return 0
}}
OutPutSentiment (O,L){
If (|O|>25 || |L|>0.5)
Return O
Else
Return 0
}
```

To begin, the difference between extremely positive and extremely negative remarks is determined. If one item of feedback is significantly > the other (> 0.1), the very positive or very negative emotion is returned. When there is no proof or the differences are not significant enough, the final choice is taken on the basis of the difference between very positive and very negative attitude. The sentence is classified as very

positive if the very positive feeling is greater than the very negative sentiment.

5. CONCLUSION

Online imposters are like bacteria in terms of future business. The internet marketplace has a bright future ahead of it, and if used properly, it will benefit both sellers and customers, but it will be a complete waste if people lose trust. As a result, it is critical to take the required efforts to identify fakes and prosecute them under rigorous rules. This study was conducted to identify fake business accounts on Instagram

Fake business accounts are harmful for social media platforms because they have the potential to change notions like popularity and influence on Instagram, as well as have an impact on the economy, politics, and society. For the Instagram platform, this paper has introduced a false business account identification. As a result, people will be able to spot fake business accounts and avoid them. People must be truthful if people actually hunger to do business in an online bazaar. In the following step, the proposed system will be implemented adn automated structure will be created to gather information on consumer needs. The data will be evaluated in the steps outlined in this article following successful data collection. Finally, the user will receive some findings from the system's visible output. This proposed strategy, as well as other important elements, can be modified to improve results.

REFERENCES

[1] Traci Krepper. "E-Commerce Fraud Attack Rates Hit New Highs in 2017".April 10, 2018.

[2] Dewan P, Bagroy S, Kumaraguru P (2016) Hiding in plain sight: characterizing and detecting malicious Facebook pages. In: 2016 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM), San Francisco, USA, pp 193–196.

[3] Grand View Research, Inc. "Fraud Detection And Prevention Market Size Worth $62.70 Billion By 2028". May 20, 2021.

[4] Nirmala B, SP.Chokkalingam, G.Sai Neelima . "Abnormal User Detection of Malicious Accounts in Online Social Networks using Cookie Based Cross Verification". International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075, Volume-8, Issue-9S4, July 2019: 202-205.

[5] Carta, S., Podda, A. S., Recupero, D. R., Saia, R., & Usai, G. (2020). Popularity prediction of instagram posts. Information, 11(9), 453.

[6] Dey, A., Reddy, H., Dey, M., & Sinha, N. (2019). Detection of Fake Accounts in Instagram using Machine Learning. AIRCC's International Journal of Computer Science and Information Technology, 11(5), 83-90.

[7] Sheikhi, S. (2020). An Efficient Method for Detection of Fake Accounts on the Instagram Platform. Rev. d'Intelligence Artif., 34(4), 429-436.

[8] G. A. Buntoro, "Analisis Sentimen Calon Gubernur DKI Jakarta 2017 Di Twitter," Integer J., vol. 2, no. 1, pp. 32–41, 2017.

[9] Arslan, Y., Birturk, A., Djumabaev, B., & Küçük, D. (2017, December). Real-time Lexicon-based sentiment analysis experiments on Twitter with a mild (more information, less data) approach. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 1892-1897). IEEE.