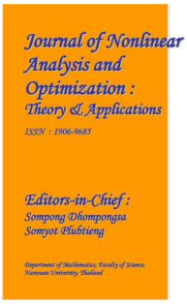
Journal of **N**onlinear **A**nalysis and **O**ptimization

Vol. 14, Issue. 2 : 2023

ISSN : **1906-9685**



INSTAGRAM FAKE PROFILE DETECTION USING MACHINE LEARNING

[1]S Sri Lavanya, [2]N.Nikhitha Reddy, [3]Nishath Afreen K.S, [4]Noothi Srivarshini, [5]N.Chudamani Charitha [1]Assistant Professor, [2,3,4,5]UG Students, Dept. of CSE (AI & ML), Malla Reddy Engineering College for Women (Autonomous), Hyderabad, India. E-Mail: sslavanya79@gmail.com

ABSTRACT

One of the major issues with Online Social Networks (OSNs) is fake interaction, which is used to artificially boost an account's popularity. The identification of fraudulent involvement is essential to prevent company losses, inaccurate audience targeting in advertising, inaccurate product prediction algorithms, and a negative impact on the atmosphere of social networks. This initiative focuses on the identification of automated and phoney accounts that cause phoney activity on Instagram. We are aware of no publicly accessible dataset for automated and phoney accounts. Two datasets have been created for this purpose in order to detect automated and phoney accounts. Machine learning approaches including Naive Bayes, logistic regression, support vector machines, and neural networks are used to find these accounts. Due to the dataset's unnatural bias, a cost-sensitive evolutionary algorithm is also used for the detection of automated accounts. Smote Nc technique is used to address the unevenness issue in the fictitious dataset. The results are 86% and 96%, respectively, for the automated and false account detection issues. Nowadays, the majority of people utilise social networking sites on a daily basis. Numerous people create profiles on social networking websites every day and connect with others there, regardless of their location or time. False identities are prevalent in different types of crime, as well as advanced persistent threats. Social networking site users not only benefit from them but also worry about the security of their personal information. We must first identify the user's social network accounts in order to determine who is disseminating threats in social networks. Based on the classification, it is required to distinguish between real and phoney profiles on social media. Several categorization techniques have traditionally been used to identify phoney social media accounts. However, there are ways to improve social media's ability to identify phoney profiles. The suggested effort uses technology and machine learning to boost the percentage of predicted phoney profiles.

INTRODUCTION

Online social networks (OSNs), such as Facebook and Instagram, are becoming more and more important in today's society. OSNs are utilised not only as a means of communication but also for business promotion and popularity. At first look, measures like follower count or characteristics of the shared content, like the amount of likes, comments, or views, are used to gauge an account's popularity. As a result, users of social media platforms may have a propensity to artificially inflate those platforms' metrics in order to gain greater advantages from OSNs. The reputation of a social media account can be improved using a number of standard techniques. employing bots, buying social media metrics like likes, comments, and followers, and employing networks or platforms that let users exchange analytics are a few examples. A piece of software known as a "bot" performs automatic tasks over the Internet.

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

According to a Ghost Data analysis from 2018, about 95 million Instagram accounts are automated. 2016 saw more Internet traffic produced by bots than by people. Additionally, sellers can easily sell likes and followers by creating false profiles. For instance, IDigic, a firm, offers 50k followers for just $250.

All of the aforementioned behaviours are artificial and are referred to as phoney involvement. In other words, the term "fake engagement" refers to all kinds of automated actions, including posting comments and likes, following accounts, and producing articles and posts. Additionally, the term "fake engagement" can refer to purchasing social media analytics. The detection of users who inorganically expand their accounts is important because it forces businesses to pay users more for advertising than it is worth, causes advertisers to target the incorrect demographics, causes recommendation systems to operate inefficiently, and makes it more difficult to obtain high-quality services and goods. The detection of automated accounts, or bot accounts, and fake accounts are the two independent topics under the heading of fake engagement. As previously said, bot accounts are users who engage in automated actions to boost their popularity metrics, such as following users and enjoying content from similar audiences. Fake accounts are those that are used to increase a certain account's social media stats after paying for this service. It can also be referred to as phoney followers to draw attention to it more effectively. The primary distinction between automated and phoney accounts is that the former enhances its own metrics while the latter enhances the metrics of other users while contributing to a negative social media atmosphere.

LITERATURE SURVEY

The proliferation of social media platforms, such as Instagram, has led to an increase in the creation of fake profiles. Fake profiles can be used for various malicious activities, including spreading misinformation, engaging in spamming or phishing, and conducting online scams. Detecting and removing fake profiles is crucial for maintaining the integrity and security of social media platforms. In this project, we aim to develop a machine learning-based system to detect fake profiles on Instagram. The main objective of this project is to create an automated system that can accurately identify and flag fake profiles on Instagram. By utilizing machine learning techniques, we can analyze various features and patterns in user profiles to determine their authenticity. To train our machine learning model, we need a diverse and representative dataset of real and fake Instagram profiles. We collect data by scraping publicly available Instagram profiles, including both genuine and known fake accounts. The dataset should include features such as username, profile picture, bio, number of followers, number of posts, engagement metrics, and other relevant information. In today's society, social media is an integral part of everyone's life. It is mostly used for sharing information, staying in touch with friends, and other similar activities. The number of Instagram users has been rising quickly in recent years. Compared to other social networking sites, Instagram has grown in popularity over the past ten years. More than 1 billion people are currently using Instagram, which has seen exponential growth. The majority of the incorrect information and dangerous activity on these social networks is spread through fake accounts.

Therefore, many researchers have been applying machine learning approaches to address security issues in social networks, according to the literature. Studies that were surveyed mainly concentrated on spam detection on social media for microblogging. To address the issue of spam and fraudulent accounts on social media, they have looked into a variety of methods. One of the reasons for this study is the lack of a comprehensive solution to phoney accounts on the Instagram platform as of yet. In order to accurately classify distinct Instagram user accounts, we have proposed an effective strategy for identifying phoney accounts on the Instagram platform in this study.

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

EXISTING SYSTEM

As of my knowledge cutoff in September 2021, there isn't a specific pre-built system provided by Instagram for fake profile detection using machine learning (ML). However, Instagram and other social media platforms employ various automated techniques and algorithms to detect and combat fake profiles. While the exact details of their systems are not publicly disclosed, they likely utilize a combination of rule-based algorithms, anomaly detection, and machine-learning approaches.

YEAR	TITLE	AUTHOR	INFERENCE
2017	Random Walk Based Fake Account Detection in Online Social Networks	Jinyuan Jia, Binghui Wang, Neil Zhengiang Gong	Random walk-based methods, which leverage the structure of an online social network to distribute reputation scores for users.
2017	Detecting Fake Accounts in Online Social Networks at the Time of Registrations	Dong Yuan, Yulani Miao, Zheng Yang, Qi Li, Dawn Song	In this work, there is Ianus, a Sybil detection method that leverages account registration information.
2019	Analysis and detection of fake profile over social network	Vijay Tiwari	This project reviews many methods to detect the fake profiles and their online social bot.
2020	Identifying Fake Profile in Online Social Network: An Overview and Survey	Shruti Joshi, Himanshi Gupta Nagariya	In this project, a detailed overview of various studies done in this direction and a survey of all the techniques already used and can be used in the future is provided

Table.1. Literature Survey

PROPOSED SYSTEM

Several supervised algorithms with varied degrees of accuracy are used in this study to find fake Instagram profiles. Each model may recognise a bogus profile based only on attributes that are visible. For each supervised model, the accuracy and loss graphs are shown using the same set of data. Furthermore, comparative graphs of the model accuracy of several models are shown. The models are trained using the appropriate optimisation techniques, loss functions, and logical operations.

Detecting fake Instagram accounts can be a challenging task due to the evolving nature of fake profiles. However, here's a proposed system that combines various techniques and strategies to help identify fake Instagram accounts: Account Creation Analysis, Content Analysis,User Interaction Analysis,Machine Learning Models,Reporting Mechanisms

It's important to note that no system can guarantee 100% accuracy in detecting fake Instagram accounts. However, by employing a combination of these techniques and leveraging machine learning, you can significantly improve the accuracy of detection and minimize the presence of fake accounts on the platform

SYSTEM ARCHITECTURE

This architecture provides a framework for building an Instagram fake profile identification system. However, the specific implementation details may vary depending on the chosen technologies, resources, and the scale of the system.

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

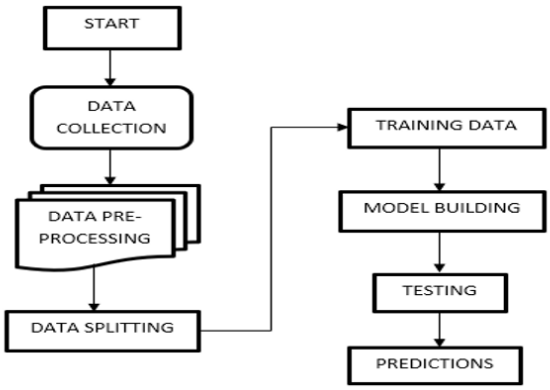


Fig.1. System architecture

Machine learning methods, data analysis, and rule-based systems are frequently combined in the architecture for spotting phoney Instagram profiles. Based on the findings of the research, give each profile a risk score. Using this score, moderators can automatically flag questionable profiles for manual review and additional inquiry, or they can use it to rank profiles for further examination. To assist in decision-making and system monitoring, provide reporting and visualisation capabilities to display the analysis results, including statistics, trends, and insights on false profile detection

DEFINE PROBLEM

Since 2012, Instagram has been a social media platform for sharing photos and videos online. It is accessible on both Android and iOS devices. More than one billion users have signed up for Instagram as of May 2019. Instagram has been revealed to use third-party programmes known as "bots" in recent years. While it is true that these might impersonate users and damage their reputation, resulting in "identity theft," there have also been more examples of deceptive means of promoting a company's brand image known as "influencer marketing."

Angler phishing is a new scam that has emerged as a result of businesses using social media to respond to their customers' requirements. Due to all of these malpractices, it is essential to use effective fraud detection tools, which is why we provide our recommendation.

The following modules and components can be utilised to build Instagram Fake Profile Detection Using Machine Learning:

Data Collection

a. Here dataset used is a MIB dataset.
b. The data set consisted of 3474 real profiles and 3351 fake ones.
c. The data set used TWT, INT, and FSF for fraudulent accounts whereas E13 and TFP were used for authentic ones.
d. The information is kept in CSV format for machine extraction.

Preprocessing

a. The data collection is pre-processed before being given to a model.
b. This method aims to identify if a profile is real or fake based on how it appears. The specifics have now all been settled.
c. Following the combination of an accurate and unreliable user data set, each profile is given the extra label "fake," a Boolean variable.

Model Deployment

a. Utilize machine learning algorithms to train a classification model on the pre-processed data.
b. Various algorithms such as logistic regression, random forests, support vector machines, or neural networks can be employed
c. Experiment with different models to determine the best-performing approach**.**

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

Max Voting

a. This voting procedure is typically employed for categorization issues

b. In this method, each model's forecast of the data is treated as a vote and numerous models are utilized to predict each piece of information.

c. The final forecast uses the bulk of the model.

Identity Fake Profile

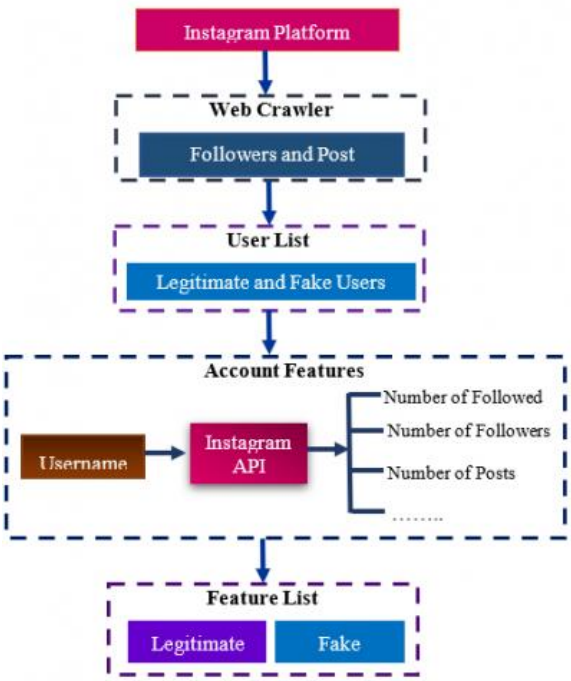


Fig.2.Software system architecture

Implementation

Keras

On top of the machine learning framework Tensorflow, Keras is a Python-based deep learning API. "Keras" is:

Simple -- but not too simple. Keras lessens the cognitive strain on developers so you may concentrate on the crucial aspects of the issue.

Flexible -- straightforward workflows should be quick and straightforward, whereas arbitrarily advanced workflows should be feasible via a clear path that builds upon what you've already learned, according to the progressive disclosure of complexity principle adopted by Keras.

Powerful -- Keras offers performance and scalability that is unmatched in the market; it is utilised by businesses and organisations like NASA, YouTube, and Waymo.

Sklearn

Scikit-learn is mostly written in Python and significantly makes use of the NumPy module for computations involving arrays and linear algebra. To further the effectiveness of this library, some basic algorithms are also written in Cython. Utilising wrappers created in Cython for LIBSVM and LIBLINEAR, support vector machines, logistic regression, and linear SVMs are done. In certain conditions, expanding these functions with Python might not be practical.

Tensorflow:

TensorFlow, a free and open-source software framework, is used for dataflow and differentiable programming across a range of tasks. It is a symbolic math library that is also used by machine learning programmes that use neural networks. It is utilised by Google for both research and production. To work

in machine learning, it is a requirement in the industry to have TensorFlow experience. The Google Brain team created TensorFlow for usage within Google. On November 9, 2015, it was made available under the Apache 2.0 open-source licence.

Pandas:

Pandas is an open-source Python toolkit that provides high-performance data analysis and manipulation tools using its powerful data structures. Python was mostly used for data munging and preprocessing. On data analysis, it had little of an effect. Pandas discovered the answer. No matter where the data came from, we may use Pandas to complete the five typical steps of data processing and analysis: prepare, modify, model, and analyse. Many academic and professional fields, including finance, economics, statistics, analytics, etc., use Python with Pandas.

Numpy:

NumPy is a general-purpose library for managing arrays. It provides an extremely quick multidimensional array object along with the ability to interact with these arrays. The foundational Python module for scientific computing, to put it simply.

Matplotlib:

Publication-quality graphics are produced in a variety of physical formats and cross-platform interactive settings using the Python 2D plotting package Matplotlib. Matplotlib can be used with four graphical user interface toolkits, the Python and IPython shells, the Jupyter notebook, web application servers, and Python scripts. Matplotlib tries to make simple things straightforward and difficult things doable. You can make graphs, histograms, power spectra, bar charts, error charts, scatter plots, and more with just a few lines of code. For examples, view the sample plots and thumbnail galleries. The pyplot package provides a MATLAB-like interface for simple plotting, especially when used in conjunction with IPython. Power users have total control over line styles, font settings, axis characteristics, etc. using an object-oriented interface or other means.

ALGORITHMS

Artificial Neural Network (ANN)

Artificial Neural Networks (ANN) are algorithms modelled after the brain that are used to predict issues and represent intricate patterns. The Artificial Neural Network (ANN), a deep learning method, was inspired by the notion of organic neural networks in the human brain. ANN was developed in an effort to mimic how the human brain works. Although they don't operate exactly same, biological neural networks and ANNs have many similarities. The ANN algorithm only accepts structured and numeric data.

To accommodate non-numeric, unstructured data formats including audio, text, and image, recursive neural networks (RNN) and convolutional neural networks (CNN) are used..

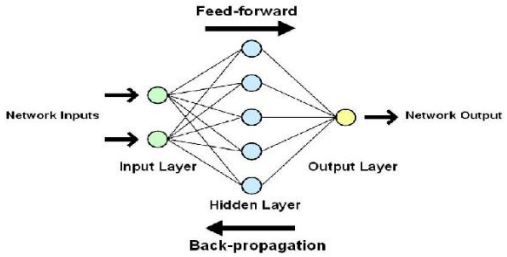


Fig.3.Architecture of ANN

Custom ANNs:

Creating a custom artificial neural network (ANN) for fake Instagram profile detection using machine learning can be an effective approach. Here's a high-level overview of the steps involved in building such a system:

1. **Dataset Collection**: Gather a large dataset of Instagram profiles labeled as either real or fake. This dataset should include various features such as profile images, bio descriptions, post content, follower/following counts, engagement metrics, and any other relevant information.
2. **Data Preprocessing:** Clean and preprocess the collected data to ensure it's in a suitable format for training the ANN. This step may involve tasks such as resizing and normalizing images, tokenizing and encoding text data, and normalizing numerical features.
3. **Feature Extraction**: Extract meaningful features from the preprocessed data that can help distinguish between real and fake profiles. For example, you can use techniques like convolutional neural networks (CNNs) to extract image features, natural language processing (NLP) methods for text features, and basic statistical measures for numerical features.
4. **Design the ANN Architecture:** Determine the structure and architecture of your custom ANN. This choice depends on the nature of the features and the complexity of the problem. You can experiment with various architectures, including feedforward neural networks, recurrent neural networks (RNNs), or even more advanced architectures like convolutional or transformer-based models.
5. **Training:** Split your preprocessed dataset into training and validation sets. Feed the training data into the ANN and use an appropriate optimization algorithm (e.g., stochastic gradient descent) to update the model's weights iteratively. Monitor the performance on the validation set to prevent overfitting and adjust hyperparameters accordingly.
6. **Evaluation and Validation**: Evaluate your trained ANN using a separate test dataset that wasn't used during training. Measure metrics such as accuracy, precision, recall, and F1-score to assess the model's performance in detecting fake Instagram profiles.
7. **Iterative Improvement:** Analyze the results and iteratively refine your model. You can try different ANN architectures, tweak hyperparameters, or incorporate additional features to enhance the detection accuracy.
8. **Deployment**: Once you're satisfied with the performance, deploy your custom ANN in a production environment. You can build an application or integrate the model into an existing system to automatically detect fake Instagram profiles.

Creating an effective fake profile detection system is a complex task that requires continuous improvement and adaptation to evolving techniques used by malicious actors. Regular updates and monitoring are crucial to maintain the system's effectiveness in detecting and preventing fake profiles.

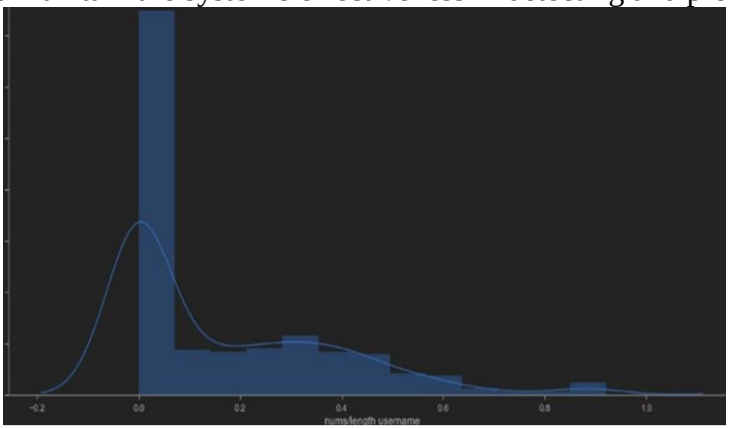


Fig.4. Dataset Distribution

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

	precision	recall	f1-score	support
0	0.89	0.93	0.91	60
1	0.93	0.88	0.91	60
accuracy			0.91	120
macro avg	0.91	0.91	0.91	120
weighted avg	0.91	0.91	0.91	120

Fig.5. Model Summary

Train model: We have set some parameters for the training model, such as batch size, step per epoch, and number of epochs.

Plot Graph: The graph below shows the training and loss distribution for the model after training.

Evaluate Model: Send 20% of the test data to the model for evaluation. Test accuracy of 99% was attained by me.

RESULTS

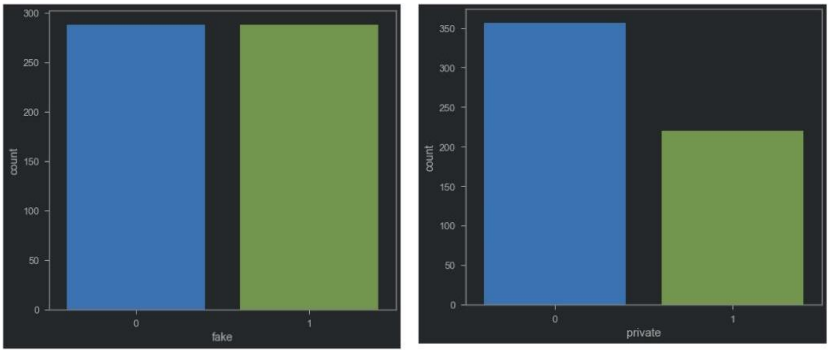


Fig.6. Data Visualization for detecting fake profile and private

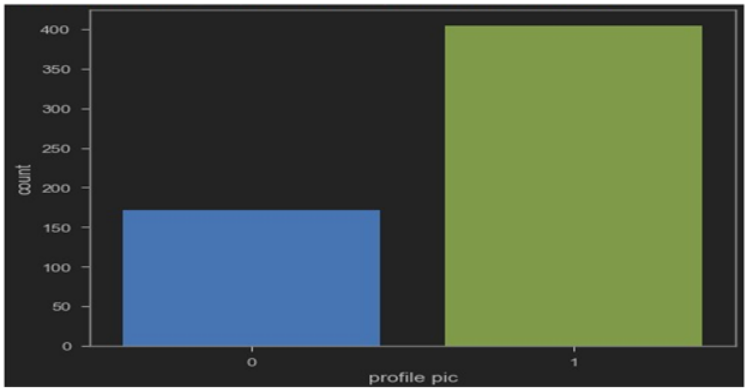


Fig.7. Data Visualization for detecting fake profile an

Fig.8. Assessing the Performance of Trained Model

http://doi.org/10.36893/JNAO.2023.V14I2.0215-0224

Fig.9. A new framework based on machine learning for spotting bogus Instagram profiles

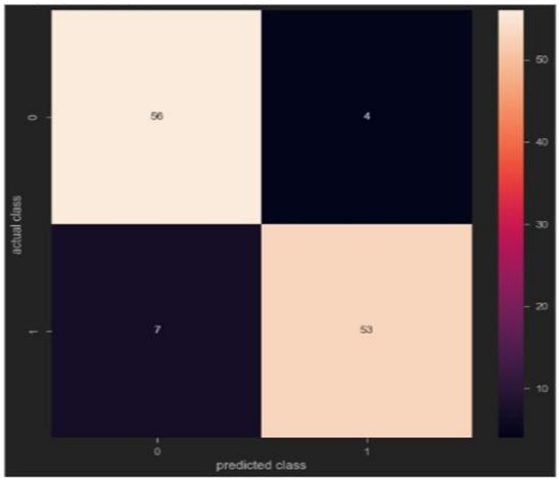


Fig.10. Prediction of fake Instagram profile detection

CONCLUSION

The project specifics demonstrate how to identify false information on reputable Instagram sources. Additionally, crowdsourced "user-generated" content on Instagram makes it easier and less expensive to distinguish between real and fake profiles. I believe that using such a method could help users of social media build and support their own reputations. These results will help determine whether social media narratives follow classic story patterns. People are increasingly using social media instead of more traditional channels to get their news. However, social media has also been used to spread false information, which has a negative effect on both specific individuals and the entire population. By reviewing the literature on identification and detection, we conducted an extensive study on the topic of phoney profiles. Both in traditional and social media, we introduced the definitions and principles of fake news. We discovered that not much has been done on Instagram specifically as a social network platform while reviewing earlier similar studies on the detection of phoney profiles on social media platforms. As a result, we focused our strategy on doing the same. In this research, we presented a unique method based on machine learning principles for identifying bogus Instagram user accounts. Our accuracy rates were 90.8% and 92.5%, respectively, using the Logistic Regression and Random Forest algorithms, respectively. Previous research done for other social media platforms did not achieve as high accuracy levels (the best accuracy achieved before to this was 86%).

FUTURE SCOPE

The future scope for fake Instagram profile detection using machine learning (ML) which include several advancements:

Enhanced Feature Extraction: Improving the feature extraction process can lead to better detection of fake profiles. Researchers can explore advanced techniques in computer vision, natural language processing, and social network analysis to extract more nuanced and informative features from profile images, text content, engagement patterns, network connections, and other relevant data.

Adversarial Learning: As fake profile creators become more sophisticated, ML models need to be robust against adversarial attacks. Adversarial learning techniques can be employed to train models that are resilient to attacks aimed at evading detection

User Behaviour Analysis: Incorporating user behaviour analysis can provide valuable insights for detecting fake profiles. ML models can be trained to analyze patterns of user interactions, posting behaviour, follower/following dynamics, and engagement metrics to identify suspicious or anomalous activities associated with fake profiles.

Real-Time Detection: Advancements in ML techniques, hardware acceleration, and infrastructure can enable real-time detection of fake profiles on Instagram. This would allow for immediate actions to be taken to mitigate the impact of fraudulent accounts and provide a safer user experience.

Privacy Preservation: Balancing the need for fake profile detection with privacy concerns is crucial. Future research can focus on developing ML models and techniques that preserve user privacy while still effectively detecting fake profiles. This can involve methods such as federated learning, differential privacy, or secure multi-party computation.

It's important to note that the fight against fake profiles is an ongoing battle, and new techniques and approaches will continue to emerge.

REFERENCES

[1]. Indira Sen, Anupama Aggarwal,Shiven Mian.2018."Worth its Weight in Likes: Towards Detecting Fake Likes on Instagram". In ACM International Conference on Information and Knowledge Management.

[2]. Shalinda Adhikari, Kaushik Dutta. 2014. “Identifying Fake Profiles In LinkedIn”. In Pacific Asia Conference on Information Systems.

[3]. Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainen.2017. "Detection of Fake Profiles in Social Media”. In 13th International Conference on Web Information Systems and Technologies. International Journal of Computer Science & Information Technology (IJCSIT) Vol 11, No 5, October 2019 90

[4]. https://telecom.economictimes.indiatimes.com/news/india-saw-457-rise-in-cybercrime-in-fiveyearsstudy/67455224

[5]. Todor Mihaylov, Preslav Nakov.2016. "Hunting for Troll Comments in News Community Forums". In Association for Computational Linguistics.

[6]. Ml-cheatsheet.readthedocs.io. (2019). Logistic Regression — ML Cheat sheet documentation. [Online] Available at: https://ml cheatsheet.readthedocs.io/en/latest/logistic_regression.html#binarylogistic-regression [Accessed 10 Jun. 2019].

[7]. 3. Schoonjans, F. (2019). ROC curve analysis with MedCalc. [Online] MedCalc. Available at: https://www.medcalc.org/manual/roc-curves.php [Accessed 10 Jun. 2019].

[8]. Kietzmann, J.H., Hermkens, K., McCarthy, I.P., Silvestre,B.S., 2011. Social media? Get serious! Understanding the functional building blocks of social media. Bus.Horiz., SPECIAL ISSUE: SOCIAL MEDIA 54, 241251. doi:10.1016/j.bushor.2011.01.005.

[9]. Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015.Advanced Social Engineering Attacks. J Inf SecurAppl 22, 113–122. doi:10.1016/j.jisa.2014.09.005.