WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

UNMASKING DECEPTION USING MACHINE LEARNING TECHNIQUES

Mr.M.Ramu [1], P.Govindavasan [2], R.Ramesh [3], S.Aravinthan [4], J.Deenapraksh [5]

[1] Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineering College(Autonomous), Perambalur, Tamil Nadu.

[2,3,4,5] UG - Department of Information Technology, Dhanalakshmi Srinivasan Engineering College(Autonomous), Perambalur, Tamil Nadu.

E-Mail: ramu2009it@gmail.com, vasangaming007@gmail.com, reyaramesh07@gmail.com, deenaprakash33@gmail.com, aaravinthan459@gmail.com

ABSTRACT

Fake profile identification in social networks is a crucial task to maintain the authenticity of the platform and protect its users from fraudulent activities. Machine learning and natural language processing (NLP) techniques can be used to identify fake profiles based on various features such as user behaviour, social network connections, and textual content. In this study, we propose a machine learning and NLP-based approach to identify fake profiles in social networks. We first collect a dataset of profiles from various social networks and manually annotate them as real or fake. We then extract various features such as the number of friends, the frequency of posts, and the sentiment of the textual content. We use these features to train various machine learning algorithms such as random forests to classify profiles as real or fake. We also use NLP techniques to analyse the textual content of profiles and extract features such as the use of emoticons, the frequency of certain words, and the use of grammatical errors. We evaluate our approach on a large dataset of profiles from various social networks and show that our approach can accurately identify fake profiles with high precision and recall. Our approach can be integrated into social network platforms to automatically detect and remove fake profiles, improving the authenticity and trustworthiness of the platform for its users.

KEY WORDS: Natural Language Processing (NLP)

INTRODUCTION

Fake profile identification in social networks is a crucial task that requires a combination of machine learning and random forest techniques. With the increasing use of social media platforms, the number of fake profiles has also increased, leading to various online threats such as cyberbullying, phishing, and identity theft. Therefore, identifying fake profiles is crucial to ensure the safety and privacy of users.

Machine learning algorithms can be used to automatically identify fake profiles by analysing various features such as profile information, posting behaviour, and network properties. For instance, supervised learning algorithms such as random forests can be trained using labelled data to classify profiles as genuine or fake based on their features. NLP techniques can also be used to analyse the content of the profiles and posts to identify fake profiles. Sentiment analysis, for example, can be used to determine whether the content is genuine or fake based on the emotional tone and language used. Additionally, named entity recognition can be used to identify fake profiles based on inconsistencies in the personal information provided. The combination of machine learning and NLP techniques can be an effective approach to identify fake profiles in social networks. By analysing various features and content, such algorithms can help to ensure the safety and privacy of users on social media platforms.

PURPOSE

The purpose of unmasking deception using machine learning techniques is to develop systems that can detect and prevent fraudulent activities and misinformation. Machine learning provides a powerful toolset for identifying patterns and anomalies that are indicative of deceptive practices, such as

Deepfake Detection: Machine learning algorithms, especially deep learning and Generative Adversarial Networks (GANs), are used to identify deepfakes—highly realistic and manipulated media that can depict individuals saying or doing things they never did.

Fraud Detection: Machine learning is instrumental in detecting various forms of fraud, including identity theft, payment fraud, insurance fraud, and online scams

OBJECTIVES

In the model capable of analysing user profiles and identifying patterns indicative of fake or fraudulent activity. A diverse dataset of both genuine and fake profiles, and pre-process the data to extract relevant features for model training.In the train the machine learning model using the prepared dataset, employing algorithms like random forests, or machine learning approaches. Validate the model to ensure its accuracy, precision, and recall in detecting fake profiles.

EXISTING SYSTEM

The existing system is establishing and management of social relationships among huge amount of users has been provided by the emerging communication medium called online social networks (OSNs). The attackers have attracted because of the rapid increasing of OSNs and the large amount of its subscriber's personal data. Then they pretend to spread malicious activities, share false news and even stolen personal data. Twitter is one of the biggest networking platforms of micro blogging social networks in which daily more than half a billion tweets are posted most of that are malware activities. Analyse, who are encouraging threats in social networks is need to classify the social networks profiles of the users. Traditionally, there are different classification methods for detecting the fake profiles on the social networks that needed to improve their accuracy rate of classification. Thus machine learning algorithms are focused in this paper. Therefore detection of fake profiles on twitter using hybrid Support Vector Machine (SVM) algorithm is proposed in this paper. The machine learning based hybrid SVM algorithm is used in this for classification of fake and genuine profiles of Twitter accounts and applied the dimension reduction techniques, feature selection and bots. Less number of features is used in the proposed hybrid SVM algorithm and 98% of the accounts are correctly classified with proposed algorithm.

DISADVANTAGES

- The system relies on a limited set of features to detect fake profiles, such as follower count, retweet count, and user description. This may not capture all the nuances of a fake profile, and some fake profiles may go undetected.
- There is a risk of overfitting the SVM model to the training data, which can result in poor generalization to new, unseen data.

PROPOSED SYSTEM

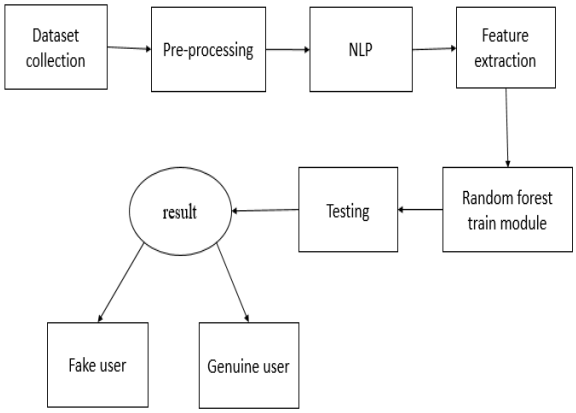
The rise of social media has led to an increase in online interactions, making it easier for people to connect and share information. However, this has also led to the creation of fake profiles, which can be used for various malicious activities such as spreading misinformation, phishing attacks, and cyberbullying. Fake profiles can also be used to manipulate online communities, making it challenging to maintain the security and authenticity of online interactions. To address this issue, machine learning algorithms such as Random Forest and Natural Language Processing (NLP) can be used to identify fake profiles in social networks. Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve accuracy and reduce overfitting, making it useful for classification tasks. NLP is a field of machine learning that focuses on processing and understanding human language, which can be used to analyse the text content of social media profiles and identify patterns or anomalies that may indicate a fake profile.

In this proposed system, we will use Random Forest and NLP to identify fake profiles in social networks. The system will collect data from various social networks, including profile information, posts, comments, and messages. The data will be pre-processed to clean and convert it into a numerical representation using techniques such as Bag-of-Words or TF-IDF. Relevant features will be extracted from the data, such as profile information, posting frequency, language use, and network activity. The data will be labelled as either genuine or fake profiles based on a set of predefined criteria. The Random Forest classifier will then be trained on the labelled data using the extracted features as input and the labels as output. The trained classifier will be tested on a separate dataset to evaluate its accuracy and performance. Finally, the system will evaluate the results and adjust the model parameters as needed to improve accuracy and reduce false positives and false negatives. The used as a tool to automatically detect fake profiles in social networks, providing an additional layer of security and authenticity for online interactions.

ADVANTAGES

- The system can automatically detect fake profiles, saving time and effort compared to manual detection methods.
- The system can achieve a high level of accuracy in identifying fake profiles, reducing the risk of false positives and false negatives.
- The identifying fake profiles, the system can help improve the security and authenticity of online interactions, reducing the risk of malicious activities such as phishing, cyberbullying, and misinformation.

SYSTEM ARCHITECTURE



FUTURE ENHANCEMENT

Multimodal Analysis: Combine textual content analysis with other modalities such as images and user interactions. Integrating image analysis techniques and sentiment analysis of comments and interactions can provide a more comprehensive understanding of profile authenticity.

Active Learning and Semi-Supervised Learning: Investigate techniques such as active learning and semi-supervised learning to make better use of limited labelled data. This can involve iteratively selecting the most informative profiles for manual annotation or leveraging unlabeled data to improve model performance.

Real-Time Detection and Scalability: Develop approaches for real-time detection of fake profiles that can scale to large social network datasets. Efficient algorithms and distributed computing techniques may be necessary to handle the volume of data and provide timely responses to emerging threats.

CONCLUSION

In conclusion, the proposed system for fake profile identification in social networks using Random Forest and NLP is a promising approach to maintaining the security and authenticity of online interactions. The system leverages machine learning algorithms such as Random Forest and NLP to analyse social media profiles, identify patterns or anomalies that may indicate a fake profile, and classify the profiles as either genuine or fake.

By collecting and pre-processing data from various social networks, extracting relevant features, labelling the data, training the Random Forest classifier, and testing the system, we can identify fake profiles with a high level of accuracy.

REFERENCES

1) "Identifying fake profiles in linkedin." Adikari, Shalinda, and Kaushik Dutta. arXiv preprint arXiv:2006.01381 (2020). A feature-based approach to detect fake profiles in Twitter." Kaubiyal, Jyoti, and Ankit Kumar Jain. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, pp. 135-139. 2019.
2) Sarah Khaled, Neamat El-Tazi and Hoda Mokhtar, "Detecting Fake Accounts on Social Media", *Conference Paper*, pp. 3672-3681, 2018.
3) Estée Van Der Walt and Jan Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans", *IEEE Access*, vol. 6, pp. 6540-6549, 2018.
4) Sk. Shama, K. Siva Nandini, P. Bhavya Anjali and K. Devi Manaswi, "Fake Profile Identification in Online Social Networks", *International Journal of Recent Technology and Engineering*, vol. 8, no. 4, November 2019.
5) S. Shinde and S. B. Mane, "Hybrid Approach For Fake Profile Identification On Social Media" in Pattern Recognition and Data Analysis with Applications, Singapore:Springer, pp. 579-590, 2022.

6) M. F. Mridha, A. J. Keya, M. A. Hamid, M. M. Monowar and M. S. Rahman, "A Comprehensive Review on Fake News Detection with Deep Learning", *IEEE Access*, 2021.
7) L. Siburian, "Data Mining Predicts Immunization Vaccine Needs Using the Naive Bayes Method (Case Study of UPT Primary Health Center)", *Resolution: Informatics and Information Engineering*, vol. 1, no. 5, pp. 282-290, 2021
8) R. Kareem and W. Bhaya, "Fake Profiles Types of Online Social Networks: A Survey", *Int. J. of Engineering and Technology*, vol. 7, no. 4.19, pp. 919-925, 2018.
9) M. Singh, "Tagging Fake Profiles In Twitter Using Machine Learning Approach" in Mobile Computing and Sustainable Informatics, Singapore:Springer, pp. 181-197, 2022.
10) M. J. Awan, M. A. Khan, Z. K. Ansari, A. Yasin and H. M. F. Shehzad, "Fake Profile Recognition Using Big Data Analytics In Social Media Platforms", *Int. J. of Computer Applications in Technology*, vol. 68, no. 3, pp. 215-222, 2022.
11) M. Jabardi and A. S. Hadi, "Twitter Fake Account Detection And Classification Using Ontological Engineering And Semantic Web Rule Language", *Karbala Int. J. of Modern Science*, vol. 6, no. 4, pp. 404-413, 2020.
12) Frunze Alex and Frolov Aleksey, Methods for Detecting Fake Accounts on the Social Network VK, pp. 342-346, 2021.
13) D. Martín-Gutiérrez, G. Hernández-Peñaloza, A. B. Hernández, A. Lozano-Diez and F. Alvarez, "A Deep Learning Approach for Robust Detection of Bots in Twitter Using Transformers", *IEEE Access*, vol. 9, pp. 54591-54601, 2021.
14) K. Patel, S. Agrahari and S. Srivastava, "Survey on Fake Profile Detection on Social Sites by Using Machine Learning Algorithm", *2020 8th International Conference on Reliability Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1236-1240, 2020.
15) Fake news detection within online social media using supervised artificial intelligence algorithms.Ozbay, F.A. and Alatas, B., 2020. Physica A: Statistical Mechanics and its Applications, 540, p.123174.