International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

FAKE PROFILE IDENTIFICATION IN SOCIAL NETWORK USING MACHINE LEARNING AND NLP

Putta Srivani[1], G. NavyaSri[2], K. Vyshnavi[3], K. Swathi[4]

[1]Associate Professor, Department of IT,Malla Reddy Engineering College For Women(Autonomous Institution), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

[234]UG Scholar, Department of IOT,Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

Email: Pulla.srivani@gmail.com

ABSTRACT

Social media platforms have become a very integral part of everyday life, enabling people to connect, communicate, and share information across the globe without time or location barriers. However, these platforms are increasingly being targeted by malicious actors who create fake profiles to deceive users, spread false information, and engage in fraudulent activities. It is vital for a social network to detect fake profiles and eliminate them as it ensures security and integrity. The conventional ways used to detect fake profiles typically depend on heuristic methods or classification based on simple rules. The need to improve accuracy toward fake profile detection has given motivation to look into new kinds of advanced computational methods for this purpose. This paper therefore presents an approach by utilizing machine learning and NLP techniques to enhance the process in detecting and classifying the fake profiles on social networks. Our method uses algorithms such as Support Vector Machines (SVM) and Naïve Bayes for efficient classification based on the analysis of user behavior, textual content, and metadata associated with profiles. NLP techniques are particularly useful for extracting linguistic patterns and identifying anomalies in user-generated content, further improving detection rates. The proposed framework aims to achieve higher accuracy and reliability compared to traditional methods. This research thus addresses the challenges associated with fake profiles and improves the overall security of social media platforms and promotes a safer online environment for users.

Keywords-Fake profile detection,Social networks,Machine Learning (ML),Natural Language Processing (NLP),Support Vector Machine (SVM),Naïve Bayes algorithm,User classification.

I. INTRODUCTION

Social media have become a modern feature in the lives of individuals. Many users worldwide consume hours per day on this activity. OSNs operate with many different purposes for these social interaction networks, ranging from simple platforms for social purposes such as Facebook and MySpace to more complex information platforms, like Twitter and Google Buzz. While these networks provide ample benefits, they pose numerous challenges to security and privacy and are an important issue that concerns users and service providers alike. In interactions within OSNs, individuals often share partial or complete personal information, which makes them vulnerable when exposed publicly to attacks, as identity theft is one of the most serious. Identity theft occurs when an

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

attacker uses someone's information without his consent for fraudulent reasons. This has been one of the problems that have emerged in popularity in the past decade, with millions of users affected globally. Identity theft victims can face financial losses, reputational damage, relationship strain, or even legal action against them. Most social networks have no strict verification mechanism when it comes to the users' accounts. Moreover, default privacy settings offer little protection, making a conducive environment for malicious activity. Malicious profiles, or profiles created with fake credentials, are especially troublesome. Generally, these profiles are linked to malicious activities like phishing, spam, online impersonation, and the spreading of false information. Profiles on social networks can be categorized as static or dynamic. Static data consists of information such as age, work, and hobbies entered while registering for a profile, while dynamic data consists of actual live behavior patterns and activities. Previous studies have based detection algorithms primarily on static and dynamic data. Most social media platforms, however, limit exposure to dynamic data, thereby rendering some of these techniques less effective.U Problems associated with fake profiles are cyberbullying, violation of privacy, spread of misinformation, and identity theft on the Internet. Despite implementing security measures such as the Facebook Immune System (FIS) to fight against threats like phishing and spam, platforms are finding it hard to detect and remove fake profiles at scale. This paper introduces a new approach based on machine learning and natural language processing techniques to enhance the detection of fake profiles. Using algorithms Such as Support Vector Machines (SVM) and Naïve Bayes, this research aims to improve classification accuracy, thereby addressing critical security issues and promoting safer online environments.

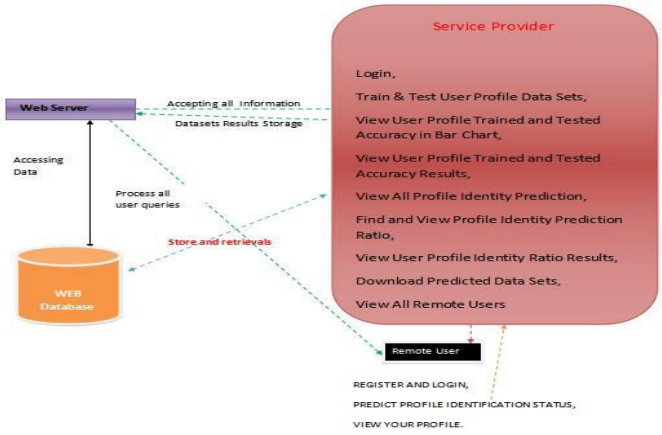

Fig 1: System Architecture

II. RELATED WORK

Strangers Intrusion Detection: Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies

Author: Michael Fire, Goldschmidt R., and Elovici Y. (2012)

This study investigates the detection of spammers and fake profiles in social networks using topology anomalies. The authors propose a method to identify suspicious behaviors based on structural deviations in the network graph. This research highlights the importance of analyzing social network topology to detect unusual patterns that may indicate malicious users.

Neuralnet: Training of Neural Networks

Author: Günther F. and Fritsch S. (2010)

This work presents a framework to train neural networks in R. Although not exactly centered on fake profile detection, techniques discussed provide foundational insight in training neural

networks, which would be adapted for classification purposes in user behavior on social networks.

Preprocessing Techniques for Text Mining

Author: Dr. S. Kannan and Vairaprakash Gurusamy (2015)

This paper is focused on the text preprocessing techniques that are very important for text mining applications. Methods such as tokenization, stemming, and removal of stopwords are discussed by the authors, which are very essential for preparing textual data for analysis. These preprocessing steps are relevant for Natural Language Processing tasks in fake profile detection.

Detecting Fake Profiles in LinkedIn

Author: Shalinda Adikari and Kaushik Dutta (2014)

This paper discusses the analysis of fake profile detection in LinkedIn, with a special focus on professional networking scenarios. The authors propose techniques that analyze profile attributes and behaviors for distinguishing between genuine and fake accounts. The findings also underline the importance of the analysis of both static and dynamic data to increase the accuracy of detection.

Malicious Users' Circle Detection in Social Networks Based on Spatiotemporal Co-occurrence

Author:Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz (2011)

This paper presents a spatiotemporal approach to detect malicious users in social networks. By analyzing the co-occurrence of user activities over time and space, the authors present a method to identify coordinated malicious behavior, which is a common trait of fake profiles.

Analyzing Facebook Privacy Settings: User Expectations vs. Reality

Author: Liu Y., Gummadi K., Krishnamurthy B., and Mislove A. (2011)

This paper discusses the discrepancy between users' expectations and actual privacy settings on Facebook. It was found that users have inadvertently leaked their private information due to not knowing about, or having default, privacy settings. This understanding is key in analyzing the abuse of fake profiles on the network.

Poster: Preliminary Analysis of Google's Privacy

Author: Mahmood S. and Desmedt Y. (2011)

This paper outlines an initial analysis of Google's privacy mechanisms, focusing on the challenges of securely managing user data. Although this paper focuses on Google, it does provide general insight into privacy concerns that social networks are susceptible to in the hands of fake profiles.

III. IMPLEMENTATION

Initially, data from any social media platform like facebook or linkedin are collected and preprocessed. Preprocessing phase includes activities like text cleaning, labeling, source extraction, and word removal for preparing data to be analyzed. This cleaned data is then analyzed using feature extraction techniques that capture the static and dynamic characteristics of user profiles, such as demographic information and activity patterns. To classify profiles as genuine or fake, two

machine learning algorithms are used: Support vector machine (svm) and naïve bayes. Svm is employed for finding the best separating hyperplane between fake and real profiles by analyzing the data in a multidimensional feature space. Naïve bayes classifies profiles based on probabilistic relationships between different profile features, under the assumption that these features are independent. Both algorithms have been trained on a labeled dataset, where profiles have been manually labeled as either real or fake. The effectiveness of the models is measured using precision, accuracy, recall, and f1 score. To make more accurate classification, the system utilizes the best of both worlds of static data (user biography, profile photo) and dynamic data (posting frequency, content engagement) to reach a final decision, enhancing the overall detection performance. The system is implemented in python using libraries such as scikit-learn for machine learning, nltk for nlp functions, and django for back-end integration. A mysql database is used to store user data and fake profile detection results. This implementation provides a scalable effective way to address the problem of fake profiles, providing improved accuracy and real-time detection in social networks.

IV. ALGORITHM

Decision Tree Classifiers

Decision trees are extensively used in classification tasks as they are interpretable and easy to understand. They are developed based on recursive partitioning of the feature space. The process begins with the selection of the feature that best splits the dataset into subsets, and then each subset is further split based on subsequent features. If all objects in a subset belong to the same class, it becomes a leaf node in the tree. Otherwise, a new test is applied, recursively partitioning the dataset until the leaf nodes are pure. Decision trees are efficient for both regression and classification tasks and provide clear visual representation of decision-making rules.

Gradient Boosting

Gradient boosting is a machine learning procedure used to develop predictive models. It involves the accumulation of a number of weak decision trees in a stage wise fashion to create predictive models. During gradient boosting, one adds a new model such that it corrects some errors made by the former. The method optimizes a differentiable loss function that makes it more adaptable compared to other boosting procedures. Gradient-boosted trees tend to be better than random forests because they have a focus on reducing residuals in a sequential manner. This technique has been extremely effective for both classification and regression tasks.

KNN K-Nearest Neighbors K-Nearest Neighbors One of the very basic powerful classifiers based upon the locality principle of the data. Upon receiving the classification problem for a new point of data, it discovers in a feature space that whose are the 'K' nearest neighbors of a certain class, then KNN attributes majority class among the above neighbours to a new piece of data. KNN is a non-parametric, lazy-learning algorithm, which never assumes the underlying distribution of the data and does not even build a model during the learning phase. It's simple but may be highly computationally expensive

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

during the classification phase, especially in the case of large data.

Logistic Regression Classifiers

Logistic regression is that type of classification algorithm whose dependent variable is categorized. More often than not, it applies to binary variables like Yes/No, 0/1. It gives an application form with respect to the dependent and independent variables by using logistic functions for predicting the probabilistic values. The estimations of the coefficients from logistic functions are done via the techniques such as MLE. Multinomial logit is the extension variant applied to the problems consisting of three or more categories. They are used for binary class assignment and are preferred due to ease and interpretability.

Naive Bayes

The Naive Bayes classifier is based on the Bayes theorem and assumes that the features used to predict the class are conditionally independent given the class label. This makes the computation efficient and predictions are made very fast. It often performs well in practice even with the assumption of independence, and is highly effective for text classification tasks like spam filtering or sentiment analysis. This algorithm calculates the posterior probability of every class given the input features and outputs the class with the highest probability.

Random Forest

Random Forest is an ensemble learning technique that trains hundreds and thousands of decision trees in the training phase and gives back the class for which most of the trees have voted in the case of classification problems (or average of prediction for regression). It addresses the problem of overfitting, typically encountered with individual decision trees by averaging multiple trees in an attempt to reduce variance. Random Forest is quite stable across different types of data and is useful in high-dimensional datasets where there may be complex relationships and many features. Its robustness and scalability make it a very popular tool in practical applications.

Support Vector Machine (SVM)

SVM is a discriminant classifier that tries to find the best separating hyperplane between different classes in the feature space. SVM is known for handling high-dimensional data and kernel tricking, which transforms data into higher dimensional spaces to make them linearly separable. It's especially useful in classification problems where the classes are not linearly separable. SVMs are less prone to overfitting, especially when the margin between classes is large, and they find applications in both classification and regression problems.

RESULT

Fig:1 User Login

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

Fig:2, Accuracy Bar Chart

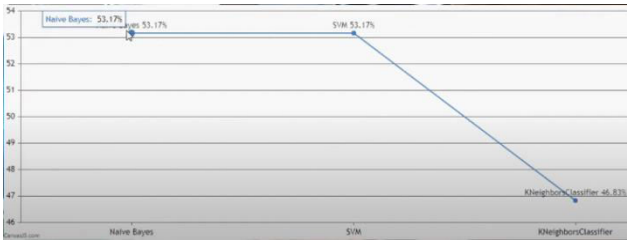

Fig:3, Tested &Trained Results

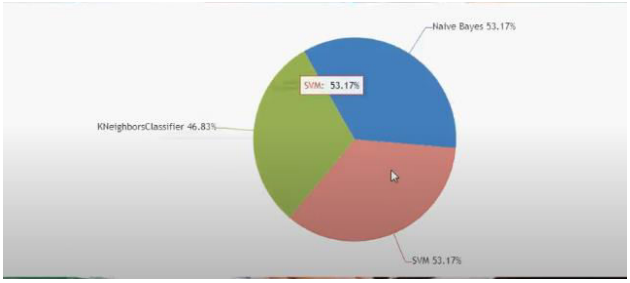

Fig:4:Pie Chart Results

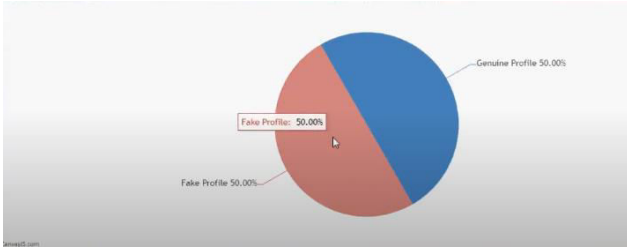

Fig:5:Pie Chart Results

CONCLUSION

We discuss here a new approach combining the strengths of machine learning algorithms with those of NLP techniques for addressing this problem. Detecting fake profiles is risky for the privacy and security of social media users. Hence, developing methods to detect these with reasonable accuracy and efficiency becomes crucial. Using a Facebook dataset, we illustrate our approach's effectiveness. The techniques used here are NLP preprocessing applied to user-generated content. These techniques are then extracted into meaningful features to determine deeper understanding of profile behavior and text patterns. Those features are processed through a machine learning algorithm called SVM and Naïve Bayes classification. The proposed method improves the detection accuracy and therefore is potentially a reliable solution for the identification of fake profiles. Our results, therefore, emphasize the necessity of using NLP along with machine learning techniques in order to overcome the drawbacks of the traditional detection methods. The technique utilizes language models and computational intelligence to produce a more robust framework to detect and mitigate the threat of the fake accounts. Future studies can be developed by implementing this methodology into other social media platforms and testing whether the generalization and effectiveness vary differently with this context. This may include advanced techniques in deep learning, which could further enhance the performance in detection.

REFERENCES

[1] Michael Fire et al. (2012). "Strangers intrusion
detection-detecting spammers and fake profiles in social networks based on topology anomalies." Human Journal 1(1): 26-39.Günther, F. and S. Fritsch (2010). "neuralnet: Training of neural networks." The R Journal 2(1): 30-38

[2] Dr. S. Kannan, Vairaprakash Gurusamy, “Preprocessing Techniques for Text Mining”, 05 March 2015.

[3] Shalinda Adikari and Kaushik Dutta, Identifying Fake Profiles in LinkedIn, PACIS 2014 Proceedings, AISeL

[4] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,"Malicious users' circle detection in social network based on spatiotemporal co-occurrence," in Computer Networks and InformationTechnology(ICCNIT),2011International Conference on, July, pp. 35–390.

[5] Liu Y, Gummadi K, Krishnamurthy B, Mislove A," Analyzing Facebook privacy settings: Userexpectations vs. reality", in: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,ACM,pp.61–70.

[6] Mahmood S, Desmedt Y," Poster: preliminary analysis of google?'s privacy. In: Proceedings of the 18th ACM conference on computer and communications security", ACM 2011, pp.809–812.

[7] Stein T, Chen E, Mangla K," Facebook immune
system. In: Proceedings of the 4th workshop on social network systems", ACM 2011, pp

[8] Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi,"Malicious and Spam Posts in Online Social Networks," Computer, vol.44, no.9, IEEE2011, pp.23–28.

[9] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y.Dai, B. Zhao, Understanding latent interactions in
online social networks, in: Proceedings of the 10th
ACM SIGCOMM Conference on Internet Measurement, ACM, 2010, pp. 369–382

[10] Kazienko, P. and K. Musiał (2006). Social capital in online social networks. Knowledge-Based Intelligent Information and Engineering Systems, Springer

[11] Fotiadis, "Machine learning applications in cancer prognosis and prediction", Computational and Structural Biotechnology Konstantina Kourou Themis P. Exarchos Konstantinos P. Exarchos Michalis V. Karamouzis Dimitrios I. Journal, vol. 13, pp. 8-17, 2015, ISSN 2001-0370.

[12] L. Deng and X. Li, "Machine Learning Paradigms for Speech Recognition: An Overview", IEEE Transactions on Audio Speech and Language Processing, vol. 21, no. 5, pp. 1060-1089, May 2013.

[13] KH Teoh et al., "Face Recognition and Identification using Deep Learning Approach", Journal of Physics: Conference Series, 2021.

[14] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, "Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial", IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3039-3071, Fourthquarter 2019.

[15] Tan Qiaoyu, Liu Ninghao and Hu Xia, "Deep Representation Learning for Social Network Analysis", Frontiers in Big Data, vol. 2, 2019, ISSN 2624-909X.

[16] V. Rama Krishna and K. KanakaDurga, "Automatic detection of illegitimate websites with mutual clustering", International Journal of Electrical and Computer Engineering, vol. 6, no. 3, pp. 995-1001, 2016.

[17] G Narsimha and P. Srinivas Rao JayadevGyani, "Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP (2018)", International Journal of Applied Engineering Research, vol. 13, no. 6, ISSN 0973-4562.

[18] Mohammed Ali Al-Garadi, Mohammad Rashid Hussain, Henry Friday Nweke, Ihsanali. Ghulammujtabal, Hasanalikhattak

HarunachiroMa and Andabd Ullahgani, Predicti-Ngcyber Bullying on Social Networks.

[19] G. Sai Pooja, P. Rajarajeswari, V. YaminiRadha, G. NavyaKrishna and B. Naga Sri Ram, "Recognition of fake currency note using convolutional neural networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 5, pp. 58-63, 2016.

[20] Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainenin, "Detection of fake profiles in social media-Literature review", International Conference on Web Information Systems and Technologies, vol. 2, pp. 363-369, 2018.

[21] D. Ramalingam and V. Chinnaiah, "2 Fake profile detection techniques in large-scale online social networks: A comprehensive review", Computers & Electrical Engineering, vol. 65, pp. 165-177, 2018.