e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

FAKE SOCIAL MEDIA PROFILE DETECTION USING MACHINE LEARNING

Dr. R. S. Khule[*1], Pooja Gavande[*2], Harshada Sonawane[*3], Anushka Niphade[*4], Pooja Phad[*5]

[*1]Professor, Information Technology, Matoshri College of Engineering and Research Centre, Nashik

[*2,3,4,5]Student, Information Technology, Matoshri College of Engineering and Research Centre, Nashik

ABSTRACT

The social network, which is such an important part of our lives, is plagued with online impersonation and fraudulent accounts. Issues related to social media, such as confidentiality, online abuse, misuse, bullying, etc. are most used by fake accounts that appear to have been generated on behalf of organizations or individuals, which can damage the reputation and reduce the number of likes and followers of individuals. On the other hand, fake account creation is expected to cause more damage than any other form of cybercrime.

This issue motivates us to develop a fraudulent social media account detection system using machine learning. In online social networks, fake profiles are commonly used by intruders to carry out malicious activities such as harassing a person, identity theft, and privacy violations. As a result, determining whether an account is genuine or fraudulent is one of the most difficult tasks on the online social network site. We introduced several classification techniques in this work, including the Support Vector Machine algorithm and a deep neural network. It also compares classification methods on the Spam User dataset.

Keywords: food waste, environmental impact, freshness detection, IoT-based system, sensors, algorithms, volatile organic compounds (VOC), real-time information, application.

I. INTRODUCTION

With the tremendous increase in internet usage since its inception, cybercrime and online scamming have become extremely abundant. This surge in online scams is only helped by the presence of social media, which serves as one of the most popular platforms for scammers to target their victims. Social media platforms such as Instagram, Facebook, WhatsApp, Twitter, have become the primary hub for scamsters, and these platforms facilitate their dangerous activities. The fraudsters carry out such scams using fake accounts which help them hide their identity. To prevent such scams, we need a tool that helps us differentiate between fake and legitimate profiles.

Issues related to social media, such as confidentiality, online abuse, misuse, bullying, etc. are most used by fake accounts that appear to have been generated on behalf of organizations or individuals, which can damage the reputation and reduce the number of likes and followers of individuals. Social media is widespread these days. They are used both for communication, learning, meeting new people, and for business and advertising. One of the problems with social networks is fake accounts, which are used for various anonymous actions. Fake accounts can be used both for deception, blackmail, and extortion, which adversely affects people's trust in each other on social networks, and for spreading fake news, recruiting into terrorist organizations, and driving people to suicide. However, it should be noted that fake accounts are used not only for harm, but also for various personal purposes that do not affect ordinary users, but such accounts interfere with researchers working in the field of social network analysis. In this regard, it was decided, within the framework of this work, to conduct a study to identify fake on the social network.

People use Twitter to share their feelings, news, events and to post their daily activities such as eating, drinking, travelling and so forth. Therefore, malicious users can check everyone's activities from their timeline and twitter becomes a place for hateful users to commit the frauds. These users which are having hostile intentions create fake accounts and spread various fake news, fake links, and photos. Most internet users are not aware of these fake accounts; they accepted the requests and suffer in the process. Therefore, detecting fake accounts on twitter is obligatory for everyone who uses it.

II. LITERATURE SURVEY

In this study [1], author proposed the fake profile detection model that incorporates sentiment-based attributes to differentiate real and fake OSN profiles. The study is grounded in the fact that the posts of real users reveal

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

varied categories of emotions such as joy, sadness, anger, fear, etc. based on their life experiences. On the contrary, fake users share posts to accomplish a specific purpose, and therefore, it is highly likely that their post content will contain similar types of emotions. The experiments are conducted on the posts of Facebook users. The detection model is trained on 12 emotion-based attributes including Plutchik's eight basic emotions, positivity, and negativity. Furthermore, a noise removal technique is presented to remove the outliers from the dataset. Finally, several machine learning techniques including Support Vector Machine (SVM), Naive Bayes, and Random Forest have been used to train the detection model.

In this paper [2] an effort is accomplished to give an idea of profile cloning recognition in Online Social Networks (OSN) utilizing Network Theory. This study examines Node Similarity Communication Matching algorithm utilizing profile cloning recognition in Online Social Network depending on malicious user's latest activities in the social network. In this proposed method, the various activities to be studied includes the activities such as Updates, Wall posts and comments, By recent activities etc. Malicious, which hacks users' identity is identified based on the comparison of threshold values of user's personal profile attributes and network similarity analysis. The processes used in the research include Creating Account, user operation, monitoring, searching recent activity, detecting cloned profile process, selecting profile to be examined, and deciding Real/Fake profile. The processes are additionally examined with experiments and the outcomes clearly revealed that the proposed algorithms are beneficial and effective when compared with the known methods. It is exhibited with large number of profile data that the method used can find the cloning profile with about 93.87 Percent accuracy.

This paper surveys [3] on the existing work on a) fake profile detection b) personality trait recognition c) depression detection based on using machine learning algorithms in social network analysis and presents a comparative study of the different approaches.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

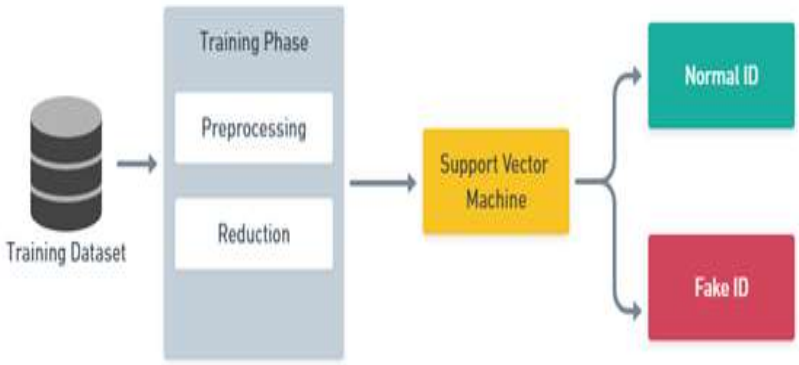

Figure 1 – System Architecture

In our research work, a novel approach has been presented for the identification of fake profiles on social media using supervised machine learning algorithms. The proposed model has applied data preprocessing techniques to datasets before analyzing them. A technique has been applied to identify the non-significant attributes in datasets and to do attribute reduction. The proposed model was trained using supervised machine algorithms individually for the dataset including fake and genuine users. An ensemble classifier has been used to make the prediction more accurate.

Support Vector Machine (SVM) is an elegant and robust method for binary classification in a large dataset, as demonstrated by the model proposed in this project. Regardless of the non-linearity of the decision boundary, SVM can distinguish between fake and genuine profiles with a high degree of accuracy (>90%). This method can

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

be extended to any platform that requires binary classification on public profiles for a variety of purposes. This project only uses publicly available information, which is convenient for organisations that want to avoid any breach of privacy, but organisations can also use private data to further extend the capabilities of the proposed model. Detecting fake social media accounts using the Support Vector Machine (SVM) algorithm involves several steps:

- **Data Collection:** Gather a labelled dataset consisting of real and fake social media accounts. This dataset should include a set of features (e.g., account creation date, number of followers, posting frequency, profile information) that can be used to distinguish between real and fake accounts.
- **Data Pre-processing:** Prepare the data for SVM by performing various pre-processing steps, such as removing irrelevant features, handling missing values, and normalizing numerical features. Additionally, split the dataset into training and testing subsets.
- **Feature Extraction:** Extract relevant features from the dataset that can capture the characteristics of fake social media accounts effectively. This could involve techniques like text analysis (e.g., sentiment analysis, keyword extraction), network analysis (e.g., connectivity patterns), or behavioural analysis (e.g., posting frequency, interaction patterns).
- **Feature Selection:** Identify the most informative features from the extracted set to improve the SVM model's performance. This step helps in reducing noise and dimensionality, making the model more efficient and accurate. Common techniques for feature selection include correlation analysis, recursive feature elimination, or information gain.
- **Model Training:** Train an SVM classifier using the labelled training data and the selected features. SVM aims to find an optimal hyperplane that separates the real and fake accounts in the feature space, maximizing the margin between the two classes. The training process involves solving an optimization problem to determine the best hyperplane.

IV. RESULT

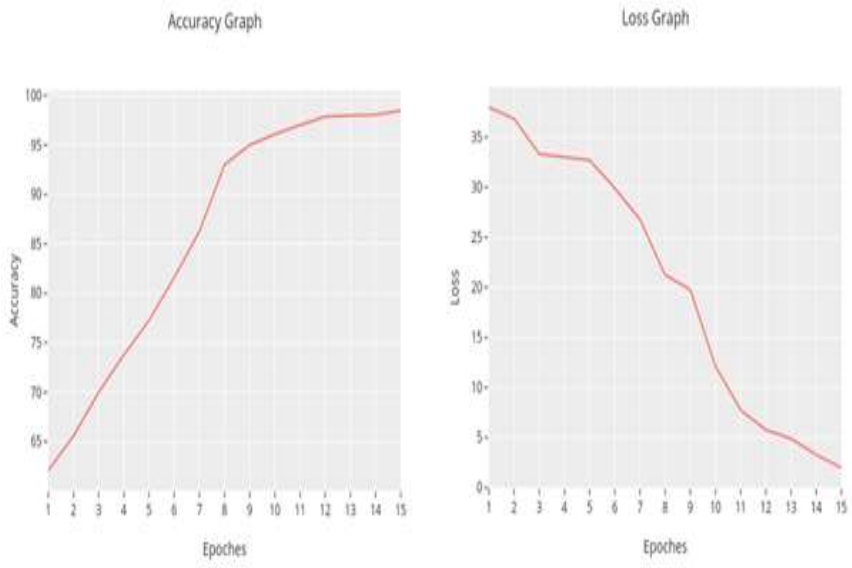

Figure 2 – Accuracy and Loss

As an output, our algorithm uses user profile information to predict if a given profile is fake or genuine. The proposed work has reported accuracy rates ranging from 85% to over 95%, depending on the dataset, model architecture, and evaluation metrics used.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

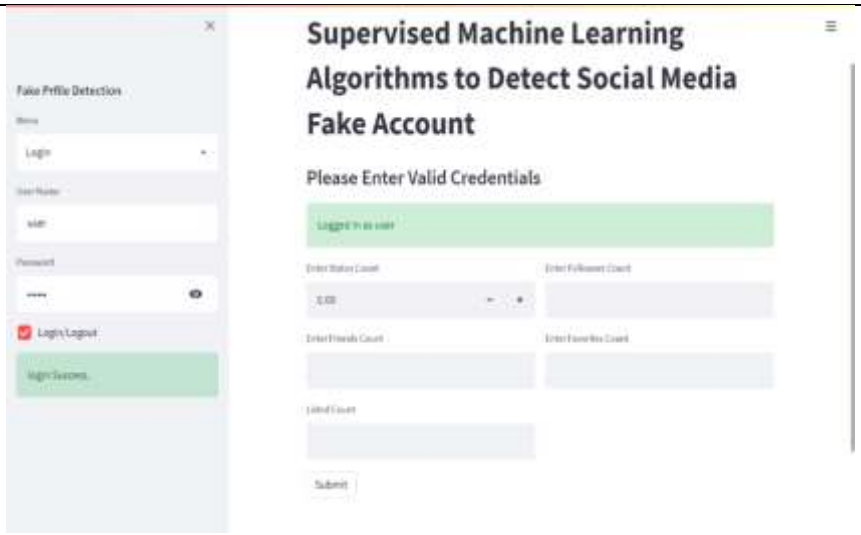

Figure 3 - Home Page

V. CONCLUSION

The detection of fake social media accounts through machine learning is a crucial step towards ensuring the integrity and trustworthiness of online platforms. By harnessing the capabilities of machine learning algorithms, we can effectively combat the proliferation of fraudulent accounts and the associated harmful activities they engage in. This technology enables the analysis of various data points such as user behavior, content patterns, and network structures, allowing for accurate identification and mitigation of fake accounts. Furthermore, the implications of fake social media account detection extend far beyond mere user experience. The prevalence of misinformation, propaganda, and online scams significantly impacts society, politics, and even public safety. Machine learning algorithms have the potential to address these issues by systematically filtering out inauthentic accounts, thereby reducing the spread of false information and manipulation. However, it is important to continuously enhance and refine these machine learning models to stay ahead of ever-evolving tactics employed by those seeking to deceive. Collaboration between researchers, social media platforms, and policymakers is crucial in developing robust detection systems that adapt to new and emerging threats. By leveraging the power of machine learning, we can create a digital landscape that fosters transparency, credibility, and meaningful connections, ultimately benefiting individuals, communities, and society as a whole.

VI. REFERENCES

[1] S. Revathi and D. M. Suriakala, "Profile Similarity Communication Matching Approaches for Detection of Duplicate Profiles in Online Social Network," 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 2018, pp. 174-182

[2] Romanov, A., Semenov, A., Veijalainen, J.: Revealing fake profiles in social networks by longitudinal data analysis. In: 13th International Conference on Web Information Systems and Technologies, January 2017

[3] Song, J., Lee, S., Kim, J.: CrowdTarget: target-based detection of crowdturfing in online social networks. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 2015, pp. 793–804. ACM, New York (2015)

[4] Nazir, A., Raza, S., Chuah, C.-N., Schipper, B.: Ghostbusting Facebook: detecting and characterizing phantom profiles in online social gaming applications. In: Proceedings of the 3rd Conference on Online Social Networks, WOSN 2010. USENIX Association, Berkeley, CA, USA, p. 1 (2010)

[5] Adikari, S., Dutta, K.: Identifying fake profiles in Linkedin. Presented at the Pacific Asia Conference on Information Systems PACIS 2014 Proceedings (2014)

[6] Stringhini, G., Kruegel, C., Vigna, G.: Detecting spammers on social networks. In: Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC 2010, pp. 1–9 (2010)

[7] Yang, C., Harkreader, R.C., Gu, G.: Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers. In: Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection, RAID 2011, pp. 318–337. Springer, Heidelberg (2011)

[8] Elyusufi, Y., Seghiouer, H., Alimam, M.A.: Building profiles based on ontology for recommendation custom interfaces. In: International Conference on Multimedia Computing and Systems (ICMCS) Anonymous IEEE, pp. 558–562 (2014)

[9] Elyusufi, Y., Alimam, M.A, Seghiouer, H.: Recommendation of personalized RSS feeds based on ontology approach and multi-agent system in web 2.0. J. Theor. Appl. Inf. Technol. 70(2), 324–332 (2014) Social Networks Fake Profiles Detection 39

[10] Elyusufi, Z., Elyusufi, Y., Ait Kbir, M.: Customer profiling using CEP architecture in a Big Data context. In: SCA 2018 Proceedings of the 3rd International Conference on Smart City Applications Article No. 64, Tetouan, Morocco, 10–11 October 2018. ISBN: 978-1-4503- 6562-8

[11] Granik, M., Mesyura, V.: Fake news detection using naive Bayes classifier. In: Conference: IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), May 2017

[12] Ameena, A., Reeba, R.: Survey on different classification techniques for detection of fake profiles in social networks. Int. J. Sci. Technol. Manage. 04(01), (2015)

[13] Beatriche, G.: Detection of fake profiles in Online Social Networks (OSNs), Master's degree in Applied Telecommunications and Engineering Management (MASTEAM), (2018)

[14] S. Revathi and D. M. Suriakala, "Profile Similarity Communication Matching Approaches for Detection of Duplicate Profiles in Online Social Network," 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 2018, pp. 174-182.