Social Media Fake Account Detection Using Machine Learning

Ms.Rohini Ushir
Department of Computer Technology
K. K. WAGH POLYTECHNIC, Nashik
rkushir@kkwagh.edu.in

Kaveri Ashok Yeola Student of ComputerTechnology
K K WAGH POLYTECHNIC, Nashik
kaveriyeola2006@gmail.com

Jayashri Yogesh Gharate Student of Computer Technology
K K WAGH POLYTECHNIC, Nashik
jayashrigharate04@gmail.com

Samiksha Sunil Bhadane Student of ComputerTechnology
K K WAGH POLYTECHNIC, Nashik
samikshabhadane28@gmail.com

Tanvi Narendra Sawant
Student of ComputerTechnology
K K WAGH POLYTECHNIC, Nashik
Tanvisawant8698@gmail.com

----------***----------

Abstract:

The rise of social media platforms has led to an increase in the number of fake accounts, posing a significant challenge in maintaining user trust and platform integrity. To address this, machine learning algorithms have been employed for the detection and identification of fake accounts. In this project, we explore several supervised machine learning techniques, including Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forest, Logistic Regression, and Artificial Neural Networks (ANN). These algorithms analyze account behaviors, interactions, and other user-specific features to classify accounts as legitimate or fake. By leveraging diverse datasets and evaluating various feature sets, the models aim to improve the accuracy of fake account identification, offering a robust solution for enhancing social media safety. Each algorithm brings unique strengths to the identification process. SVM excels in handling high-dimensional data, while KNN is useful for local proximity-based classification. Logistic Regression offers a probabilistic framework that is simple and interpretable, whereas ANN, with its multi-layered structure, enables complex pattern recognition. Our comparative analysis of these techniques highlights their effectiveness and trade-offs, providing a comprehensive approach to detecting fake accounts and aiding in developing more secure social media platforms.

Keywords:- Support vector machines (SVM), K-Nearest Neighbours Algorithm (KNN), Random Forest, Logistic Regression & Artificial Neural Network (ANN), Python.

I.INTRODUCTION

In recent years, social media platforms have become a ubiquitous part of our daily lives. With the rise of fake accounts and bots, it has become increasingly challenging to distinguish between real and fake accounts. These fake accounts can be used for various malicious purposes, such as spreading misinformation, phishing, and identity theft. In this paper, we will discuss a machine learning-based approach for identifying fake social media accounts. Our proposed method involves a multi-step process that combines various features to accurately identify fake accounts. The first step involves data collection and preprocessing. We will collect a large dataset of social media profiles, both real and fake, from various platforms such as Facebook, Twitter, and Instagram. The data will be cleaned and preprocessed to remove any irrelevant information and prepare it for further analysis. The second step

involves feature extraction. We will extract various features from the preprocessed data, such as user behavior, network structure, content analysis, and account metadata. These features will be used to train our machine learning models. The third step involves model selection and training. We will experiment with different machine learning algorithms such as Support vector machines (SVM), K-Nearest Neighbors Algorithm (KNN), Random Forest Logistic Regression & Artificial Neural Network (ANN) to find the best-performing model for our task. The models will be trained on the preprocessed data and evaluated using various metrics such as accuracy, precision, recall, and F1 score. Once we have selected the best-performing model, we will deploy it on a production environment to identify fake accounts in real-time. We will also continuously monitor the performance of the model and fine-tune it as needed to improve its accuracy over time. Our proposed method for identifying fake social media accounts using machine learning is a multi-step process that combines data collection, feature engineering, model selection and training, and model deployment and evaluation. By leveraging the power of machine learning algorithms, we can accurately distinguish between real and fake social media accounts and mitigate the negative impacts of fake accounts on social media platforms.

II. LITERATURE SURVEY

1) In proposed system different classification methods to point out the fake accounts on social media. But we must increase the accuracy rate in identifying fake accounts on these sites. Machine Learning technologies and Natural Language processing (NLP) to increase the accuracy rate of detecting the fake accounts. We opted for Random Forest tree classifier algorithm. Here this idea came up with machine learning algorithms besides NLP techniques. From the social media sites, we can easily find the fake profiles by implementing these techniques. In this Paper to point out the fake profiles we have taken the Instagram dataset. Examine the dataset, used the NLP pre-processing techniques and to organize the profiles we used machine learning algorithm such as Random Forest classifier and Gradient Boost classifier.[1]

2) Online Social Networks (OSN) are contributed in all areas such as Research in all domains, Job-related areas, Technology oriented areas, Health care, and business-oriented areas, Information gathering and data collection, and so on. One of the biggest problems on these social media platforms is fake profiles. Impersonating to be someone else and causing harm and defamation to the real person or advertising or popularizing removed propaganda on someone's name to get more benefit is the motto of such profile creators. There have been many studies regarding these fake accounts and how can they be mitigated. Many approaches such as graph-level activities or feature analysis have been taken into consideration to identify fake profiles. These methods are outdated when compared to a rising issues of these days. In this paper, we proposed a technique using machine learning for fake profile detection which is efficient. The benchmark data set is collected and mixed with manual data first furthermore; a data cleaning technique is used to present the data more feasibly. Then the preprocessed data is used for model building with sufficient information such as profile name, profile ID name, number of followers, and so on. We added Cross validation process where many training algorithms are implemented on the given data and are then tested on the same data. Based on the experiments the RF classifier performed better than the other classification methods. The Random Forest classifier is used to forecast the profile whether is fake or genuine in an efficient way. [2]

Problem Definition

The rise of fake accounts on social media platforms poses significant challenges to user privacy, platform integrity, and public trust. These accounts are often used for malicious purposes such as spreading misinformation, phishing, and manipulating public opinion. Traditional methods of detecting fake accounts are insufficient due to the large scale and complexity of social media data. The problem, therefore, is to develop an effective and scalable solution for identifying fake social media accounts using machine learning (ML) algorithms. This study aims toapply and compare the performance of five widely-used ML

algorithms Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forest, Logistic Regression, and Artificial Neural Networks (ANN)—to determine the most accurate and efficient approach for detecting fake accounts based on user behavior, profile features, and activity patterns.

III. SYSTEM DESIGN

In proposed system, gather a large dataset of social media profiles, including both genuine and fake accounts. This can be done by scraping social media platforms or using publicly available datasets. Clean the data by removing duplicate profiles, irrelevant information, and missing values. Convert textual data into numerical format using techniques like bag-of-words or word embedding. Extract relevant features from the preprocessed data, such as the number of followers, engagement rate, frequency of posts, use of emoji's, and language patterns. Choose a suitable machine learning algorithm for identifying fake social media accounts based on the nature of the problem. Popular algorithms include Support vector machines(SVM), K-Nearest Neighbors Algorithm(KNN), Random forest, Logistic Regression, & Artificial Neural Network(ANN). Train the selected model on the preprocessed dataset using a suitable optimization technique like gradient descent or stochastic gradient descent. Split the dataset into training and testing sets to evaluate the model's performance. Evaluate the trained model's accuracy, precision, recall, and F1 score on the testing set to determine its effectiveness in identifying fake social media accounts. Use techniques like cross-validation and grid search to optimize the model's hyperparameters for better performance. Deploy the trained model in a production environment to identify fake social media accounts in real-time. Monitor its performance regularly and fine-tune it as needed to improve its accuracy over time.

• **Dataset:** The system begins with a dataset (sourced from Kaggle) containing both genuine and fake social media profiles.

• **Data Preprocessing:** Initial data is cleaned and prepared by removing duplicates, irrelevant fields, and handling missing values.

• **Data Split:** The dataset is divided into training (80%) and testing (20%) sets for model training and evaluation.

• **Feature Extraction:** Key features, such as follower count, engagement rate, and posting patterns, are extracted from both training and testing sets.

• **Machine Learning Algorithms:** Several models (SVM, KNN, Random Forest, Logistic Regression, and ANN) are used to train the predictive model on identifying fake accounts.

• **Feature Matching & Testing:** The testing phase evaluates the model by matching features to predict whether an account is fake.

• **Result:** The system outputs whether each tested profile is genuine or fake, providing an effective tool for social media fake account detection.

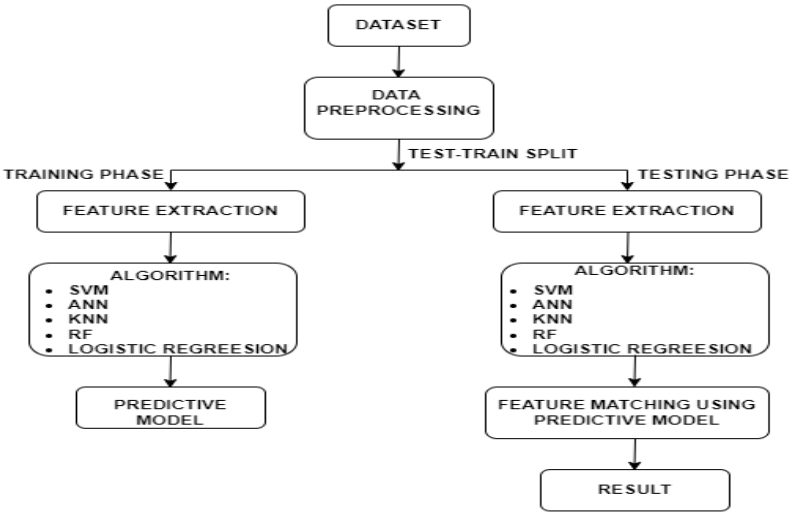

Fig -1: Proposed System Architecture

IV.PROPOSE WORKING

The proposed system aims to develop an efficient and scalable machine learning-based fake account detection model for social media platforms. This system will analyze user behavior, network structure, and content characteristics to identify fake accounts accurately.

- **Data Collection & Preprocessing** – Gather and clean data, extract relevant features.
- **Feature Engineering** – Analyze user activity, text content, and network connections.
- **Model Training** – Use machine learning (Random Forest, SVM, XGBoost) and deep learning for detection.
- **Real-time Detection** – Implement automated monitoring and flagging of fake accounts.
- **Privacy Protection** – Ensure compliance with data protection laws while maintaining accuracy.
- **Evaluation & Improvement** – Continuously test and refine the model for better performance.
- **Deployment & Collaboration** – Integrate with social media platforms for large-scale implementation.

FUTURE SCOPE

The future of social media fake account detection using machine learning lies in enhancing accuracy, adaptability, and scalability. While the current model achieves 95% accuracy, exploring advanced algorithms and deep learning techniques can further improve detection rates. As fake account tactics evolve, the system must adapt dynamically to new patterns. Scalability is another key factor, requiring optimization to handle large user bases efficiently. Moving from post-creation detection to real-time identification will help prevent fake accounts from causing harm. Additionally, ensuring user privacy while maintaining security is crucial. Collaboration with social media platforms can provide better datasets and insights, leading to more effective models. Finally, continuous evaluation using real-world scenarios will help refine the system, making it more robust and reliable.

V. CONCLUSION

The proliferation of fake accounts on social media platforms has become a major concern for online communities. To address this issue, machine learning algorithms have been proposed as a solution for identifying fake accounts based on various features such as user behavior, network structure, and content analysis. The success of these algorithms depends heavily on the quality and relevance of the extracted features, the choice of machine learning algorithm, cross-validation techniques for training, evaluation using metrics such as accuracy, precision, recall, and F1 score, and deployment in production environments. By following these best practices, social media companies can develop effective machine learning-based fake account identification systems that promote a safer and more trustworthy online community for their users**.**

VI. REFRENCES

[1] Latha P, Sumitra V,"Fake Profile Identification in Social Network using Machine Learning and NLP", 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT) | 978-1-6654-7995-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3IOT53935.2022.9767958, 978-1-6654-7995 0/22/$31.00 ©2022 IEEE

[2] Kotra Shreya, Amith Kothapelly," Identification of Fake accounts in social media using machine learning", 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), 978-1 6654-5635-7/22/$31.00 ©2022 IEEE

[3] Adikari, Shalinda, and Kaushik Dutta. "Identifying Fake Profiles in LinkedIn." In PACIS, p. 278. 2014.

[4] Yeh-Cheng chen and ShystunfelixWu,Fake Buster: A Robust fake Account detection by Activity Analysis,2018

[5] Malicious Account Detection on Twitter Based on Tweet Account Features using Machine Learning.