Fake Profile Detection on Social Media

P. S. Birajdar[1], Reshma V. Kokate[2], Pratibha V. Mandkal[3], Priya P. Sakat[4], Sonali V. Rathod[5], Pratiksha S. Murte[6]

[1]Technical Ass., Shree Siddheshwar Women's College of Engineering,Solapur.

[2,3,4,5,6] Department of Computer Science and Engineering, Shree Siddheshwar Women'sCollege of Engineering, Solapur.

***Abstract*—In an age where social media has become an integral part of our lives, the challenge of detecting fake accounts on platforms like Instagram has gained significant importance. This project, titled "Instagram Fake Account Detection using Machine Learning," employs Python as its primary tool to tackle this problem. It leverages two powerful machine learning algorithms, the Random Forest Classifier and the Decision Tree Classifier, to accomplish this task. , the Decision Tree Classifier exhibits its effectiveness with a training accuracy of 92% and a test accuracy of 92%.**

***Index Terms*—K Nearest Negibour, Logistic Regression, Support Vector Machine, XG boost.**

I. INTRODUCTION

False profiles are frequently made under fictitious identities, and they spread defamatory and abusive posts and images to influence society or advance anti-vaccine conspiracy theories, among other things. Phony personas are an issue on all social media platforms nowadays.

Most false profiles are made with spamming, phishing, and gaining more followers in mind. The fraudulent accounts are completely capable of committing online crimes.

Fake accounts represent a serious risk, including identity theft and data breaches. When consumers access the URLs sent by these false accounts, all user information is sent to distant servers where it may be used against them. Furthermore, phony profiles purportedly created on behalf of businesses or individuals can damage their reputation and reduce the number of follows and likes they receive. Social media propaganda is a challenge in addition to all of these. Conflicts arise as a result of false accounts spreading inaccurate and inappropriate information.

II. OBJECTIVES

The objective of this research is to develop a machine learning-based solution for detecting fake profiles on social networking websites. This entails creating algorithms that can analyze various aspects of user profiles, including attributes, behavior patterns, and engagement metrics, to accurately identify fraudulent accounts. Techniques such as natural language processing will be employed to analyze profile descriptions and textual content, while anomaly detection algorithms will detect irregular activity indicative of fake profiles.

III. PROBLEM STATEMENT

The increasing prevalence of fake profiles on social media platforms poses significant challenges, including the spread of misinformation, phishing scams, identity theft, and decreased trust among users.

IV. EXISTING SYSTEM

When building social media accounts, techniques like user verification must Used. User behaviour research must be used to find suspicious activity. It will be advantageous to use a bot detection system that uses real-time AI analysis. You must make use of automatic bot prevention technology. By making the LSTM, XG boost, random forest, and multi-layered neural network models, the author made a contribution to technology. These methods are some instances of machine learning with supervision.

Additionally, LSTM uses tweets to categorize data, and soon its output will be able to be paired with such a convolutional CNN architecture. Several sections make up the document. Prior research, data preprocessing, technique, experimental results, model accuracy, conclusion, and forthcoming investigations are all presented in an organized manner.

There are following Disadvantages-
Limited Explanation of Predictions, Sensitivity to Imbalanced Datasets, Privacy Concerns, Dependency on Data Quality.

V. PROPOSED SYSTEM

The proposed system builds upon the strengths of the existing system, which achieved impressive accuracy levels, while also addressing potential limitations. It incorporates algorithm diversity, robust feature engineering, interpretability, adaptability to emerging threats, and enhanced efficiency to deliver a comprehensive and effective solution for Instagram fake account detection. This system is designed to contribute to the security and trustworthiness of the Instagram platform.There are following advantages- Enhanced Accuracy, Less time duration to predicting the successful attributes by using student grade data, Scalability and Efficiency, Reliable Data Balancing.

VI.LITERATURE SURVEY

1.K. Harish, R. Naveen Kumar, Briso Becky Bell J, Fake accounts are regularly made by people, software, or machines. They are employed in the spread of rumors and illegal actions like phishing and identity theft. They are employed in the spread of rumors and illegal actions like phishing and identity theft. Based on the information that is easily accessible, they employed the CNN model, Random forests, and XG Boost supervised learning approaches in this architecture to train the system on how to identify fake accounts.

2.Faiza Masood, Ghana Ammad, Ahmad Almogren, Assad Abbas, we perform a review of techniques used for detecting spammers on Twitter. A taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: fake content, spam based on URL, spam in trending topics, and fake users. we presented a taxonomy of Twitter spam detection approaches and categorized them as fake content detection, URL based spam detection, spam detection in trending topics, and fake user detection techniques. We also compared the presented techniques based on several features, such as user features, content features, graph features, structure features, and time features.

3.Sannella Prabhaker, These features encompass critical aspects of Instagram profiles, including the presence of a profile picture, the ratio of numerical characters in usernames, the breakdown of full names into word tokens, the ratio of numerical characters in full names.

VI. SYSTEM ARCHITECTURE

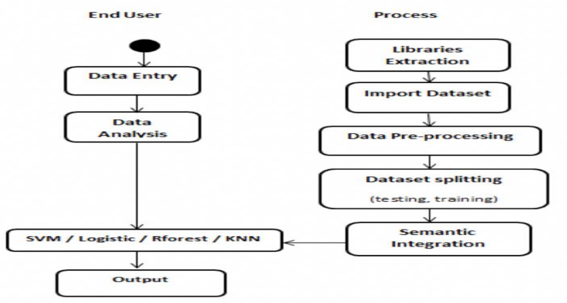

Fig 1. System Architecture

1. K-Nearest Neighbour:

It is used for both pattern recognition along with classification. In KNN, a specific test tuple set is compared to the training data set already available which is identical to the test data set. It calculates the distance between the training data and the testing data using the Euclidean distance function. Class membership is the output of the KNN classification.

2. Random Forest Algorithm:

The Random Forest consists of a large number of individual trees which functions as an ensemble individual tree divides a random forest class prediction, and the class with the most votes is our model’s prediction. Random forest (RF) is similar to bootstrapping algorithm along with Regression tree Classification and Decision Trees(CART).We have 1000 observations of 10 parameters in the entire population. RF attempts to create several CART models with different initial variables with samples.

3. Support Vector Machines (SVM)

Support Vector Machine (SVM) is also a type of computer algorithm that can be trained to assign labels to the objects. It is a powerful tool for solving both classification and regression problems. It is one of the supervised learning methods and one of the best-known classification methods. SVMs are based on statistical learning theory, which is used to solve two-class binary problems without the loss of generality.

4. Logistic Regression:

Logistic Regression (LR) it is a type of linear algorithm, which is the method of relating dependent and independent variables using a logistic distribution functional form. It obtains a linear relationship between the output and input. LR measures the probability of class inclusion for one of the data set’s different categories. This is used for modelling the binary response data. If the response is in binary, it takes the form of the success and indicates failure.

Use case Diagram:

A use case diagram is used to represent the dynamic behavior of a system. Itencapsulates the system's functionality by incorporating use cases, actors, and their relationships. It models the tasks, services, and functions required by a system/subsystem of an application. It depicts the high-level functionality of a system and also tells how the user handles a system.

The main purpose of a use case diagram is to portray the dynamicaspect of a system. It accumulates the system's requirement, which includes bothinternal as well as external influences. It invokes persons, use cases, and severalthings that invoke the actors and elements accountable for the implementation ofuse case diagrams. It represents how an entity from the external environment caninteract with a part of the system.

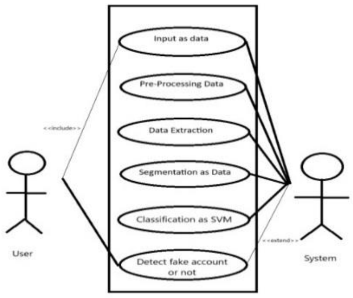

Fig 2. Use Case Diagram

ER-Diagram:

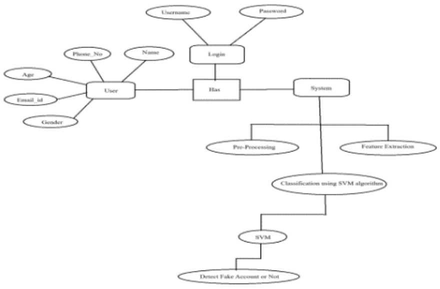

Fig 3. ER-Diagram

ER Diagram stands for Entity Relationship Diagram, also known as ERD is a diagram that displays the relationship of entity sets stored in a database. In other words, ER diagrams help to explain the logical structure of databases. ER diagrams are created based on three basic concepts: entities, attributes and relationships.

CONCLUSION

In conclusion, the research focuses on leveraging different machine learning techniques, such as Random Forests, LSTM, and neural networks, to effectively identify fake profiles on social media platforms like Facebook, Twitter, and Instagram. While many approaches rely on supervised learning algorithms to classify profiles, unsupervised methods and advanced techniques like Natural Language Processing and gradient boosting algorithms also show promise in improving accuracy. The advantages of these methods include their ability to detect malicious accounts, help improve security, and provide efficient time management for academic and organizational purposes. However, challenges remain, such as evolving fake profile tactics, privacy concerns, and the ethical implications of data collection. Despite these hurdles, the integration of deep learning and AI technologies offers exciting potential for more robust and real-time detection systems in the future.

ACKNOWLEDGMENT

It plunges us in exhilaration taking privilege in expressing our heartfelt gratitude to all those who helped, encouraged and foreseeing successful completion of our project. Ecstasies to work under gregarious guidance of Prof P.S.Birajdar to whomwe are extremely indebted for his valuable and timely suggestions. We wish to convey our sincere thanks to Prof. S.M.Gungewale Head of the Dept. of Computer Science & Engineering, for her support. We are also thankful to Dr. T. A. Chavan, Principal, Shree Siddheshwar Women’s College of Engineering, Solapur for making requisite facilities available to us. We would like to give our thanks to all teaching and non-teaching staff members for their keen interest and excellent support. We would also like to thanks to all those who had directly or indirectly contributed their assistance in finishing out this project successfully.

REFERENCES

[1] Meshram, E.P., Bhambulkar, R., Pokale, P., Kharbikar, K. and Awachat, A. (2021) Automatic Detection of Fake Profile Using Machine Learning on Instagram117-127. https://doi.org/10.32628/IJSRST218330

[2] G.Swathi, R.Vaishnavi, S.N.Sabiha, P.R.Anand, P.N.Kumar, , “Ensemble fake profile detection using

machine learning (ML)," J. Inf. Comput. Sci., vol. 10, pp. 1071–1077, 2023. https://www.ijset.in/wpcontent/uploads/IJSET_V11_issue6_627.pdf

[3] Sarker, A., Chakraborty, P., Sha, S.S., Khatun, M., Hasan, M.R. and Banerjee, K. (2020) Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data. Journal of Computer and Communications,8,50-62. https://doi.org/10.4236/jcc.2020.87005