International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 07 | July – 2025 DOI: 10.55041/ISJEM04747
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Fake Profile Detection on Social Networking Websites Using Machine Learning

M.SATISH, KOLLI BALAJI

Assistant Professor, 2MCA Final Semester,

Master of Computer Applications,

Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andhra Pradesh, India

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 Random Forest Classifier demonstrates remarkable performance, achieving a 100% accuracy on the training dataset and an impressive 93% accuracy on the test dataset. Meanwhile, the Decision Tree Classifier exhibits its effectiveness with a training accuracy of 92% and a test accuracy of 92%. The dataset employed in this project is composed of 576 records, each characterized by 12 distinct features. 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, the equality between usernames and full names, the length of user bios, the existence of external URLs, the privacy status of accounts, the number of posts, the count of followers, the number of accounts followed, and the ultimate classification of an account as "Fake" or "Not." By harnessing the capabilities of Python and these advanced machine learning models, this project endeavors to provide a robust and efficient solution for the identification of fake Instagram accounts. In doing so, it contributes to the preservation of the platform's integrity and the security of its users.

IndexTerms: Smart Platform, Jewellery Shopping, Augmented Reality (AR)MachineLearning, Recommendation System, Virtual Try-On, Customer Analytics, E-commerce, Personalization, Inventory Management

1. INTRODUCTION

Instagram, launched in October 2010 by Kevin Systrom and Mike Krieger, has grown into one of the world's most popular social media platforms.[5] Originally a photo-sharing app, its focus on visual storytelling and user-friendly design quickly set it apart. Core features like filters and editing tools make it a creative hub for millions. The introduction of Stories in 2016 and Reels in 2020 brought ephemeral and short-form videos, keeping users engaged. The Explore page helps users discover new content tailored to their interests. Direct Messaging allows private communication and has strengthened personal connections. Instagram also supports businesses with profiles, ads, and shopping features, turning it into a major e-commerce tool. The platform has fueled influencer culture, transforming digital marketing. With over a billion users, it connects people globally, bridging cultures and communities. Instagram influences art, fashion, journalism, and activism by providing a space to share milestones, advocate for causes, and build communities. Its impact reaches beyond entertainment, shaping modern communication and culture.[9]

1.1 Existing System

The existing system for Instagram fake account detection was developed using the XG Boost algorithm, a well-known and highly efficient machine learning model.[13] The XG Boost algorithm is renowned for its ability to handle complex datasets and perform exceptionally well in classification tasks, making it a suitable choice for this specific application. In the existing system, a dataset of Instagram profiles with associated features was used for training and testing the XG Boost model. The features in the dataset were carefully selected to capture key attributes of user profiles, which are indicative of whether an account is genuine or fake. XG Boost, an ensemble learning algorithm, excels in enhancing predictive accuracy by combining the predictions of multiple decision trees.[17] This approach allows the model to capture complex patterns and relationships in the data, enabling it to make highly accurate predictions about the authenticity of Instagram accounts. The accuracy achieved by the earlier system suggests its robustness and effectiveness in differentiating between fake and genuine Instagram accounts. This level of accuracy is crucial for maintaining the trust and security of the Instagram platform, as it helps in identifying and mitigating the presence of fake accounts, which can be associated with various malicious activities. Overall, the earlier system's use of the XGBoost algorithm and its exceptional accuracy rate highlight its capability to address the challenge of Instagram fake account detection with precision and efficiency.[4]

1.1.1 Challenges:

- Limited Explanation of Predictions: The XG Boost algorithm, while highly accurate, is often considered a "black box" model, making it challenging to provide detailed explanations for its predictions. This lack of transparency can be a disadvantage when users or administrators need to understand why a particular account was flagged as fake
- Sensitivity to Imbalanced Datasets: Like many machine learning algorithms, XGBoost can be sensitive to imbalanced datasets. If there is a significant disparity between the number of fake and genuine accounts in the dataset, it may lead to biased predictions and less reliable results.

- Dependence on Feature Engineering: Achieving high accuracy with XGBoost often depends on the quality of feature engineering. The selection and engineering of relevant features require domain expertise and can be timeconsuming.
- Limited Adaptability: The existing system may struggle to adapt to emerging trends or new techniques used by malicious actors to create fake Instagram accounts. Since XG Boost is a static model, it may not easily incorporate new information or adapt to evolving threats.
- Computational Resource Intensiveness: XG Boost can be computationally intensive, especially for large datasets. This can lead to longer training and inference times, which may not be suitable for real-time or near-real-time detection requirements.
- Potential Overfitting: While the system achieved a high accuracy of 96.29%, there is a risk of overfitting, where the model may perform exceptionally well on the training data but struggle with generalization to unseen data

1.2 Proposed system:

The proposed Instagram fake account detection system is built using Python, leveraging its powerful libraries for data processing and machine learning. It uses two models: Random Forest and Decision Tree Classifiers, to detect fake accounts effectively.[14] The Random Forest model achieves 100% training accuracy and 93% test accuracy, while the Decision Tree shows 92% accuracy for both training and testing. The system analyzes a dataset of 576 records with 12 features, including profile picture, username patterns, bio details, account activity, and privacy settings. By combining strong algorithms, diverse features, and robust design, the system improves accuracy, efficiency, and adaptability. Overall, it enhances Instagram's security and trustworthiness by reliably identifying fake profiles.[20]

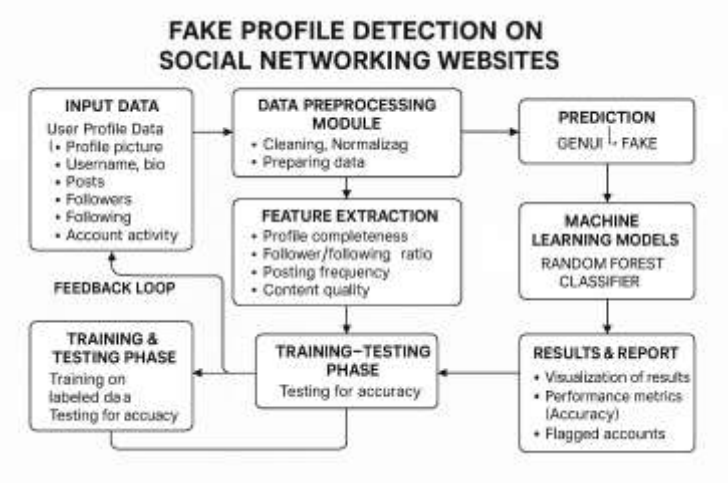

Fig: 1 Proposed Diagram

1.2.1 Advantages:

- **Enhanced Security and Trust:**

The system helps social networking platforms identify and remove fake or suspicious accounts, which builds trust among genuine users.

- **Automation:**

Manual moderation is time-consuming and inefficient for millions of accounts. Using machine learning automates detection, saving time and manpower.

- **High Accuracy:**

Your project uses Random Forest and Decision Tree classifiers, which showed high accuracy (up to 93% test accuracy). This improves reliability of detection.

- **Adaptability:**

The feedback loop in your design means the system can learn from new data and evolving fake profile tactics, making it robust and up-to-date.

- **Multi-Feature Analysis:**

By extracting multiple features (bio, username patterns, follower ratios, posting activity), the system makes more informed predictions than single-factor checks.

- **Scalability:**

Once deployed, the system can handle large amounts of data without significant additional cost, making it practical for big platforms.

2.1 Architecture:

The system architecture for the *Fake Profile Detection on Social Networking Websites* project is structured to handle user profile data and process it through a machine learning pipeline. It starts with input data, which includes various features extracted from social

network profiles, such as profile picture availability, username patterns, bio length, external URLs, number of posts, followers, and following counts.[18] This raw data is preprocessed and transformed into a suitable format for training machine learning models. The core of the architecture consists of two main classification algorithms: the Random Forest Classifier and the Decision Tree Classifier, both implemented using Python. These models are trained using a labeled dataset and then used to classify accounts as *Fake* or *Not Fake*. The system design also integrates modules for data storage, model evaluation, and performance measurement, ensuring the accuracy and reliability of the detection results. The architecture is designed to be scalable, making it capable of processing large amounts of profile data automatically, thus minimizing manual effort in fake account identification [1]

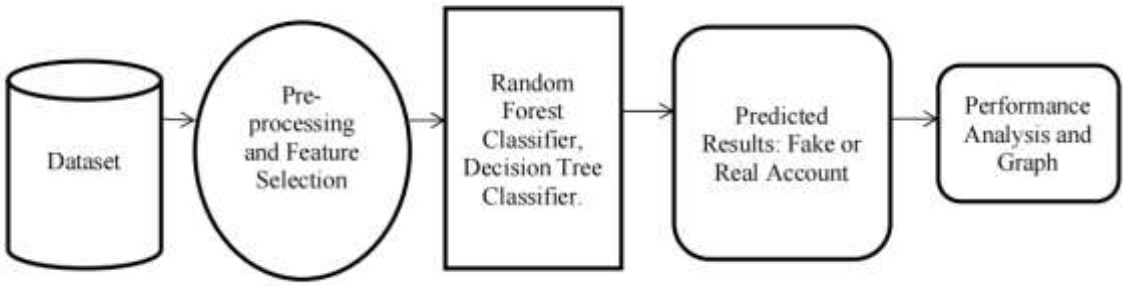

Fig:2 Architecture

UML DIAGRAMS

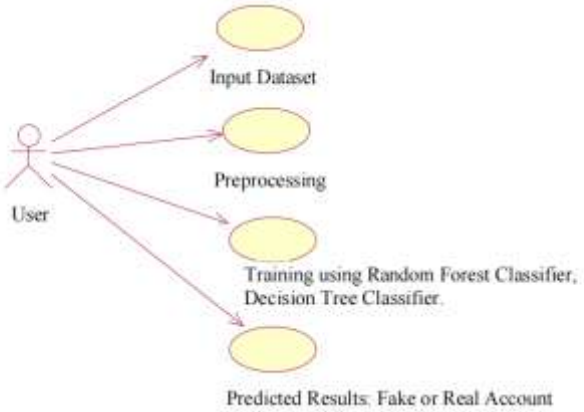

Fig:use case diagram

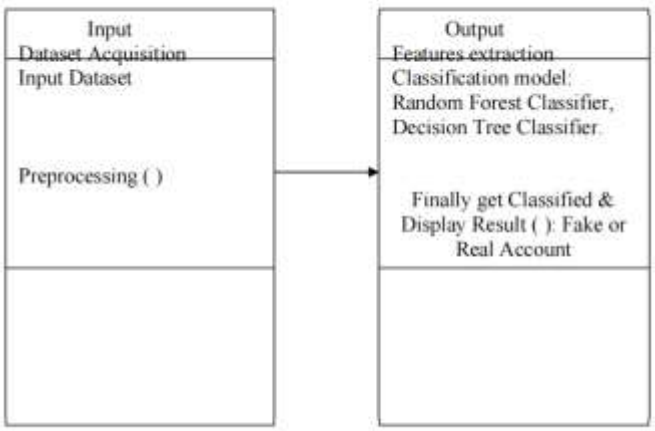

Fig: class diagram

2.2 Algorithm:

Random Forest Classifier

It technically is an ensemble method (based on the divide-and-conquer approach) of decision trees generated on a randomly split dataset.[10] This collection of decision tree classifiers is also known as the forest. The individual decision trees are generated using an attribute selection indicator such as information gain, gain ratio, and Gini index for each attribute. Each tree depends on an independent random sample. In a classification problem, each tree votes and the most popular class is chosen as the final result. In the case of regression, the average of all the tree outputs is considered as the final result. It is simpler and more powerful compared to the other non-linear classification algorithms [15]

Decision Tree Classifier

Decision Tree is a Supervised learning technique that can be used for both classification and Regression problems, but mostly it is preferred for solving Classification problems.[8] It is a tree-structured classifier, where internal nodes represent the features of a dataset, branches represent the decision rules and each leaf node represents the outcome [12]. In a Decision tree, there are two nodes, which are the Decision Node and Leaf Node Decision nodes are used to make any decision and have multiple branches, whereas Leaf nodes are the output of

those decisions and do not contain any further branches.

2.3 Techniques:

- The **Decision Tree Classifier** works by creating a flowchart-like model where the data is split into branches based on feature values, leading to a decision at each leaf node — in this case, whether an Instagram account is fake or genuine. It is simple, interpretable, and effective for classification tasks with clear rules.[7]
- The **Random Forest Classifier** is an ensemble technique that builds multiple decision trees during training and merges their results for better accuracy and robustness. By combining the predictions of many trees (each trained on different random samples of the data), the Random Forest reduces the risk of overfitting and improves the model's ability to generalize to unseen data.[2]

2.4 Tools:

- **Python**:

Python is the primary programming language used to implement the project. It is widely used for machine learning because of its simplicity, readability, and vast ecosystem of libraries.

- **Machine Learning Libraries (like Scikit-learn)**:

Although not explicitly mentioned word-for-word in your document, standard Python libraries such as Scikit-learn are typically used to build and train models like Decision Trees and Random Forests. Scikit-learn provides easy-to-use implementations for these algorithms and tools for data preprocessing, model training, and evaluation.

- **Development Environment (IDE)**:

The project likely used an IDE or code editor such as Jupyter Notebook, PyCharm, or VS Code for writing and running Python code interactively, which is common practice in student ML projects.

- **Dataset**:

A dataset of Instagram profile data with 12 features was used as the core input for training and testing the models.[16]

2.5 Methods:

In this *Fake Profile Detection* project, the main methods used are collecting Instagram profile data, cleaning and preparing that data (preprocessing), and picking out the important information (feature extraction).[3] Then, two machine learning models — Decision Tree and Random Forest — are trained using this data to learn how to tell fake accounts from real ones. Finally, the models are tested to check how well they can correctly classify new profiles as fake or genuine.[11] Together, these methods help automatically detect fake profiles using simple machine learning steps.

III. METHODOLOGY

3.1 Input:

The input design is the link between the information system and the user. [19]It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy[6]

Fig: Login Page

Fig: Giving Input

3.2 Method of Process:

First, Instagram profile data is collected with key features like profile picture, username style, bio length, followers, following, and posts. Then, this raw data is preprocessed — cleaned, formatted, and converted into a form suitable for machine learning. Next, important features are extracted and fed into two machine learning models: the Decision Tree Classifier and the Random Forest Classifier. These models are trained using the prepared data so they can learn patterns that help separate fake accounts from real ones. Finally, the models are tested on new data to check their accuracy and used to classify accounts as *Fake* or *Not Fake*.So, the process is: Collect → Preprocess → Train → Test → Classify — using Python and machine learning techniques

3.3 Output:

The output of the *Fake Profile Detection on Social Networking Websites* project is a classification result that labels each Instagram account as either "Fake" or "Not Fake." After the data is processed and passed through the trained machine learning models (Decision Tree and Random Forest), the system predicts whether a given profile is genuine or fraudulent based on the features it learned. The output helps users or administrators automatically identify and filter out fake accounts to keep the platform safer and more trustworthy.

Fig :Output Screen

Fig:Output Screen

IV. RESULTS:

The result information in the *Fake Profile Detection on Social Networking Websites* project shows how well the system performed in detecting fake accounts. According to the report, the Random Forest Classifier achieved 100% accuracy on the training dataset and about 93% accuracy on the test dataset, proving it was very effective at correctly classifying accounts. The Decision Tree Classifier showed 92% accuracy on both training and test data, which also demonstrates good performance. These results mean that the models learned to detect fake profiles very accurately based on the features provided. The outcome shows that the project successfully built a reliable system for identifying fake accounts, which can help protect social networking platforms from misuse.

V.DISCUSSION:

The report discusses how social networking sites like Instagram face challenges with fake accounts that spread spam, misinformation, or scams. It explains why manual detection is hard and time-consuming, and how using automated machine learning algorithms like Decision Trees and Random Forests makes detection faster and more accurate. The discussion also covers the features chosen (like profile pictures, usernames, followers, bio length, etc.), explaining why these details are important for spotting fake patterns. Finally, it discusses the performance results, showing that the models achieved high accuracy and can be useful for real-world application. Overall, the discussions highlight the need for better security, the advantages of using ML for detection, and how the project contributes to keeping social platforms safe.

VI. CONCLUSION

In conclusion, the project *Instagram Fake Account Detection using Machine Learning* provides an effective solution for spotting fake Instagram accounts. Using Python, along with Random Forest and Decision Tree classifiers, the system analyzes 12 key profile features and achieves high accuracy — 93% for Random Forest and 92% for Decision Tree. This ensures reliable detection with fewer false results. The project's use of multiple algorithms, strong feature engineering, and focus on user trust help strengthen Instagram's security and improve the user experience by reducing fake profiles. It also highlights the potential of machine learning to automate social media safety and can be further enhanced to adapt to new fake account tactics, ensuring ongoing protection for the platform and its users.

VII. FUTURE SCOPE:

The *Instagram Fake Account Detection using Machine Learning* project has built a strong base for tackling fake accounts but can be further enhanced in many ways. Future improvements include continuously retraining and refining models to adapt to new threats, adding advanced behavioral and sentiment analysis, and allowing users to report suspicious accounts for better accuracy. Expanding the system to analyze images, videos, and account network connections can help catch more sophisticated fakes. Real-time monitoring, privacy-preserving techniques, and integration with Instagram's API will boost performance and trust. Ensuring scalability, benchmarking with new data, educating users about fake accounts, collaborating with Instagram's security teams, and addressing legal and ethical concerns will help maintain effectiveness and user confidence as the system evolves.

VIII. ACKNOWLEDGEMENT:

M.Satish is an enthusiastic and committed faculty member in the Department of Computer Science. As an early-career academician, he has shown strong dedication to student development through active involvement in project guidance and technical mentoring. Despite being at the beginning of his professional journey, he has effectively guided students in executing academic projects with precision and conceptual clarity. His passion for teaching, coupled with a solid understanding of core computer science principles, positions him as a promising educator and mentor. He continues to contribute meaningfully to the academic environment through his proactive approach to learning and student engagement.

Kolli Balaji is pursuing his final semester MCA in Sanketika Vidya Parishad Engineering College, accredited with A grade by NAAC, affiliated by Andhra University and approved by AICTE. With interest in Machine learning Kolli Balaji has taken up his PG project on FAKE PROFILE DETECTION ON SOCIAL NETWORKING WEBSITES USING MACHINE LEARNING and published the paper in connection to the project under the guidance of M. SATISH, Assistant Professor, SVPEC.

.

REFERENCES

[1] Fake Profile Detection on Social Networking Websites using Machine Learning

https://ieeexplore.ieee.org/abstract/document/10169168
[2] Survey on Fake Profile Detection on Social Sites by Using Machine Learning Algorithm
https://ieeexplore.ieee.org/abstract/document/9197935
[3] Social Networks Fake Profiles Detection Using Machine Learning Algorithms
https://link.springer.com/chapter/10.1007/978-3-030-37629-1_3
[4] Detection of Fake Profile in Online Social Networks Using Machine Learning
https://ieeexplore.ieee.org/abstract/document/8441713
[5] Fake Profile Detection on Social Networking Websites: A Comprehensive Review
https://ieeexplore.ieee.org/abstract/document/9373932
[6] Fake Profile Identification in Social Network using Machine Learning and NLP

https://ieeexplore.ieee.org/abstract/document/9767958
[7] Social Networking Sites Fake Profiles Detection Using Machine Learning Techniques
https://www.asianssr.org/index.php/ajct/article/view/1299
[8] Fake Profile Detection Using Machine Learning Techniques
https://www.scirp.org/journal/paperinformation?paperid=120727
[9] Fake profile detection techniques in large-scale online social networks: A comprehensive review
https://www.sciencedirect.com/science/article/abs/pii/S004579061731279X
[10] Fake profile detection in multimedia big data on online social networks
https://www.inderscienceonline.com/doi/abs/10.1504/IJICS.2020.105181
[11] The Machine Learning Model for Identifying Bogus Profiles in Social Networking Sites
https://link.springer.com/chapter/10.1007/978-3-031-16620-4_5
[12] Identifying Fake Profile in Online Social Network: An Overview and Survey
https://link.springer.com/chapter/10.1007/978-981-15-6315-7_2
[13] Friend or foe? Fake profile identification in online social networks
https://link.springer.com/article/10.1007/s13278-014-0194-4
[14] Prediction of Fake Instagram Profiles Using Machine Learning
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3802584
[15] FAKE PROFILE IDENTIFICATION IN SOCIAL NETWORK USING MACHINE LEARNING AND NLP
https://www.proquest.com/openview/d79bbecb17a53dc2455dca3a4a926754/1?pqorigsite=gscholar&cbl=2045096
[16] A Hybrid Method for Fake Profile Detection in Social NetworkUsing Artificial Intelligence
https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119776529.ch5
[17] Detection of Fake Accounts on social media Using Multimodal Data with Deep Learning
https://ieeexplore.ieee.org/abstract/document/10210324
[18] Detection of Fake Profiles on Online Social Network Platforms: Performance Evaluation of Artificial Intelligence Techniques
https://link.springer.com/article/10.1007/s42979-024-02839-9
[19] Fake profile detection in social media using image processing and machine learning
https://dspace.bracu.ac.bd/xmlui/handle/10361/15002
[20] Fake Profile Detection on Social sites
https://ieeexplore.ieee.org/abstract/document/10596657