



## Fake Social Media Profile Detection and Reporting

<sup>1</sup>Mr. N. Lakshmi Narayana, <sup>2</sup>G. Rupa Tanishq Sri Vasavi, <sup>3</sup>D. Pallavi, <sup>4</sup>Ch. Kalyani

<sup>1</sup>Assistant Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

<sup>2,3,4</sup>U. G Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

**ABSTRACT-** *The rapid growth of social media platforms has led to an increase in fake profiles that are used for spam, phishing, identity theft and spreading false information. Given the large number of users, such accounts are hard to detect manually. This paper proposes a Machine Learning-Based Fake Social Media Profile Detection and Reporting System for detecting fake accounts based on profile features such as followers, following, posts, biography, and verification status. The Random Forest algorithm is used to classify the profiles as genuine or fake for the proposed system. A reporting module for users to report suspicious accounts and an administrator dashboard to manage reported profiles. The system is developed using Python, Flask, HTML, CSS and JavaScript and it provides an accurate, secure and user-friendly solution to improve social media security.*

**KEYWORDS:** *Machine Learning, Fake Social Media Profile Detection, Random Forest, Social Media Security, Profile*

*Classification, Flask, Python, Cyber Security, Web Application.*

### INTRODUCTION

Social media platforms are now a part of how we talk to each other every day how we learn and how we do business.. The problem is that there are a lot of fake profiles on these platforms and that has created some serious security issues. We are talking about things like people stealing our identities, spam, online fraud and fake information. It is really hard to find these accounts by hand and it takes a lot of time.

Machine Learning is a way to solve this problem. It looks at things like how many people follow you how people you follow how many posts you have made, what you say about yourself and if your account is verified. By looking at these things Machine Learning can find accounts that're suspicious and figure out if they are fake or real.

The Fake Social Media Profile Detection and Reporting System is a way to find fake



profiles. It uses something called the Random Forest algorithm to decide if a profile is fake or real. This system also lets users report profiles that they think are suspicious. Then the administrators will look at them. This makes the internet a safer place stops people from doing things and makes social media a better place to be. The Fake Social Media Profile Detection and Reporting System is a solution to the problem of fake profiles, on social media platforms.

## LITERATURE SURVEY

The rise of social media usage has resulted in an increase in fake profiles being created for spamming, phishing, fraud, and spread of misinformation. In order to tackle this issue, many scientists have come up with numerous machine learning models for detection of fraudulent accounts. Models like Decision Tree, Support Vector Machine (SVM), Naïve Bayes, Logistic Regression, and Random Forest have been commonly employed in the classification of social media accounts according to their attributes.

According to recent studies, features of profiles including followers, following, post numbers, account activities, biographical information, and verification have proven to be important in detecting the presence of fake accounts. Among these

models, Random Forest proves to be more accurate and effective since it is a model that uses several decision trees to make better predictions. From the above findings, it is evident that machine learning models can help in minimizing the problem of fake profiles.

## RELATED WORK

Some researchers have designed machine learning systems to detect the fake profiles from the social networking sites. These systems consider both the profile attributes and behavioral aspects of users. In traditional techniques, the Decision Tree, Naïve Bayes, Logistic Regression, and SVM algorithms are used for classification. The recent research revealed that Random Forest offers better accuracy compared to others because the random forest combines various decision trees to minimize classification errors. The major drawback of most of the existing systems is that they have no reporting system where users can report any suspicious profile.

Furthermore, some applications do not contain administrator's interface to manage the reported fake profiles. The designed system will overcome these drawbacks of other systems through the design of Random Forest based system for detection of fake profiles along with reporting and administrator module.



## EXISTING SYSTEM

The existing systems for detecting fake social media profiles primarily rely on human intervention, user reports, and simple security protocols. The detection process of such suspicious accounts on social media sites usually takes place once they are reported by users or once any suspicious activity is observed.

This approach consumes time and cannot efficiently manage the thousands of accounts created each day. Most current approaches adopt simple rule-based techniques, which offer minimal accuracy in results and cannot detect newly created fake accounts.

In addition, such systems do not have a complete reporting tool and centralized management system for suspicious profiles. This leads to the widespread propagation of spam messages, phishing scams, identity fraud, and disinformation on social media sites.

## PROPOSED SYSTEM

In the suggested model, Machine Learning algorithms will be utilized to detect social networking profiles that have been created artificially through analyzing certain aspects of the social profile such as followers count, following count, number

of posts, biography details, profile picture, and activity on the social networking site.

There is also provision in the system to report profiles which appear to be suspicious by a user through a reporting module. There will be an administrator dashboard to help the administrator track down the reported social networking profiles and verify the outcome of their classification as either real or fake.

## SYSTEM ARCHITECTURE

The proposed system consists of Data Collection, Data Preprocessing, Machine Learning Model, Prediction Module, User Reporting Module, and Administrator Dashboard. User profile information, including followers, following, posts, biography, and profile picture details, is collected and preprocessed to remove incomplete or invalid data. The processed data is then analyzed using the Random Forest algorithm to classify the profile as genuine or fake. The prediction result is displayed to the user, and suspicious profiles can be reported through the reporting module.

The administrator reviews reported accounts, monitors detection results, and manages user reports to improve the security and reliability of the social media platform.

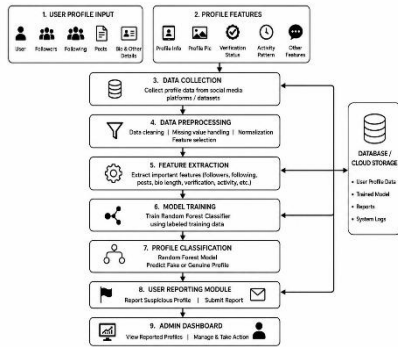


Fig 1: System Architecture

Fig 1: System Architecture

## METHODOLOGY DESCRIPTION

The methodology of the proposed system works according to a machine learning-based system to detect fake social media profiles. Profile data like followers, following, posts, biographies, profile pictures, account verifications, etc. are collected from the user at first. Preprocessing of data involves eliminating missing data and formatting the data for further use. After preprocessing of the data, the extraction of useful profile features is performed and the training of the Random Forest classification model is done using these features. Then, the model makes predictions of the input profile whether it is a Genuine or Fake one. The prediction output is given to the user via a web application. A User Reporting Module is also there to help the user to report any suspicious profiles. These profiles are stored in the database and analyzed by the

administrator using the Administrator Dashboard.

## RESULTS AND DISCUSSION

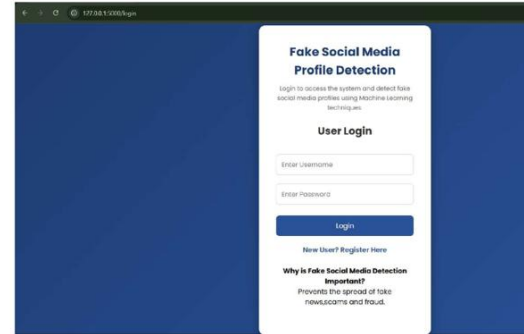


Fig. 1: User Login Page

Login page is used to verify the credentials of user which include his username and password. Once logged in, the user can use Fake Social Media Profile Detection and Reporting System to examine the social media profiles, identify the fake accounts, report them and check the prediction results on dashboard.

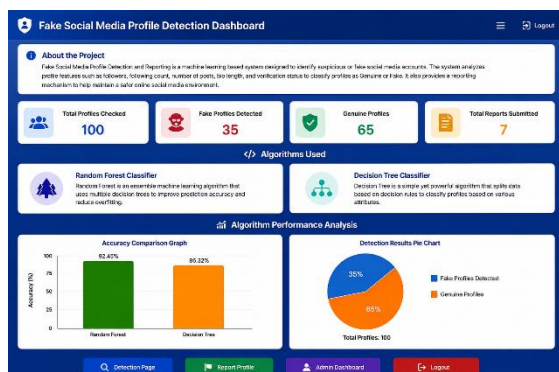


Fig. 2: User Registration Page

The User Registration Page is where a new user signs up for the system by giving some basic information like username, email, password, and contact info. Once the user registers, he/she can log into the Fake



Social Media Profile Detection and Reporting System to make use of its services.



**Fig. 3: User Dashboard**

The User Dashboard gives a general description of the system after login. The user can enter his/her profile information, view prediction results, and access the reporting module. The dashboard provides an easy-to-use interface to detect suspicious social media accounts.

**Fig. 4: Fake Profile Detection**

This page shows the outcome of prediction for the selected social media profile. In the Random Forest classifier, analysis of the attributes of the social media profile like followers, following, posts, bio information, and presence of the profile

picture helps in categorizing the social media profile into Genuine or Fake.

```
reports > reports.csv
1  vasavi,instagram,"stalking
2  "
3  vasavi,instagram,"stalking
4  "
5  vasavi,instagram,stalking
6  vasavi,instagram,stalking
7  vasavi,instagram,stalking
8  vasavi,insta,stalking
9  vasavi,insta,sdd
10 vasavi,insta,stalking
11 arvind,insta,stalking
```

**Fig. 5: Reported Profiles Management**

The page enables the user to submit a report regarding the suspicious social media profile. The reported data is saved in the database and can be accessed by the administrator. The reporting system is designed to assist in making the process of detecting frauds more effective.

## FUTURE SCOPE

Improvements in the design of the suggested Fake Social Media Profile Detection and Reporting System can be done using advanced Deep Learning methods and social media data analytics in real time. The future scope can involve detection of fake social media profiles based on images and analysis of the biography using natural language processing and behavioral pattern detection. This tool can also be upgraded to support other social media sites like



Facebook, Instagram, X (formerly Twitter), and LinkedIn.

## CONCLUSION

Fake Social Media Profile Detection and Reporting System is a very effective way for detecting fake social media profiles using the technique of Machine Learning. The Random Forest classifier classifies users based on certain profile attributes, and thus helps in combating online frauds, spam, and identity theft. The use of a built-in reporting tool and administrator panel improves the robustness of the system because users can report any suspicious profiles and administrators will be able to track those reports.

## REFERENCES

- [1] D. P. Harini, "Electronic Health Record Stage Identification using Principal Component Analysis," *Machine Intelligence Research*, vol. 18, no. 01, pp. 864- 873, 17 8 2024.
- [2] D. P. Harini, "Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications," *International Journal of Engineering & Science Research*, vol. 3, no. 9, pp. 472-478, 2013.
- [3] D. P. Harini, "Analyze and Predict of Human Cyber Attackers using Artificial Neural Network," *Journal of Basic Science and Engineering*, vol. 21, no. 1, pp. 1529 - 1536, 8 7 2024.
- [4] A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow, 3rd ed., O'Reilly Media, 2023.Explains practical machine learning model development and evaluation.
- [5] S. Cresci et al., "The Paradigm-Shift of Social Spambots," *Computer Communications*, vol. 124, pp. 79–86, 2018.Discusses techniques for detecting fake and automated social media accounts.
- [6] T. M. Mitchell, *Machine Learning*, McGraw-Hill, 1997.Explains the fundamentals of supervised learning and classification algorithms.
- [7] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 4th ed., Morgan Kaufmann, 2023.Describes data preprocessing, feature selection, and classification methods.
- [8] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.Provides advanced concepts of deep learning and intelligent prediction models.
- [9] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake News Detection on Social Media," *ACM SIGKDD Explorations*, 2017.Explores machine learning-based approaches to identify misinformation in online media.
- [10] V. Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization," *ICWSM*, 2017.Develops



methods for detecting bots and artificial accounts on social media platforms.

[11] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, pp. 436–444, 2015. Surveys the history and uses of deep learning techniques.

[12] X. Wu, X. Zhu, G. Wu, and W. Ding, "Data Mining with Big Data," *IEEE TKDE*, vol. 26, no. 1, 2014. Considers the issues of big data analytics and machine learning methods.

[13] N. Z. Gong and B. Liu, "Attribute Inference Attacks via Users' Social Friends and Behaviors," *USENIX Security Symposium*, 2016. Reviews privacy and security problems in online social networks.

[14] C. C. Aggarwal, *Social Network Data Analytics*, Springer, 2018. Provides an overview of methods for social network analysis and detection of fake profiles.

[15] S. Raschka, Y. Liu, and V. Mirjalili, *Machine Learning with PyTorch and Scikit-Learn*, Packt Publishing, 2022. The book offers detailed guidelines on the application of machine learning algorithms through the use of Python, PyTorch, and Scikit-learn packages.