

Fake Social Media Accounts and Their Detection

¹Mrs. M. Anusha,²Jada Vasavi,³Bandaru Akhila,⁴Endla Bhavani

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

^{2,3,4}U. G Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT- *This project presents an AI-based fake social media account detection system using Machine Learning techniques to identify fake accounts accurately and efficiently. Fake accounts are widely used for spreading misinformation, online fraud, spam, phishing attacks, and identity theft, making their detection essential for maintaining the security of social networking platforms. The proposed system analyzes important profile features such as profile picture availability, username, biography, number of posts, followers, following count, account privacy status, and follower-to-following ratio to classify accounts as genuine or fake. The application is developed using Python, Flask, HTML, CSS, and JavaScript to provide a simple and user-friendly interface. Three Machine Learning algorithms—Random Forest, Decision Tree, and Logistic*

Regression—are implemented and compared to improve prediction accuracy. Among them, Random Forest achieves the best performance. The system provides fast, reliable, and automated detection with minimal human intervention, helping improve the safety, trustworthiness, and overall security of social media platforms.

KEYWORDS: *Fake Social Media Account Detection, Machine Learning, Artificial Intelligence, Random Forest, Social Media Security*

INTRODUCTION

The rapid growth of social media platforms has increased the number of fake accounts used for spreading misinformation, online fraud, spam, phishing attacks, and identity theft. With advancements in Artificial Intelligence (AI) and Machine Learning (ML), fake account detection has become

more accurate and efficient. This project combines Machine Learning techniques with profile feature analysis to automatically identify fake social media accounts and improve the security and reliability of social networking platforms. The proposed system not only detects fake accounts with high accuracy but also adds an additional layer of protection by enabling intelligent, automated account verification and reducing the need for manual monitoring.

LITERATURE SURVEY

Fake social media account detection has gained significant attention in recent years due to the rapid growth of social networking platforms and advancements in Artificial Intelligence and Machine Learning technologies. A fake social media account is generally defined as a user profile created to impersonate individuals, spread misinformation, perform online fraud, send spam, conduct phishing attacks, or engage in other malicious activities. The core concept of fake account detection revolves around analyzing user profile features and applying intelligent Machine Learning algorithms to accurately distinguish genuine accounts from fake ones. This approach enhances the

security, reliability, and trustworthiness of social networking platforms while reducing manual effort through automated and intelligent decision-making. The trained model processes the input features and predicts whether the social media account is genuine or fake.

RELATED WORK

Several researchers have contributed to the development of fake social media account detection systems to improve the security and reliability of online social networking platforms. Early research primarily focused on rule-based and manual verification methods to identify fake accounts based on predefined patterns and suspicious activities. However, these approaches were limited in accuracy, scalability, and their ability to detect newly created fake accounts. Recent studies have adopted Machine Learning techniques to analyze profile features such as followers, following, posts, biography, and account activity. These intelligent approaches have significantly improved detection accuracy, reduced manual effort, and enabled automated identification of fake social media accounts.

EXISTING SYSTEM

The existing fake social media account detection methods mainly rely on manual verification and rule-based techniques to identify suspicious accounts. These methods are time-consuming, less accurate, and difficult to apply to the rapidly growing number of social media users. Traditional approaches often fail to detect newly created or intelligently designed fake accounts. They also lack automated analysis and real-time detection capabilities. As a result, fake accounts continue to spread misinformation, spam, phishing attacks, and online fraud. Overall, the existing systems lack scalability, intelligence, and high detection accuracy.

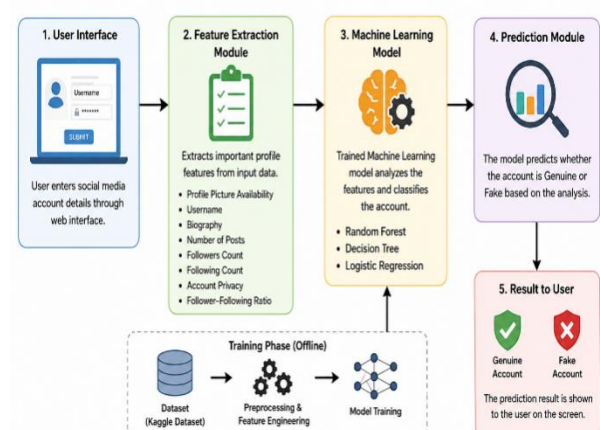
PROPOSED SYSTEM

The proposed system helps identify fake social media accounts using Machine Learning. It examines important profile details such as the profile picture, username, biography, number of posts, followers, following count, and account privacy to determine whether an account is genuine or fake. The system uses Random Forest, Decision Tree, and Logistic Regression algorithms, with Random Forest providing

the best accuracy. It offers a simple and user-friendly interface, reduces manual effort, and supports a safer, more secure, and trustworthy social media environment.

SYSTEM ARCHITECTURE

The proposed Fake Social Media Account Detection System includes a user interface, feature extraction module, Machine Learning model, and prediction module. It analyzes profile details such as username, biography, posts, followers, following count, and account privacy to classify accounts as genuine or fake. The system provides fast, accurate, and real-time predictions, helping improve the security and trustworthiness of social networking platforms.



**Fig 1: System Architecture
METHODOLOGY DESCRIPTION**

The proposed system uses Machine Learning to detect fake social media accounts. It collects and analyzes user profile features, processes the data, and classifies accounts as genuine or fake using algorithms such as Random Forest, Decision Tree, and Logistic Regression. The prediction result is displayed through a simple web interface.

RESULTS AND DISCUSSION

The home page is the main interface of the application. It provides the project title, a brief description, and a "Get Started" button to access the system. The page is designed to be simple, user-friendly, and easy to navigate for fake account detection.



Fig 2: Home Page of Fake Social Media Account Detection System

The Login Page allows authorized users to access the system by entering their username and password. After successful authentication, users are redirected to the

dashboard. This ensures that only valid users can access the fake account detection system.

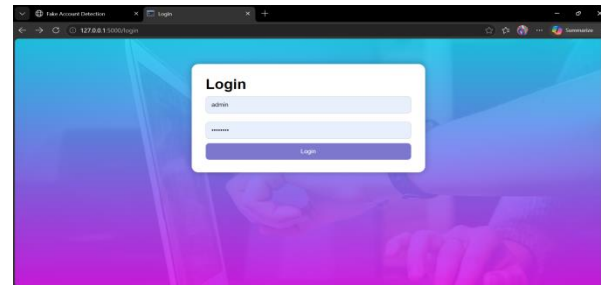


Fig 3: Login Page

The Dashboard provides an overview of the system. It displays important information such as the dataset size, number of machine learning algorithms used, and the best-performing model (Random Forest). The dashboard also provides options to analyze social media accounts, compare algorithm accuracy, and log out of the application.

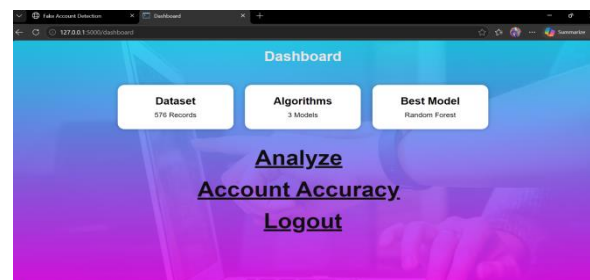


Fig 4: Dashboard Page

The Real Account Result Page displays a message indicating that the analyzed social

media account is genuine based on the machine learning model's prediction.

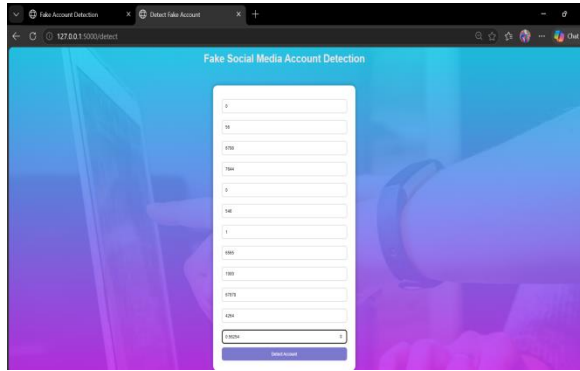


Fig 5: Analyzer Page for Fake

After submitting the account details, the system analyzes the input and predicts whether the account is Fake. The result page displays the prediction along with the confidence score and the machine learning algorithm (Random Forest) used for classification.

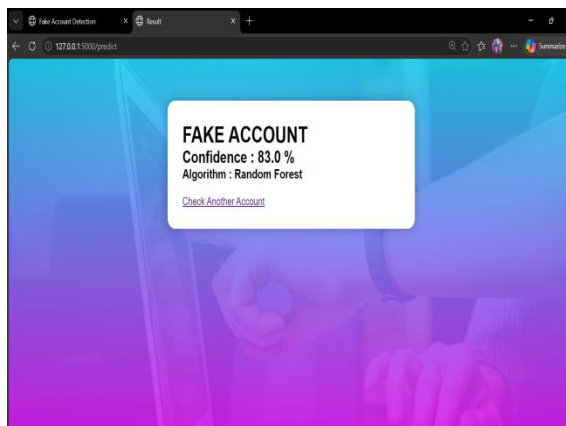


Fig 6: Fake Account Detection Result

The Fake Account Result Page displays a message indicating that the analyzed social media account is fake, helping users identify suspicious accounts.

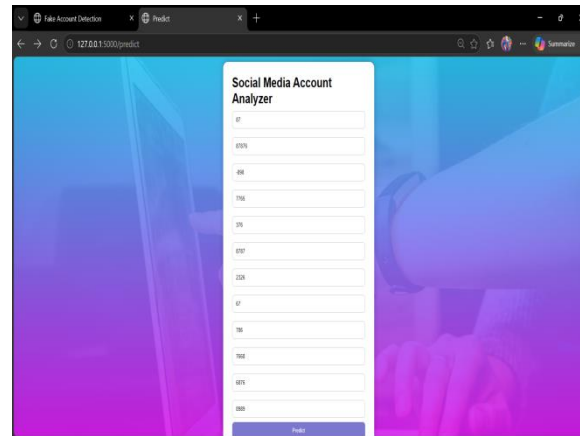


Fig 7: Anayzer Page for Real

If the entered account belongs to a genuine user, the system classifies it as a Real Account. The page displays the prediction result, confidence percentage, and the algorithm used, enabling users to verify the authenticity of social media accounts.

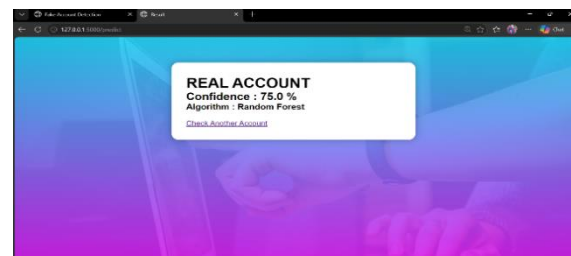


Fig 8: Real Account Detection Result

The Accuracy Comparison Page presents the performance of different machine learning algorithms used in the project, including Random Forest, Decision Tree, and Logistic Regression. It compares their accuracy percentages, helping identify the most effective model for fake account detection. In this project, Random Forest achieved the highest accuracy and was selected as the final prediction model.

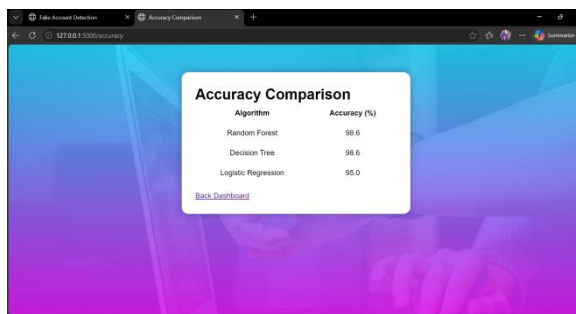


Fig 9: Accuracy Comparison

CONCLUSION

The Fake Social Media Accounts and Their Detection system provide a reliable solution for identifying fake accounts using Artificial Intelligence and Machine Learning. It analyzes important profile features to classify accounts as genuine or fake with good accuracy. The system helps reduce online fraud, spam, phishing, identity theft, and the spread of false information. Developed using

Python, Flask, HTML, CSS, and JavaScript, it offers a simple and user-friendly interface. Random Forest achieved the highest prediction accuracy among the implemented algorithms. Overall, the system improves the security, trustworthiness, and reliability of social networking platforms while supporting a safer online environment.

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, "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.
3. D. P. Harini, "Scalable and Secure Sharing of Client Medical Records in Cloud," *International Journal Of Computer Sc*, vol. 4, no. 4, pp. 161-163, 2013.
4. *Electrical and Computer Engineering (IJECE)*, 2022. [Online]. Available: <https://ijece.iaescore.com/index.php/IJECE/article/view/28634>
5. S. Cresci, M. Petrocchi, A. Spognardi, and R. Di Pietro, "Fake Twitter Followers Detection," in *Proc. IEEE Int. Conf. Data Science and Advanced Analytics (DSAA)*,



International Journal of DATA SCIENCE AND IOT MANAGEMENT SYSTEM

Peer Reviewed, Referred & Indexed Journal

ISSN: 3068-272X

www.ijdim.com

Original Research Paper

-
2015. [Online]. Available: <https://ieeexplore.ieee.org/document/7341362>
6. O. Varol, E. Ferrara, C. A. Davis, F. Menczer, and A. Flammini, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," in *Proc. Int. AAAI Conf. Web and Social Media (ICWSM)*, 2017. [Online]. Available: <https://ojs.aaai.org/index.php/ICWSM/article/view/14898>
11. O. Varol, E. Ferrara, C. A. Davis, F. Menczer, and A. Flammini, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," in *Proc. Int. AAAI Conf. Web and Social Media (ICWSM)*, 2017. [Online]. Available: <https://ojs.aaai.org/index.php/ICWSM/article/view/14898>
12. A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2022. [Online]. Available: <https://www.oreilly.com/library/view/hands-on-machine-learning/9781098125967/>
13. M. A. Russell, *Mining the Social Web*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2018. [Online]. Available: <https://www.oreilly.com/library/view/mining-the-social/9781491973547/>
14. Botometer, "Botometer: Machine Learning for Social Bot Detection." [Online]. Available: <https://botometer.osome.iu.edu/>
15. C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, "BotOrNot: A System to Evaluate Social Bots," in *Proc. 25th Int. Conf. Companion on World Wide Web (WWW Companion)*, 2016. [Online]. Available: <https://dl.acm.org/doi/10.1145/2872518.2889302>
16. Akinapalli, S. (2026). An Ai-Powered Data Trust And Quality Scoring Framework For Enterprise Decision Intelligence Systems. *International Journal of Data Science and IoT Management System*, 5(1), 946-950.
-