International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

[1]Dr. G. Prasuna,[2]M. Lavanya[3]P. Gopichand,[4]P. Bhavani Sree
[1]Associate 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 Profile Detection and Reporting System using machine learning techniques. The system helps to improve social media security by identifying fake profiles based on different profile features. It provides a simple, accurate, and automated way to detect fake accounts and supports users and administrators in maintaining a safe online environment. The system uses profile information and machine learning algorithms to classify accounts as real or fake. Suspicious accounts are identified and can be reported for further action, improving the overall security of social media platforms. Traditional methods of detecting fake profiles mainly depend on manual checking or user complaints, which are slow, less accurate, and difficult to manage because of the large number of social media users. These methods also fail to identify many fake accounts at an early stage. There is a need for an intelligent, automatic, and low-cost system that can detect fake social media profiles with better accuracy and help reduce online fraud, spam, and other harmful activities.***

KEYWORDS: Artificial Intelligence (AI), Machine Learning, Fake Social Media Profile Detection, Social Media Security, Random Forest, Support Vector Machine (SVM), Neural Network, Data Analysis, User Authentication, Automated Reporting.

INTRODUCTION

Social media platforms are widely used for communication, business, education, and entertainment. As the number of users increases, fake social media profiles are also growing rapidly. These fake accounts are commonly used for spam, online scams, fake promotions, cyberbullying, and spreading false information. Detecting such profiles manually is difficult, time-consuming, and not always accurate. With the development of Artificial Intelligence

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

and Machine Learning, fake profile detection has become more reliable and efficient. This project combines machine learning algorithms with profile feature analysis to identify fake social media accounts. The proposed system not only detects fake profiles but also provides a reporting feature to improve the security and trust of social media platforms.

LITERATURE SURVEY

Fake social media profile detection has gained significant attention in recent years due to the rapid growth of online social networking platforms. A fake social media profile is generally defined as an account created with false or misleading information for activities such as spam, scams, fake promotions, or spreading false information. The main objective of fake profile detection is to analyze user profile features and identify suspicious accounts using machine learning techniques. The core concept of these systems revolves around automated profile analysis and intelligent decision-making using data collected from different social media profile attributes.

RELATED WORK

Several researchers have contributed to the development of fake social media account detection systems to improve online security, user trust, and platform integrity. Early approaches relied on manually defined rules and simple profile analysis techniques to identify suspicious accounts based on limited features such as usernames, profile pictures, and posting frequency. With the advancement of Machine Learning, researchers began using classification algorithms such as Random Forest, Support Vector Machine (SVM), Decision Trees, and Neural Networks to analyze user behavior and detect fake accounts more accurately. Recent studies have incorporated feature engineering, ensemble learning, and deep learning techniques to examine profile attributes, follower-following relationships, account activity, and behavioral patterns for improved detection performance. These methods have significantly increased detection accuracy while reducing false positives. However, challenges such as evolving spam techniques, imbalanced datasets, feature selection, and real-time detection continue to affect system performance. The proposed system addresses these challenges by applying machine learning algorithms to classify social media accounts as genuine or fake based on multiple profile features,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

providing an accurate, reliable, and efficient detection solution.

EXISTING SYSTEM

The existing fake social media account detection systems primarily rely on manual verification, rule-based filtering, and basic profile analysis to identify suspicious accounts. These methods examine limited features such as usernames, profile pictures, posting frequency, or follower count, making them less effective against sophisticated fake profiles. Many platforms depend on users to report suspicious accounts, resulting in delayed detection and increased risk of misinformation and spam. Traditional approaches often use fixed rules that cannot adapt to evolving fake account behaviors. As fake profiles become more advanced, these systems struggle to accurately distinguish between genuine and fraudulent users, leading to false positives and false negatives. Furthermore, existing methods generally lack intelligent learning capabilities and real-time detection, reducing their effectiveness in maintaining social media security. Overall, the existing system provides limited accuracy, scalability, and adaptability for detecting fake social media accounts.

PROPOSED SYSTEM

The proposed system implements a Machine Learning-based fake social media account detection approach to accurately classify user profiles as genuine or fake. It analyzes multiple profile attributes such as platform, profile picture availability, bio length, username randomness, follower count, following count, account age, and posting frequency to identify suspicious behavior. The system applies data preprocessing techniques, including label encoding and feature scaling, before training multiple machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Neural Network (MLP). The algorithm with the highest accuracy is automatically selected as the final prediction model. The trained model is then integrated into a Flask-based web application, enabling users to enter account details and receive instant predictions. This approach improves detection accuracy, reduces manual effort, and provides a reliable, scalable, and efficient solution for identifying fake social media accounts.

SYSTEM ARCHITECTURE

The architecture of the proposed Fake Social Media Account Detection System consists of a user interface, Flask web application, dataset processing module,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

machine learning module, trained model, and prediction module. The user uploads a training dataset through the web interface, where the dataset is processed using data preprocessing techniques such as feature selection, label encoding, and feature scaling. The processed data is then used to train multiple machine learning algorithms, including Random Forest, Support Vector Machine (SVM), and Neural Network (MLP).

The system evaluates the performance of each algorithm and automatically selects the model with the highest accuracy. The trained model, along with the scaler and label encoder, is stored for future use. During prediction, users enter social media account details through the web application. The input data is preprocessed and passed to the trained model, which classifies the account as either Fake or Real. The prediction result is displayed instantly along with visual analysis, providing an accurate, reliable, and efficient solution for fake social media account detection.

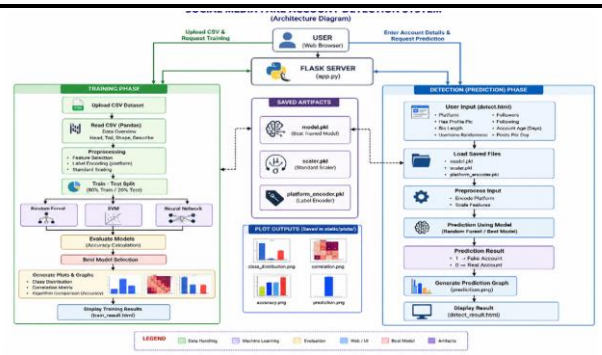


Fig 1: System Architecture

METHODOLOGY DESCRIPTION

The methodology of the proposed Fake Social Media Account Detection System is designed to accurately identify fake and genuine social media profiles using machine learning techniques. The system follows a structured workflow that includes data collection, data preprocessing, feature selection, model training, performance evaluation, and prediction. Initially, the social media dataset is collected and processed by removing unnecessary data, selecting relevant features, encoding categorical values, and normalizing numerical attributes. The processed dataset is then divided into training and testing sets for model development. Multiple machine learning algorithms, including Random Forest, Support Vector Machine (SVM), and Neural Network (MLP), are trained and evaluated using accuracy metrics. The model with the highest accuracy is selected and saved for future predictions. During the

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

detection phase, users enter social media account details through the Flask web application, where the trained model analyzes the input features and classifies the account as either Fake or Real, providing a fast, accurate, and reliable detection system.

RESULTS AND DISCUSSION

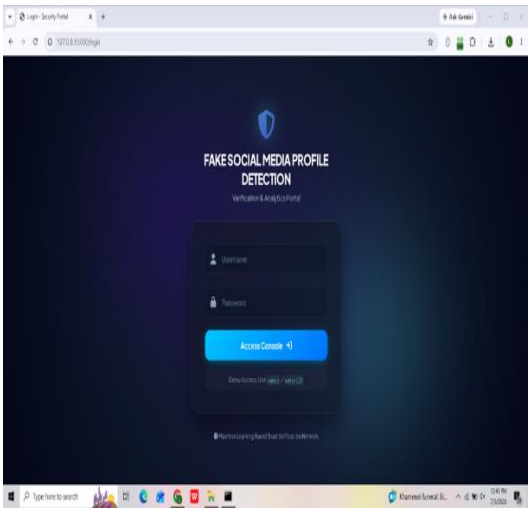


Fig 2: Login Page

This is the login page of the Fake Social Media Profile Detection System. It provides a secure authentication interface where the administrator enters a valid username and password to access the application. Only authorized users can log in and use the system features.

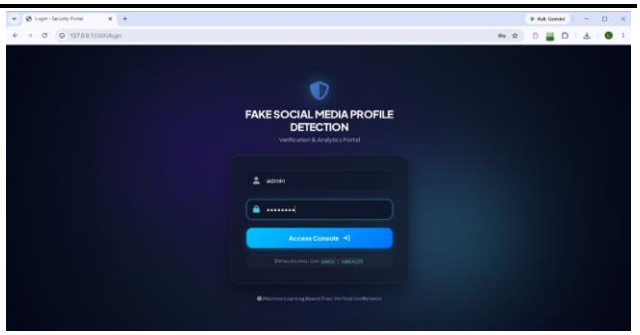


Fig 3: Login Verification (Admin Credentials)

This screenshot demonstrates the login verification process. The administrator enters valid credentials, and the system authenticates the user before granting access to the dashboard, ensuring secure access to the application.

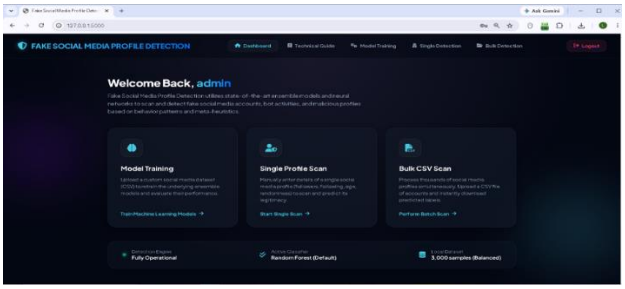


Fig 4: Dashboard (Home Page)

After successful login, the administrator is redirected to the dashboard. The dashboard provides quick access to the major modules of the system, including Model Training, Single Profile Detection, Bulk CSV Detection, and Technical Guide. It also displays the current status of the detection engine and the active machine learning model.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

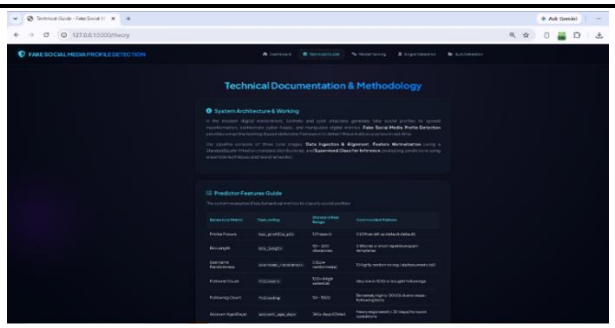


Fig 5: Technical Guide

The Technical Guide page explains the working methodology of the system. It provides information about the machine learning pipeline, input features, prediction process, and behavioral metrics used to classify social media profiles as real or fake.

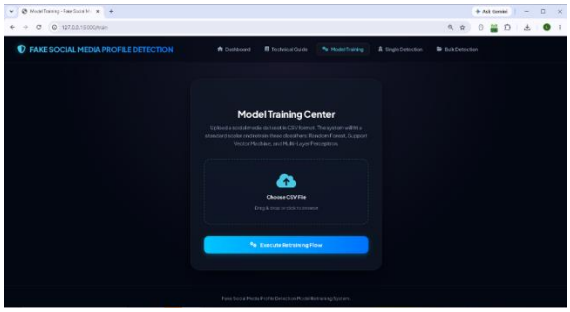


Fig6: Model Training Page

The Model Training page allows the administrator to upload a CSV dataset for retraining the machine learning models. The uploaded dataset is preprocessed, and the system trains classifiers such as Random Forest, Support Vector Machine, and Multi-Layer Perceptron to improve prediction performance.

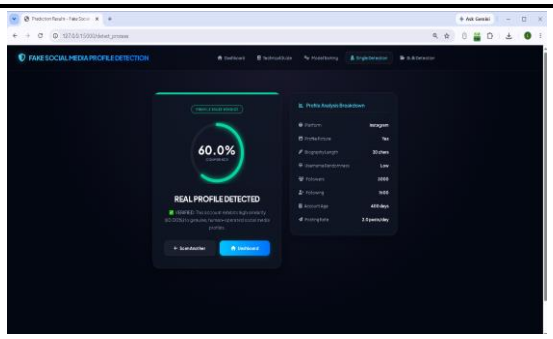


Fig 7: Real Profile Detection Result

This screen shows the prediction result for a genuine social media profile. Based on the analyzed features, the machine learning model classifies the profile as **Real Profile Detected** and displays the confidence score along with the profile analysis summary.

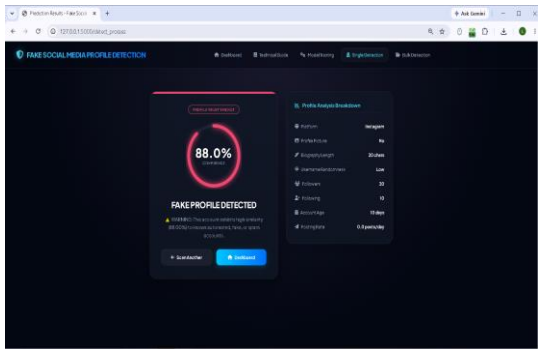


Fig 8: Fake Profile Detection Result

This screen displays the prediction result for a fake social media profile. The machine learning model identifies suspicious behavioral characteristics and classifies the profile as Fake Profile Detected along with the confidence score. A detailed analysis of the input features is also shown.

CONCLUSION

The proposed Fake Social Media Account Detection System enhances online security

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

by accurately identifying fake and genuine social media profiles using machine learning techniques. By analyzing important profile features and selecting the best-performing classification algorithm, the system provides reliable and efficient detection of suspicious accounts. The integration of a Flask-based web application enables users to perform real-time account verification through a simple and user-friendly interface. This approach reduces manual effort, improves detection accuracy, and helps minimize the spread of fake accounts, spam, and online fraud. Overall, the system offers a secure, scalable, and intelligent solution for maintaining the integrity and trustworthiness of social media platforms.

FUTURE SCOPE

The proposed Fake Social Media Account Detection System can be further enhanced by integrating advanced Deep Learning techniques such as Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and Graph Neural Networks (GNN) to improve detection accuracy and identify more complex fake account patterns. The system can be extended to analyze additional features, including user posts, comments, images, hashtags, and social network relationships for more comprehensive account verification. Integration with real-time social media APIs would enable continuous monitoring and instant detection of newly created fake accounts. Cloud deployment can improve scalability and support large-scale data processing across multiple platforms. Furthermore, incorporating explainable AI techniques can provide transparent prediction results, helping administrators understand the reasons behind account classification and enhancing trust in the detection system.

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] Nagalakshmi, R., et al. (2024). Multi Relations and Context-Aware Fake User Profile Detection Using Ensemble and LSTM Models. International Journal of Engineering Research & Technology

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

(IJERT). https://doi.org/10.5281/zenodo.18139480

[5] Bhambulkar, R., Choudhary, S., & Pimpalkar, A. (2023). Detecting Fake Profiles on Social Networks: A Systematic Investigation. Proceedings of the IEEE SCEECS 2023. https://doi.org/10.1109/SCEECS57921.2023.10063046

[6] Yang, C., Harkreader, R., & Gu, G. (2013). Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2013.2245530

[7] Ahmed, H., Traore, I., & Saad, S. (2018*). Detecting Opinion Spam and Fake Accounts on Social Networks Using Machine Learning. Future Generation Computer Systems.* https://doi.org/10.1016/j.future.2017.12.028

[8] Subrahmanian, V. S., et al. (2016). The DARPA Twitter Bot Challenge. Computer, 49(6), 38–46. https://doi.org/10.1109/MC.2016.183

[9] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race. Proceedings of the 26th International Conference on World Wide Web Companion. https://doi.org/10.1145/3128572

[10] Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. Communications of the ACM, 59(7), 96–104. https://doi.org/10.1145/2818717

[11] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2015). Fame for Sale: Efficient Detection of Fake Twitter Followers. Decision Support Systems, 80, 56–71. https://doi.org/10.1016/j.dss.2015.09.003

[12] Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? IEEE Transactions on Dependable and Secure Computing, *9*(6), 811–824. https://doi.org/10.1109/TDSC.2012.75

[13] Davis, C. A., Varol, O., Ferrara, E., Flammini, A., & Menczer, F. (2016). BotOrNot: A System to Evaluate Social Bots. Proceedings of the 25th International Conference Companion on World Wide Web, 273–274. https://doi.org/10.1145/2872518.2889302

[14] Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Human-Bot Interactions: Detection, Estimation, and Characterization. Proceedings of the International AAAI Conference on Web and Social Media (ICWSM), *11*(1), 280–289.

[15] Alothali, E., Zaki, N., Mohamed, E. A., & Alashwal, H. (2018). Detecting Social Bots on Twitter: A Literature Review. 2018 International Conference on Innovations in Information Technology (IIT), 175–180. IEEE. https://doi.org/10.1109/INNOVATIONS.2018.8605995

[16] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.