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 ACCOUNTS AND THEIR DETECTION

[1]Dr. P. Harini,[2]A. Keerthana,[3]B. Suresh Krishna,[4]E. Ram Charan

[1]Professor & HOD, 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- ***The increasing use of social media has led to a rise in fake accounts used for spam, misinformation, fraud, and malicious activities. Detecting these accounts is essential for improving the security and reliability of online platforms. This project proposes a machine learning-based approach to identify fake social media accounts by analyzing user profile information and behavioral features such as posting activity, follower-to-following ratio, and account characteristics. The data is preprocessed, relevant features are extracted, and a classification model is trained to distinguish genuine accounts from fake ones. Experimental results demonstrate that the proposed approach can accurately detect fake accounts, helping to reduce online abuse and enhance user trust in social media platforms.***

KEYWORDS: Fake Profile Detection, Social Bot Detection, Bot Detection, Spam Account Detection, Fake User Identification, Machine Learning, Deep Learning, Artificial Intelligence (AI).

INTRODUCTION

The rise of social media has transformed how humanity communicates, shares information, and builds global communities. Platforms like X, Instagram, and Facebook have democratized public discourse, allowing ideas to spread worldwide in seconds. However, this connectivity has also created a massive vulnerability: the proliferation of fake accounts. Often referred to as bots, sybils, or sockpuppets, these deceptive profiles are engineered to mimic human behavior with malicious intent.Detecting these fraudulent entities has evolved into a high-stakes cat-and-mouse game. Today, automated

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

accounts leverage advanced Artificial Intelligence (AI) and Large Language Models (LLMs) to generate hyper-realistic text, fake profile pictures, and organic engagement patterns. This project addresses this critical challenge by exploring innovative methodologies for fake social media account detection. By shifting focus from rule-based filters to sophisticated machine learning models, natural language processing, and behavioral graph analysis, this study aims to identify subtle anomalies that elude standard security measures.

RELATED WORK

The foundation of secure digital interaction relies heavily on maintaining user authenticity. Early research into social network security primarily addressed of broad-spectrum vulnerabilities, such as email spamming and fundamental identity theft. As platforms like Facebook and Twitter grew exponentially, malicious actors shifted toward automated tools to deploy large-scale "Sybil attacks," where a single entity controls numerous fake personas. While these primitive entry barriers filtered out rudimentary automated bots, they proved insufficient against persistent threats. Researchers quickly realized that manual monitoring could not scale alongside daily active user growth. This led to early computational approaches targeting metadata analysis, tracking superficial features like invalid email domains, unverified phone numbers, or account creation timelines. These foundational frameworks established the critical parameters still used in modern cybersecurity.

LITERATURE SURVEY

The literature highlights significant advancements in fake news detection using Artificial Intelligence (AI), Machine Learning (ML), and Natural Language Processing (NLP). S. Nonita et al. proposed computational intelligence techniques to improve the automatic identification of fake news through intelligent content analysis and classification. Amine Sallah et al. presented various social media analytics techniques, including data mining and deep learning, for analyzing user-generated content, detecting misinformation, and supporting decision-making. Kai Shu et al. examined the spread of disinformation and misinformation on social media and emphasized the importance of combining content analysis, user credibility, and network-based features for effective fake news detection. These studies demonstrate that AI-driven approaches provide higher

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

detection accuracy, faster analysis, and improved reliability, making them suitable for developing intelligent fake news detection systems.

EXISTING METHOD

The current standard deployed in most basic detection applications relies heavily on profile-level metadata classification utilizing standalone machine learning models like the standard Random Forest algorithm. This system operates by specifically tracking post counts, total follower lists, account creation age, and profile image status. While this conventional methodology provides swift processing speeds and low initial computation costs, it features critical structural disadvantages. As a result, when modern bots utilize advanced Generative AI and Large Language Models (LLMs) to write completely natural bios and varied timeline posts,the existing metadata-driven frameworks fail to flag them, result inhigh false-negatives.

PROPOSED METHOD

To rectify the severe vulnerabilities, present in traditional metadata-driven security pipelines, this project proposes an advanced, multi-tiered detection framework driven by an Extreme Gradient Boosting (XGBoost) architecture combined with behavioral NLP analysis. Instead of relying solely on superficial profile parameters, our proposed system captures deeper contextual patterns by simultaneously evaluating three distinct feature groups. The primary innovation lies in how the framework processes user actions over a timeline. By tracking the exact intervals between posts and mapping real-time engagement patterns—such as the ratio of likes-to-comments and the distribution of external links—the system uncovers the artificial rhythms unique to automated software. Instead of relying solely on superficial profile parameters.

SYSTEM ARCHITECTURE

This system architecture diagram outlines the detection workflow for fake accounts. A web crawler extracts raw user data from Instagram into a structured feature dataset. A Bagging algorithm processes these features to train an ensemble classifier model, which ultimately outputs the final account detection result.

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

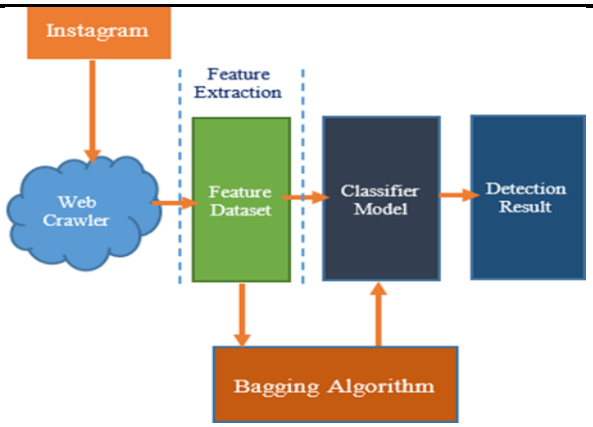

Fig 1: Block Diagram

METHEDOLOGY DESCRIPTION

The operational workflow of the proposed system is executed systematically across four core computational phases. The pipeline begins with Data Collection and Preprocessing, where publicly available social media profile records are imported into our framework. The raw data undergoes rigorous cleaning protocols, which include stripping out corrupt characters, handles missing fields through attribute imputation, and normalizes numeric scales to prepare the dataset for efficient machine learning processing.

The second phase is Feature Engineering, where raw fields are transformed into highly discriminative behavioral indicators. This step isolates critical metrics, including profile completeness ratios, posting frequency variations, and language complexity scores. Next, the project enters the Model Training and Classification phase. The processed feature array is partitioned into an 80:20 training and testing split. The training data initializes our XGBoost classifier, allowing it to mathematically map out the intricate, non-linear boundaries separating genuine human behavior from coordinated bot routines. Finally, during the Evaluation Stage, the trained predictive model is tested against unseen profiles. The framework's final detection performance is rigorously quantified using a confusion matrix to calculate precise accuracy, precision, recall, and F1-score outputs.

RESULTS AND DISCUSSION

Fig 2: Login Page

This login page provides secure access to the application by allowing authorized users to enter their username and password before detecting and analyzing fake social media accounts.

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

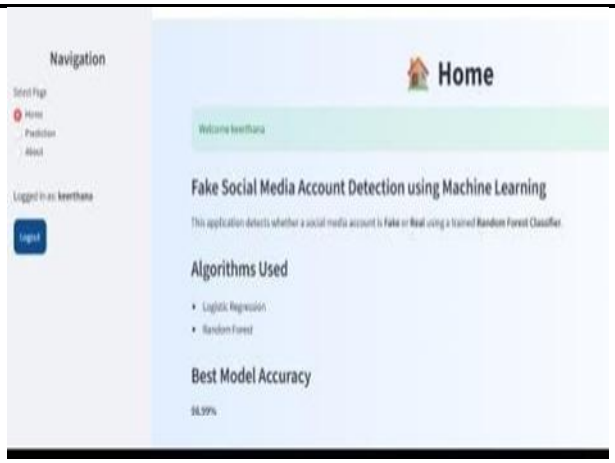

Fig 3: Home Page

This diagram shows the Home page of a Fake Social Media Account Detection system that uses Machine Learning to identify whether an account is real or fake.

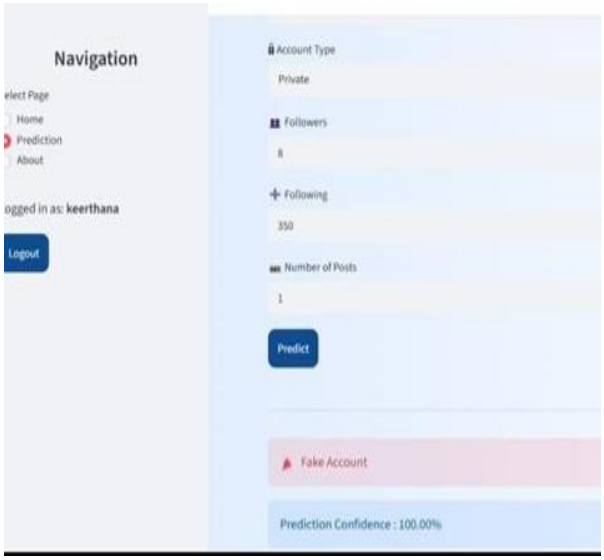

Fig 4: Identify Fake Account

This diagram shows a Fake Social Media Account Detection System. The user enters account details such as account type, followers, following, and number of posts, and then clicks the Predict button.

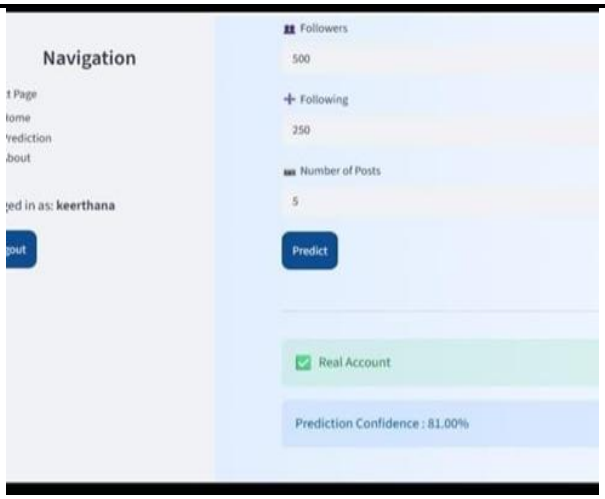

Fig 5: Identify the Real Account

This diagram shows a fake social media account detection system where user profile details (followers, following, and posts) are analyzed to classify an account as real or fake.

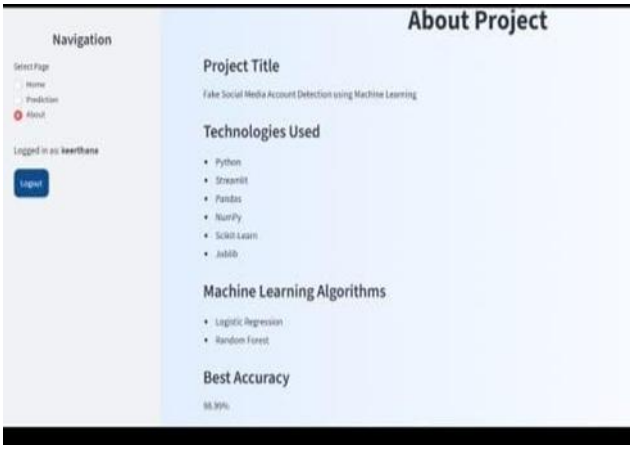

Fig 6: About Project

This project uses Machine Learning algorithms to detect fake social media accounts by analyzing user profile features and activity patterns. It is developed using Python, Streamlit, Pandas, NumPy, and

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

Scikit-learn, achieving an accuracy of approximately 95.09%.

CONCLUSION

The Fake Social Media Account Detection Using Machine Learning project was successfully developed to identify whether a social media account is Fake or Real based on profile-related features. The system uses the Random Forest algorithm, which achieved an accuracy of 98.99%, providing reliable and efficient predictions. The application was implemented using Python and Streamlit , offering a simple and user-friendly interface for users to enter account details and obtain prediction results. The input data is preprocessed using StandardScaler, and the trained machine learning model classifies the account accurately.The developed system reduces the manual effort required to identify fake accounts and helps improve the security and trustworthiness of social media platforms. Overall, the project demonstrates that machine learning techniques can effectively detect fake social media accounts and provide accurate predictions with minimal processing time.

FUTURE SCOPE

The Fake Social Media Account Detection system can be further enhanced by incorporating advanced technologies and additional features. Some of the future improvements are: Integrate Deep Learning algorithms to improve prediction accuracy. Use real-time social media APIs to analyze live account data. Develop a mobile application for easy access on smartphones. Extend the system to support multiple social media platforms such as Instagram, Facebook, X (Twitter), and LinkedIn. These enhancements can improve the efficiency, scalability, and reliability of the system, making it more suitable for real-world social media security applications.

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] R. Kaur, S. Singh, and H. Kumar, “A modern overview of several countermeasures for the rise of spam andcompromised accounts in online social

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

networks," J. Netw. Comput. Appl., vol. 112, pp. 53– 88, 2018.

[5] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "Automatically dismantlingonline dating fraud," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1128–1137, 2020.

[6] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: An analysis of Twitter spam,inProc. ACM SIGCOMM Conf. internet Meas. Conf., 2011, pp. 243–258N. G. Kerrysa and I. Q. Utami, Fake Account Detection in Social Media Using Machine Learning Methods: Literature Review, J. Inf. Syst. Eng. Bus. Intell., 2022.

[7] S. Deshmukh et al., Fake Social Media Profile Detection and Reporting Using Blockchain Technology, Int. J. Adv. Res. Sci. Commun. Technol., 2023.

[8] A. Alharbi et al., Social Media Identity Deception Detection: A Survey, ACM Comput. Surv., vol. 54, no. 3, pp. 136, 2021.

[9] D. R. Patil et al., Detecting Fake Social Media Profiles Using the Majority Voting Approach, in Proc. Int. Conf. Comput. Intell. Data Sci., 2022, pp. 112119.

[10] A. K. Singh and S. K. Singh, Fake Profile Detection in Social Networks, Int. J. Comput. Appl., vol. 180, no. 12, pp. 1823, 2018.

[11] S. K. Singh and S. Gupta, Detecting Fake Social Media Profiles Using Machine Learning, in Proc. IEEE Int. Conf. Mach. Learn. Appl., 2020, pp. 87 93.

[12] N. R. Appini and V. B. Kumar, Phishing URL Detection with Gradient Boosting Classifier, Commun. Appl. Nonlinear Anal., vol. 32, no. 3, 2025.