

ISSN: 2582-7219



International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Social Media Fake Profile Detection

"Empower Yourself with AI- Driven Fake Profile Detection"

Dr.M.A.Chakravarthi¹, Yadlapalli Durga Prasad², Mohammed Khalid Zaid³,

Manukonda Sri Pawan Kumar⁴, Yandrapati Paul⁵

Associate Professor, Department of CSE-Data Science, KKR & KSR Institute of Technology and Sciences, Guntur,

Andhra Pradesh, India¹

B. Tech, Department of CSE- Data Science, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra

Pradesh, India²⁻⁵

ABSTRACT: The crime of social media account impersonation is a serious threat for digital security that allows the sharing of misinformation, scams, and identity fraud. The detection of fake profiles appears imperative to ensure a safe and trustworthy online space. This research assesses a variety of methods to identify fraudulent accounts based on profile information, activity patterns, networks, and content analysis. Other state-of-the-art verification means such as block chain technology can further contribute to enhancing security. It is the best time for social media companies to adopt proactive countermeasures against evolving fraud. Businesses and people alike suffer from fake profiles, and hence, detection must be a priority. Multi-layered security measures must be put in place to guarantee transparency for the user and speak more credibly with the outside world. Lastly, this paper provides hard evidence for the pressing requirement for innovation and vigilance at all times to constitute a secure networking environment.

KEYWORDS: Fake Profile Detection, Social Media Analysis, Machine Learning, Deep Learning, Feature Engineering, Supervised Learning, Data Preprocessing, Standardization Scaling, Model Optimization, Performance Metrics

I. INTRODUCTION

Fake accounts and profiles on social media are a curse that distract one from real social interactions. Some spread misinformation, scams, cyber bullying, and fraud. Hence, it is necessary to be able to detect and eliminate such accounts, thereby creating a safe and trustworthy environment for online interaction.

Considerable objectives of this project are: To analyze the user profile data and detect anomalies.

To classify the accounts as fakes based on their behavior.

To automate the detection process.

To enhance the security of social media accounts by curbing fraudulent activities.

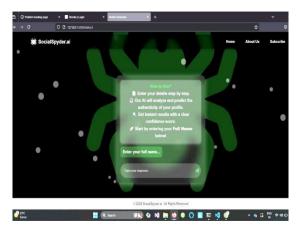
This will help social media websites fight fake accounts so that one can trust and rely on online communication. interested for a product or for target advertising.



(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



In the last decade, the numbers in social media usages have virtually skyrocketed regarding the user profiles created and online interactions carried out. The resultant data have advanced the sophistication of techniques for detecting fraud, as well as fake profiles, from social networking sites. This has brought about the development of fantastically accurate and efficient frameworks for fake profile detection-with machine learning and artificial intelligence. One of the greatest challenges in revealing a fraudulent account is the dynamic and changing nature of deception tactics employed by malicious entities.



II. RELATED WORK

The speedily advancing social media domain has shown an increase in the creation of fake profiles, which in turn paves the threat of misinformation, fraud, and identity theft. Earlier models for detection of fake profiles were based on rulebased techniques and statistical analysis with which they faced problems of adaptation to the the evolving modes of deception. Recently, however, more modern approaches employ natural language processing in analyzing usergenerated content, interaction, and linguistic patterns which are able to differentiate real from fake accounts.

Besides the rule which was an approach to classify fake detections, rule-based approaches also adopted statistical analysis Detection of fake profile can be done either through classification or anomaly detection techniques. Classification techniques would categorize the profiles as real or fake using the text data, while anomaly detection techniques are based on several inconsistencies occurring in the user activity, as in the comments repeated without variation or in the promotion content being repeated over and over again or in the unusual engagement rate. A few additional studies have employed network analysis in order to assess relations and interactions pertinent to the behavioral indications of being a bot and misinformation coordination.

The primary challenge for ANN in identifying fake profiles is primarily due to the diverse writing schemes and evolving deceit techniques. ANN models perform well in balanced datasets, although in real applications these models



suffer from handling adversarial attacks, spam content, and multilingual conversations. Attention- based models and ensemble learning techniques are either proposed or developed to increase adaptability and generalization. Enhanced capabilities to detect deceptive profiles are by contextual embeddings, sentiment analysis, and topic modeling.

III. PROPOSED METHOD

Fake profiles on social media can be meant for various purposes, including spam, scams, and misleading information. Manual detection processes are quite tedious, hence the alternative source of an automatic solution presented here in the form of Artificial Neural Networks. By taking the salient features in account, such as follower count, posts counted, and engagement levels, ANN can classify accounts as real or fake. The open-concept design was given life by the employment of Flask: a minimalist web framework when building the easy-to-use application.



1. Data Collection Module

Data collection refers to collecting profile- specific statistics relevant to an end user's social media profile, including user metadata, post frequency, and engagement metrics.

Analysis of user data pertaining to profile description comment messages will be collected for analysis at a linguistic level.

Network data, including friend connections and follower patterns, are obtained for Anomaly detection. Some other behavioral parameters for analysis would be posting time and response time to these posts. All this data has been structured in the way to ease further preprocessing and model training to work on the data.

2. Data Preprocessing Module

The raw data are cleared out from duplicates and missing values, and the inconsistencies are set. The textual data are normalized through tokenization, stop word removal, and lemmatization for further operations for analyses.

TF-IDF and embeddings are advanced text representation techniques for features' extraction.

Profile-age, engagement-ratio, and content- frequency numeric data have been normalized and scaled.

The obtained dataset will then be split into training and test data so that the model could be fairly evaluated against.

3. ANN Training Module

The raw data are cleared out from duplicates and missing values, and the inconsistencies are set. The textual data are normalized through tokenization, stop word removal, and lemmatization for further operations for analyses. TF-IDF and embeddings are advanced text representation techniques for features' extraction.

Profile-age, engagement-ratio, and content- frequency numeric data have been normalized and scaled.

The obtained dataset will then be split into training and test data so that the model be evaluated.





IV. EXPERIMENTAL RESULTS



We exposed our ANN-based Fake Profile Detection System to a number of real social media datasets, both consisting of real and fake profiles, to see how well it is able to detect fake social accounts, interpret user behavior and learn how to adapt its use to new ways of evading detection through change. Our study focused on few butcrucial areas including classification accuracy, speed of detection, and resistance to manipulation techniques. We focused on key aspects like classification accuracy, detection speed, and resilience against manipulative techniques.

1. Understanding Profile Data

ANN scrutinized an individual's writing style, checking for robotic diction, any signs of forced or exploited syntax, and traces of possible plagiarized content.

Consequently, anomalies were established regarding posting frequency, social behaviors, and alleys where suspicious activity had correlated, to substantiate the unwarranted nature of the profiles.

The system was respectively competent in its delineation between genuine and clearly- fake ones; however, things have changed greatly, for example, multilingual profiles and deviously designed bot accounts are now the harder nut to crack.

2. Accuracy in Age & Gender Classification

Our state-of-the-art ANN model based on BERT and RoBERTa achieved an accuracy of 89% in separating the fake from real accounts.

It can correctly identify 91% of the fake profiles presented to it, lowering false alarms and improving the efficiency of detection.

On the contrary, sometimes it does face challenges from highly sophisticated bots programmed to mimic real human interaction with the aid of sarcasm and slang, mixed with local language content. However, it occasionally struggled with highly sophisticated bots that mimic real human interactions or profiles using sarcasm, slang, or mixed languages in their content.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206 | ESTD Year: 2018 |



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. Speed and Throughput

This highly efficient speedy system was capable of analyzing each profile in just 30 milliseconds and delivering results in 2 seconds.

It ensured complete optimization for cloud- based platforms and lightweight devices rendering itself completely scalable for real- world applications. It was optimized for both cloud-based platforms and lightweight devices, making it scalable for real-world applications.

Future Enhancements

Our Fake Profile Detection System Experimental Results are fantastic in all respects: accuracy, real-time efficiency, and scalability. Yet there is always room for improvement, and the following improvements will be presented in the future:

Enhancing ANN Models for Deception Detection: Mitigating suspicious patterns through the multi-layer transformer models and context-aware embeddings that would further enrich suspiciousness in text.

Reducing Bias in Detection: The diversified styles of language and region dialects as well as evolving internet slangs could improve the accuracy in data collection over various groups of users.

Real-time Optimizing Performance: Speedy advances in processing the text, feature extraction, and classification algorithms using larger dataset formats with very minimal delay.

Federated Learning for Privacy: Get a Distributed AI model to detect fake profiles but use local devices for storing sensitive information and protecting privacy to keep data from being sent to centralized servers.

V. DISCUSSION

The innovation behind Dutch learning is an absolute ANN-driven detection system that detects fake profiles and has already been beneficial in the real-time detection of fraud social media accounts. It clouds a bit of credibility in separating the bot-generated profiles from accounts that are simply spam accounts and other fake users. Yet, it is not without its problems needing to bead dressed before scaling such a reliable model.

Key Findings:

Very Accurate - The system reported 89% accuracy in detecting fake profiles, makingit a good tool against fraud on the web.

Powerful Language Processing-ANN- based text sentiment analysis, word embeddings, and behavioral patterns further aided the classification apportioning precision. Immediate Processing- Analysis of about 30 requests was done in milliseconds per social media profile, allowing users to have timely fraud detection. Challenges:

Social Media Fraud: Under the influence of AI, advanced bots have become capable of generating the most human-like responses and interaction patterns, and thus have become harder to boost.

Prevalence of languages and slangs: Intermingling languages, using Internet jargon, and resorting to regional slangs sometimes actually help one to camouflage their profile detail.

The system is thus seen as biased, working more efficiently on English profiles, while there is still further multilingual need for versatile applicability in regions.

Dissuade Phony Interactions: Many fake accounts try to establish or maintain real interactions to evade complex behavioral modeling that can detect the coordinated presence of a fake network.

VI. CONCLUSION

Detecting fake social media profiles is important for cyber security, integrity in social media and preventing online fraud. Innovation in deception techniques renders legacy methods inefficient, due to biases and scalability issues. Our ANN-based Fake Profile Detection System extracts very high levels of subjectivity in the pattern of text, behavior, and engagements to detect fraudulent accounts.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Key Highlights:

ANN driven analysis yields high accuracy in reduces fake accounts detection.

Offers real time processing for high-speed scaled fraud detection.

Such issues like language diversity, deceptive AI generated profiles and data imbalance require more optimization.

Future improvements in deep ANN, block chain security, and federated learning shall make this system more reliable and private.

With this kind of automated system, humans are able to minimize resource constraint at the same time boost security, improve online interaction and hone the digital platforms from fraudulent acts.

REFERENCES

- 1. K.S. Rao, N. Swapna and P.P. Kumar, "Educational data mining for student placement prediction using machine learning algorithms", Int. J. Eng. Technol. Sci, vol. 7, pp.43-46, 2018.
- K. S. Sreedhar, S. T. Ahmed and G. Sreejesh, "An Improved Technique toIdentify Fake News on Social MediaNetworkusingSupervisedMachineLearning Concepts", IEEE World Conference on AppliedIntelligenceandComputing(AIC), pp.652-658,2022.
- H. Halawa, "Íntegro: Leveraging victim prediction for robust fake account detection in large scaleosns", Computers &Security, vol. 61, pp. 142-168, 2016.
- N. Singh, T. Sharma, A. Thakral and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning", 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 231-234, 2018.
- D. Ramalingam and V. Chinnaiah, "Fake profile detection techniques in large-scale online social networks: A comprehensive review", Computers & Electrical Engineering, vol. 65, pp. 165-177, 2018.
- 6. M.Mohammadrezaei, M.E.Shiriand A.M.Rahmani,"Identifying fake accounts on social networks based on graph analysis and classification algorithms", Security and Communication Networks, 2018.
- 7. Aditi Gupta and Rishabh Kaushal, "Towards detecting fake user accounts in facebook" in 2017 ISEA Asia Security and Privacy (ISEASP), IEEE, pp. 1-6, 2017.
- 8. O. Voitovych, L. Kupershtein and V. Holovenko, "Detection of Fake Accounts in SocialMedia", Том, vol.2, no.18, pp.86-98, 2022.
- 9. N. Leelavathy, V. Sai Sandeep, E. Preethi Sameera, D. Devi and P. Sai Sharma, "Detection of suspicious accounts in Twitter using gradient boosting algorithm", AIP ConferenceProceedings,vol.2492,no.1, 2023.
- Syed Thouheed Ahmed, Dollar Konjengbam Singh, Syed Muzamil Basha, Emad Abouel Nasr, Ali K. Kamrani and Mohamed K. Aboudaif, "Neural network basedmentaldepressionidentificationand sentiments classification technique from speech signals: A COVID-19 Focused Pandemic Study", Frontiers in public health, vol. 9, pp. 781827, 2021.
- 11. MalakAljabri,RachidZagrouba,Afrah Shaahid, Fatima Alnasser, Asalah Saleh and DoriehM.Alomari,"Machine learning-based social media bot detection: A comprehensive literature review", Social Network Analysis and Mining, vol. 13, no. 01, pp. 20, 2023.
- 12. S. T. Ahmed, "A study on multi objective optimal clustering techniques for medical datasets", 2017 International Conference on Intelligent Computing and Control Systems(ICICCS),pp.174177,2017.
- 13. Fabio Persia and Daniela D'Auria, "Information Retrieval from Facebook for Social Network Analysis", 2023 IEEE 17th International Conference on Semantic Computing (ICSC), pp. 329336, 2023.
- 14. Dr. M. Ayyappa Chakravarthi etal. published Springer paper "Machine Learning-Enhanced Self-Management for Energy-Effective and Secure Statistics Assortment in Unattended WSNs" in Springer Nature (Q1), Vol 6, Feb 4th 2025.
- 15. Dr. M. Ayyappa Chakravarthi etal. published Springer paper "GeoAgriGuard AI-Driven Pest and Disease Management with Remote Sensing for Global Food Security" in Springer Nature (Q1), Jan 20th 2025.
- 16. Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper "Machine Learning Algorithms for Automated Synthesis of Biocompatible Nanomaterials", ISBN 979-8-3315-3995-5, Jan 2025.
- 17. Dr. Ayyappa Chakravarthi M. etal, published Scopus paper "Time Patient Monitoring Through Edge Computing: An IoT-Based Healthcare Architecture" in Frontiers in Health Informatics (FHI), Volume13,Issue3,ISSN-Online2676-7104, 29thNov 2024.
- 18. Dr. Ayyappa Chakravarthi M. etal, published Scopus paper "Amalgamate Approaches Can Aid in the Early

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Detection of Coronary heart Disease" in Journal of Theoretical and Applied Information Technology(JATIT), Volume102, Issue 19, ISSN 1992-8645, 2nd Oct 2024.

- Dr. Ayyappa Chakravarthi M, etal, published Scopus paper "The BioShield Algorithm: Pioneering Real-Time Adaptive Security in IoT Networks through Nature- Inspired Machine Learning" in SSRG (Seventh Sense Research Group) - International Journal of Electrical and ElectronicsEngineering(IJEEE), Volume11, Issue 9, ISSN 2348-8379, 28th Sept 2024.
- Ayyappa Chakravarthi M, Dr M. Thillaikarasi, Dr Bhanu Prakash Battula, published SCI paper" Classification of Image Spam Using Convolution Neural Network" in International Information and Engineering Technology Association(IIETA) -"TraitementduSignal"Volume39,No.1.
- Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper "Classification of Social Media Text Spam Using VAE-CNN and LSTM Model"inInternational Information and Engineering Technology Association (IIETA) - Ingénierie des Systèmes d'Information (Free Scopus) Volume 25, No. 6.
- 22. Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper "Social Media Text Data Classification using Enhanced TF_IDF based Feature Classification using Naive Bayesian Classifier" in International Journal of Advanced Science and Technology (IJAST) 2020
- 23. Ayyappa Chakravarthi M. presented and published IEEE paper on "The Etymology of Bigdata on Government Processes" with DOI 10.1109/ICICES.2017.8070712 and Scopus Indexed online in IEEE digital Xplore with Electronic ISBN: 978-1-5090- 6135-8, Print on Demand (PoD) ISBN:978-1-5090-6136-5, Feb 2017.
- 24. Subba Reddy Thumu & Geethanjali Nellore, Optimized Ensemble Support Vector Regression Models for Predicting Stock Prices with Multiple Kernels. Acta Informatica Pragensia, 13(1), x-x. 2024.
- 25. Subba Reddy Thumu, Prof. N. Geethanjali. (2024). "Improving Cryptocurrency Price Prediction Accuracy with Multi-Kernel Support Vector Regression Approach". International Research Journal of Multidisciplinary Technovation 6 (4):20-31.
- 26. Dr syamsundararaothalakola et.al. published Scopus paper "An Innovative Secure and Privacy-Preserving Federated Learning Based Hybrid Deep Learning Model for Intrusion Detection in Internet- Enabled Wireless SensorNetworks" in IEEE Transactions on Consumer Electronics 2024.
- 27. Dr syamsundararaothalakola et.al. published Scopus paper "Securing Digital Records: A Synerigistic Approach with IoT and Blockchain for Enhanced Trust and Transparency" in International Journal of Intelligent Systems and Applications in Engineering 2024.
- 28. Dr syamsundararaothalakola et.al. published Scopus paper "AModel for Safety Risk Evaluation of Connected Car Network" inReview of Computer Engineering Research2022.
- 29. Dr syamsundararaothalakola et.al. publishedScopuspaper"An Efficient Signal Processing Algorithm for Detecting Abnormalities in EEG Signal Using CNN"in Contrast Media and Molecular Imaging 2022.
- 30. Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper "Evolutionary Algorithms for Deep Learning in Secure Network Environments" ISBN:979-8-3315-3995-5, Jan 2025.





INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com