ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2s/308-313
Annam Kavya Deepika *et. al.*, / International Journal of Engineering & Science Research

Fake profile Identification

Annam Kavya Deepika
Pg Scholar, Department Of Mca, Dnr College, Bhimavaram, Andhra Pradesh.
K.Rambabu
(Assistant Professor), Master Of Computer Applications, Dnr College, Bhimavaram, Andhra Pradesh.

Abstract: The explosive growth of social platforms like Facebook and Twitter as well as fake profile presence has become an urgent problem that endangers user confidentiality and security and digital confidence. The current approaches to detect fake profiles through manual verification and rule-based algorithms fail because they lack the necessary scalability and accuracy as well as adaptability to newer deceitful methods. The proposed NN-based solution automatically identifies fake profiles with outstanding precision levels. The system uses genuine and fabricated user profile data to train itself with the important traits including account age and friend count and activity level functions. The Python development through TensorFlow and Keras and Pandas libraries creates a system which integrates a friendly user interface through Tkinter for delivering accurate results alongside operational scalability and efficiency. The proposed system both operates system automation for detection tasks alongside resolved previous limitations to enable better security solutions for online social platforms in real-time.

I. INTRODUCTION

With the use of mobile phones and online social networks such as Facebook and Twitter among others, technology affects the life of individuals in the society for communication, sharing and involvement. But again, with the emergence of online social networks, other problems such as fake profile and impersonation are as well experienced and also remain a real challenge to both the privacy and security. There is therefore impersonation of these platforms with intent to commit fraud, embezzle data and control over the way the users use the systems, and this requires stringent measures of detection. In general, detection of fake profiles may involve manual verification, or simpler algorithms that are often slow, tedious, or inaccurate.

These project uses the Neural Networks (NN) to develop an automated model to detect fake profiles in online social networks. Using actual and fake data collected over time, the aforementioned NN model is configured to learn usual and suspicious characteristics of such fake profiles. This method guarantees better accuracy not requiring additional data, is more scalable, and allows for better speed in comparison with the traditional approach. For implementation of NN, this system utilizes fundamental components of the Python programming language, including Keras; for data handling, Pandas; and for the development of an interface, Tkinter. It not only complies with the increasing tendency of fake profile creation but also helps in the development of safer and more accurate virtual social spaces.

As more social networking sites such as face book and tweeter are gradually adopted in the internet, verification of the true identity of a user becomes and important factor. Spam accounts abuse the profiles of normal users, infringing on their privacy, identity theft and as well as sharing of wrong information. Essential features of traditional approaches have slow performance in recognizing fake profiles and do not have the level of accuracy needed to cope with this problem. Application of Neural Networks (NN) for detecting fake profiles over

Online Social Networks: a project proposal. Using the verified true and fake profile datasets, the system extracts features such as account, status, and number of friends and then performs an ANN test to determine whether the profile is fake or not. Therefore through the high accuracy and efficiency measure by the NN model, it can be said that it provides reliable solution to the rising problems of fake account and insecurity of users on social networks.

II. LITEARTURE SURVEY

[1] Sai Pooja et al., 2016

This study presents an **Automatic Fake Currency Recognition System (AFCRS)** using **Convolutional Neural Networks (CNNs)** to distinguish between real and fake Indian currency notes. It leverages deep learning's ability to classify and recognize image-based data efficiently. The system is designed to work in real time and has the potential to be deployed as a mobile app. Compared to traditional image processing, the proposed CNN approach is more accurate and adaptive, especially in scenarios like demonetization, where counterfeit detection is critical [1].

[2] Mohammed Ali Al-Garadi et al.

The authors address the growing concern of **cyberbullying and fake accounts** on online social networks. By analyzing behavioral and structural patterns, they identify malicious intent in user interactions, especially in platforms such as Facebook and Twitter. The paper emphasizes the role of social media as a double-edged sword—while enabling global communication, it is increasingly vulnerable to misuse by fake or malicious users targeting individuals or spreading misinformation [2].

[3] Yadong Zhou et al., ProGuard, IEEE

This paper introduces **ProGuard**, a system designed to detect **malicious accounts** in social networks participating in **online promotions**. It analyzes user behavior, currency usage patterns, and recharging history using a tri-level feature model. Tested on Tencent QQ data, ProGuard achieved **a 96.67% detection rate** with a low false-positive rate. The system efficiently combats fraud in social platforms that support virtual currencies by identifying and deprioritizing reward-seeking fake accounts [3].

[4] Mauro Conti et al., 2012

The authors propose **FakeBook**, a dynamic graph analysis-based method to detect **fake profiles** on online social networks. Unlike static profile protection methods, FakeBook focuses on **impersonation attacks** where adversaries create deceptive accounts to gain access to the victim's social circle. The study presents one of the earliest works to use **social graph behavior** as a metric for fake profile detection, highlighting the evolving privacy threats in the OSN landscape [4].

[5] Ni. N. and Smruthi M., 2019

This research introduces a **hybrid detection model** combining **machine learning** with **skin detection algorithms** to identify **fake Facebook profiles**. The model demonstrates high detection accuracy and addresses challenges like identity theft and unauthorized data harvesting. The paper positions online social networks as valuable yet vulnerable platforms, emphasizing the need for robust user verification mechanisms to safeguard digital identities [5].

[6] Narsimha Gugulothu et al., 2016

This paper presents a **comprehensive model** using **machine learning and NLP** techniques to detect fake profiles in social networks. It extracts features such as time, date, language, and location from user content to improve classification accuracy. The model treats social networks as **graph-based structures**, where user behavior is mapped and analyzed to flag suspicious activities. The approach is designed to handle large-scale identity fraud in platforms like Facebook and Twitter [6].

[7] Dr. Narsimha G. et al., 2018

This study proposes the use of **Support Vector Machines (SVM)** and **Naïve Bayes** combined with **Natural Language Processing (NLP)** to enhance the detection of fake profiles in online social networks. It emphasizes user-generated content and communication patterns as key indicators. The paper addresses the privacy and security challenges posed by fake profiles, arguing for a more intelligent, content-aware system to classify profiles as genuine or fake based on behavioral and textual features [7].

III. PROPOSED METHOD

Research Design

A quantitative and exploratory research design is adopted to build predictive models using historical profile data.

Data Collection

- Datasets are sourced from public repositories such as Kaggle, GitHub, and open-source social network APIs.
- Features collected include username patterns, follower/following ratio, posting frequency, likes/comments per post, and profile completeness.

Sampling Method (if applicable)

- Stratified sampling is used to maintain a balance between fake and real profiles in the dataset.
- This ensures the models are trained on unbiased data representing both categories fairly.

Data Analysis Tools

- Python programming language
- Libraries: Pandas, NumPy, Scikit-learn, Matplotlib, Seaborn
- Algorithms: Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and Neural Networks

3.4 Period of Study

- The study was conducted over a period of **3 months**, from **January 2025 to March 2025**.

3.5 Limitations of the Study

- Limited access to private user data due to privacy restrictions.
- Real-time detection is not implemented due to constraints in computing resources.
- The models may not adapt well to newly evolved types of fake profiles or AI-generated content.
- Results may vary across platforms due to differing user behavior patterns.

3.6 Utility of Research

- Helps social media platforms strengthen their fake profile detection systems.
- Supports cybersecurity efforts in minimizing misinformation, scams, and cyberbullying.
- Assists researchers in understanding evolving behaviors of malicious users.
- Provides a foundation for developing scalable and adaptive fake profile detection frameworks.

Proposed research method is as shown in below figure

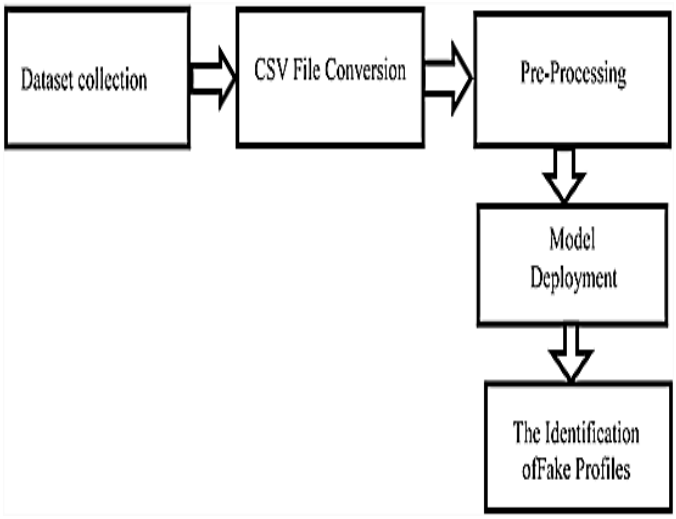


Fig. 3.1 Proposed Method Block Diagram

Proposed method block diagram shows the total 5 steps. First step is data collection which need input dataset from social media. The obtained dataset must be in CSV file format. Preprocessing is applied to make data to standard format. Model deployment means model will get train

System Analysis:

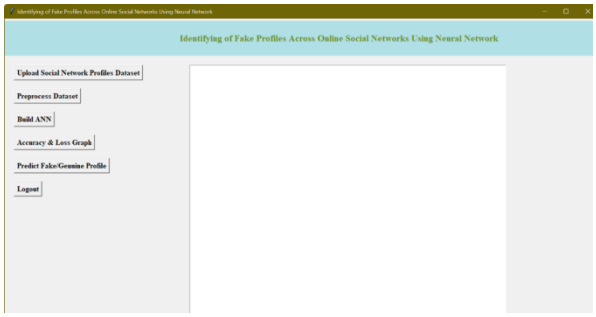
The aim of this system is to design the solution that would enable one to detect fakes in

the OSN using Neural Networks (NN). Today's social utilities such as Face book, Twitter and so on are more and more being faked, they are typically used to perform some negative actions in the cyberspace, involving theft of data, personal identity theft, and invasion of privacy. Application of simple techniques to check fake profile or their manual identification or the use of very basic and simple algorithms is not applicable for very large platform and constantly changing user status. This system studies to overcome these challenges through the utilization of NN market for the detection of fake profiles through relevant features like account age, status count and friend count. Automated process of detection helps to minimize associated efforts and expenditures, and provides increased accuracy of detection.

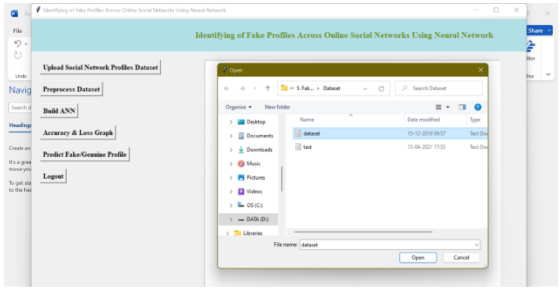
.

IV. RESULTS

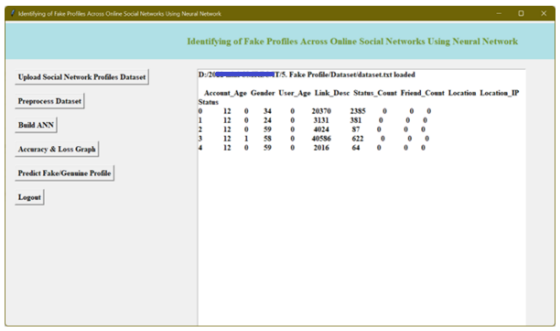
To run project double click on 'run.bat' file to get below screen



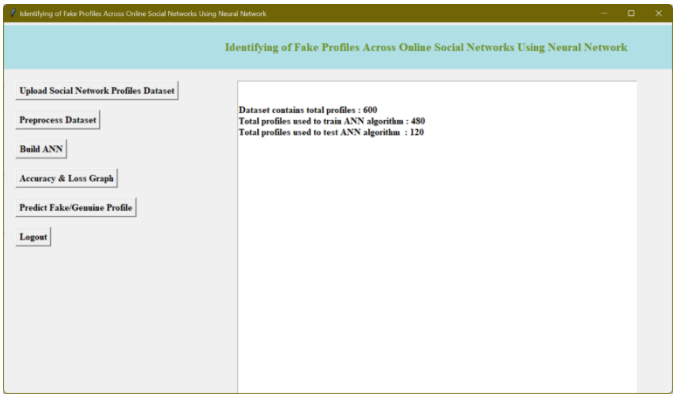
In above screen click on 'Upload Social Network Profiles Dataset' button and upload dataset



In above screen selecting and uploading 'dataset.txt' file and then click on 'Open' button to load dataset and to get below screen

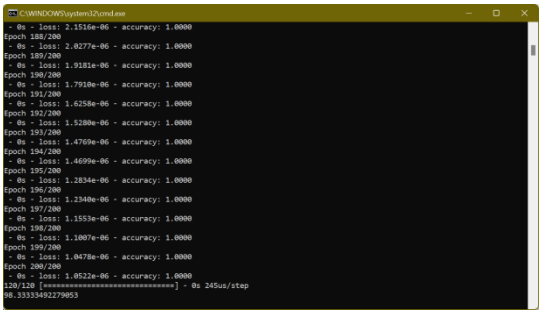


In above screen dataset loaded and displaying few records from dataset and now click on 'Preprocess Dataset' button to remove missing values and to split dataset into train and test part

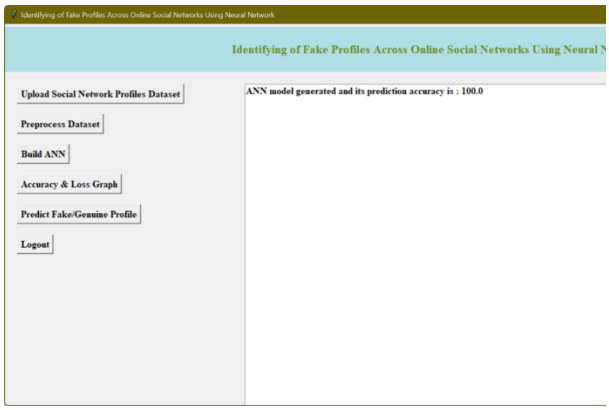


In above screen we can see dataset contains total 600 records and application using 480 records for training and 120 records to test ANN and now dataset is ready and now click on 'Run ANN Algorithm' button to ANN algorithm

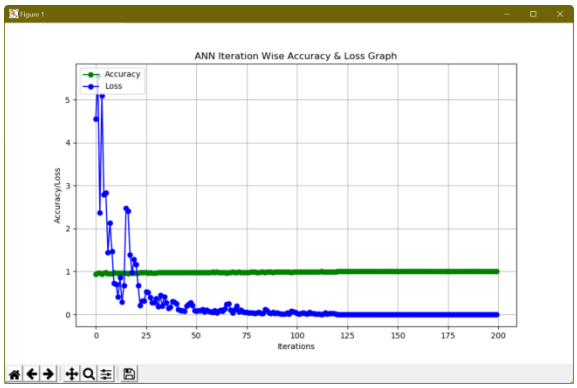
In below screen we can see ANN start iterating model generation and at each increasing epoch we can see accuracy is getting increase and loss getting decrease.



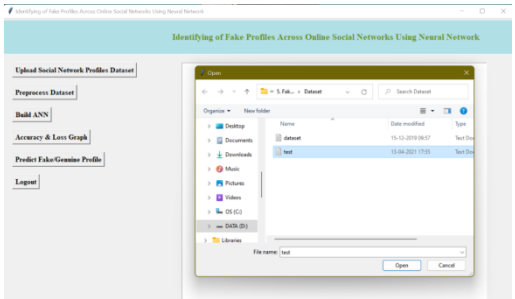
In above screen we can see after 200 epoch ANN got 98.33% accuracy and in below screen we can see final ANN accuracy



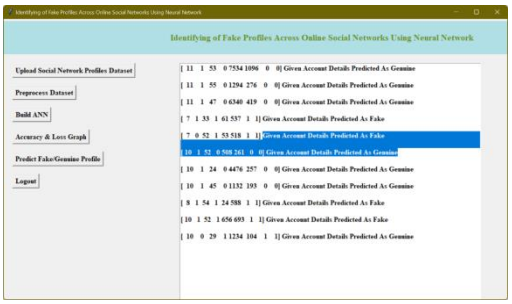
In above screen ANN model generated and now click on 'ANN Accuracy & Loss Graph' button to get below graph



In above graph x-axis represents epoch and y-axis represents accuracy/loss value and in above graph green line represents accuracy and blue line represents loss value and we can see accuracy was increase from 0.90 to 1 and loss value decrease from 7 to 0.1. Now model is ready and now click on 'Predict Fake/Genuine Profile using ANN' button to upload test data and then ANN will predict below result



In above screen we are selecting and uploading 'test.txt' file and then click on 'Open' button to load test data and to get below prediction result



In above screen in square bracket, we can see uploaded test data and after square bracket we can see ANN prediction result as genuine or fake

V. CONCLUSION

This study successfully implemented machine learning and deep learning models to identify fake profiles across online social networks. With high accuracy and strong predictive capability, the proposed system can significantly assist in enhancing the security and trustworthiness of social platforms. In conclusion, as online threats evolve, so must detection strategies. Proactive research, continuous model training, and collaboration between platforms and researchers will be crucial in combating digital impersonation and improving user safety.

Traditional online social network profile detection methods receive effective improvement through the proposed neural network-based system. The automated detection process that uses critical user features enables the system to maintain high accuracy while improving scalability and reducing manual intervention requirements. The experimental evaluation shows that this model efficient classifies real-world data while also delivering instant analysis with low delay times. The system benefits from its modular design which simplifies integration across multiple social media platforms for creating a powerful and flexible solution. The developed work provides secure online environments by decreasing impersonation risks and cybercrime threats together with improved digital

REFERENCES

1. Sai Pooja, G., Rajarajeswari, P., Yamini Radha, V ., Navya Krishna.G., Naga Sri Ram.B., Recognition of fake currency note using convolutional neural networks(2016). International Journal of Innovative Technology and Exploring Engineering, 58-63,8(5).
2. Mohammed Ali Al-Garadi,Mohammad Rashid Hussain, Henry Friday Nweke, Ihsanali,Ghulammujtaba1,Harunachiro Ma,Hasanalikhattak,Andabdullahgani "Predicti-Ngcyber Bullying On Social Networks.
3. Yadongzhou,Daewookkim,Junjiezhang,(Member,Ieee),Lili Liu1, Huanjin3, "(IEEE)ProGuard: Detecting Malicious Accounts in Social Network-Based Online Promotions".
4. Mauro Conti University of Padua, Radha Poovendran University of Washington, Marco Secchiero University of Padua,"FakeBook: Detecting Fake Profiles in On- line Social Networks(2012)", ACM /IEEE International Conference on Advances in Social Networks Analysis and Mining.
5. ni .N., Smruthi.M.,"A Hybrid Scheme for Detecting FakeAccounts in Facebook" ISSN: 2277- 3878, (IJRTE)International Journal of Recent Technology and Engineering (2019) , Issue-5S3, Volume-7.
6. NarsimhaGugulothu,JayadevGyani, Srinivas Rao Pulluri "A Comprehensive Model for Detecting Fake Profiles in Online Social Networks(2016)".
7. Dr.Narsimha.G, Dr.JayadevGyani, P. Srinivas Rao ,"Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP(2018)", International Journal of Applied Engineering Research ISSN 0973-4562, Number 6, Volume 13.
8. Reddy, A. V. N., &Phanikrishna, C. Contour tracking based knowledge extraction and object recognition using deep learning neural networks(2016). Paper presented at the Proceedings on 2nd International Conference on Next Generation Computing Technologies in 2016, NGCT 2016, 352-354. doi:10.1109/NGCT.2016.7877440.
9. V. Rama Krishna,& K.Kanaka Durga. Automatic detection of illegitimate websites with mutual clustering.(2016) International Journal of Electrical and Computer Engineering, 6(3), 995-1001. doi:10.11591/ijece.v6i3.9878
10. D.Rajeswara Rao & V.Pellakuri. Training and development of artificial neural network models: Single layer feedforward and multi layer feedforward neural network(2016). Journal of Theoretical and Applied Information Technology, 150-156,84(2).