International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

AI-BASED FAKE PROFILE DETECTION SYSTEM FOR SOCIAL NETWORKS USING NLP AND DEEP LEARNING

Sandyarani[1], Anil Gujar[2]

[1]Student, Computer Department, BSCOER, Savitribai Phule Pune University, India

[2]Professor, Computer Department, BSCOER, Savitribai Phule Pune University, India

Email: [1]sr9131180@gmail.com , [2]anilranjester@gmail.com

Abstract*:*

At present, social network sites are an integral part of daily life for most people. Every day, numerous users create profiles on social network platforms, engaging with others regardless of location and time. While social networks offer significant advantages, they also pose security risks, including identity fraud and misinformation. To mitigate these risks, it is essential to classify user profiles into genuine and fake categories. Traditionally, various machine learning-based classification techniques have been used for fake profile detection. However, improving accuracy remains a challenge. In this paper, we propose an AI-driven approach using Natural Language Processing (NLP) and Deep Learning techniques to enhance fake profile detection accuracy. Along with Support Vector Machine (SVM) and Naïve Bayes classifiers, we integrate a Convolutional Neural Network (CNN) model to analyse textual and behavioural patterns in profile data. The CNN model captures intricate patterns in user-generated content, improving classification precision and robustness. Experimental results demonstrate that our hybrid approach significantly improves detection accuracy compared to traditional machine learning methods. The proposed system provides a more reliable and scalable solution for identifying fake profiles in social networks, thereby enhancing online security and trustworthiness.

Keywords: Machine Learning, Natural Language Processing, Classification

1. INTRODUCTION

Social networking has end up a well-known recreation within the web at present, attracting hundreds of thousands of users, spending billions of minutes on such services. Online Social network (OSN) services variety from social interactions-based platforms similar to Face book or MySpace, to understanding dissemination-centric platforms reminiscent of twitter or Google Buzz, to Social interaction characteristic brought to present systems such as Flicker. The opposite hand, enhancing security concerns and protecting the OSN privateness still signify a most important bottleneck and viewed mission.

Profile information in online networks will also be static or dynamic. The details which can be supplied with the aid of the person on the time of profile creation is known as static knowledge, the place as the small print that are recounted with the aid of the system within the network is called dynamic knowledge. Static

knowledge includes demographic elements of a person and his/her interests and dynamic knowledge includes person runtime habits and locality in the network. The vast majority of current research depends on static and dynamic data. However this isn't relevant to lots of the social networks, where handiest some of static profiles are seen and dynamic profiles usually are not obvious to the person network. More than a few procedures have been proposed by one of a kind researcher to realize the fake identities and malicious content material in online social networks. Each process had its own deserves and demerits.

The problems involving social networking like privacy, online bullying, misuse, and trolling and many others. Are many of the instances utilized by false profiles on social networking sites. False profiles are the profiles which are not specific i.e. They're the profiles of men and women with false credentials. The false Face book profiles more commonly are indulged in malicious and undesirable activities, causing problems to the social community customers. Individuals create fake profiles for social engineering, online impersonation to defame a man or woman, promoting and campaigning for a character or a crowd of individuals. Face book has its own security system to guard person credentials from spamming, phishing, and so on. And the equal is often called Facebook Immune system (FIS).

The FIS has now not been ready to observe fake profiles created on Facebook via customers to a bigger extent

2. LITERATURE SURVEY

E-Learning Platforms like LinkedIn, identifying fake profiles poses significant challenges, affecting trust and engagement. Fake Profiles can mislead users, dilute the quality of interactions and undermine the credibility of the Platform (1). Social networking platforms are now a common aspect of daily life for most people. Every day, a large number of people create profiles on social networking sites and interact with others, regardless of their location or time of day (2). Online social networks (OSN) are well-known platforms for exchanging various information. However, one of the existing OSN challenges is the issue of fake accounts. The attacker harnesses malicious accounts in the infected system to spread false information, such as malware, viruses, and harmful URLs (3). Preprocessing is an important task and critical step in Text mining, Natural Language Processing (NLP) and information retrieval (IR). In the area of Text Mining, data preprocessing used for extracting interesting and non-trivial and knowledge from unstructured text data. Information Retrieval (IR) is essentially a matter of deciding which documents in a collection should be retrieved to satisfy a user's need for information (4). As organizations increasingly rely on professionally oriented networks such as LinkedIn (the largest such social network) for building business connections, there is increasing value in having one's profile noticed within the network (5). Fake and Clone profiles are creating dangerous security problems to social network users. Cloning of user profiles is one serious threat, where already existing user’s details are stolen to create duplicate profiles and then it is misused for damaging the identity of original profile owner (6). The social network a crucial part of our life is plagued by online impersonation and fake accounts. Facebook, Instagram, Snapchat are the most well-known informal communities’ sites (7). Popular Internet sites are under attack all the time from phishers, fraudsters, and spammers. They aim to steal user information and expose users to unwanted spam (8). Many people today use social networking sites as a part of their everyday lives. They create their own

profiles on the social network platforms every day, and they interact with others regardless of their location and time (9). Popular online social networks (OSNs) like Facebook and Twitter are changing the way users communicate and interact with the Internet. A deep understanding of user interactions in OSNs can provide important insights into questions of human social behavior and into the design of social platforms and applications (10). The problem of social capital in context of the online social networks is presented in the paper. Not only the specific elements, which characterize the single person and influence the individual's social capital like static social capital, activity component, and social position, but also the ways of stimulation of the social capital are described (11).

3. SYSTEM ANALYSIS AND DESIGN

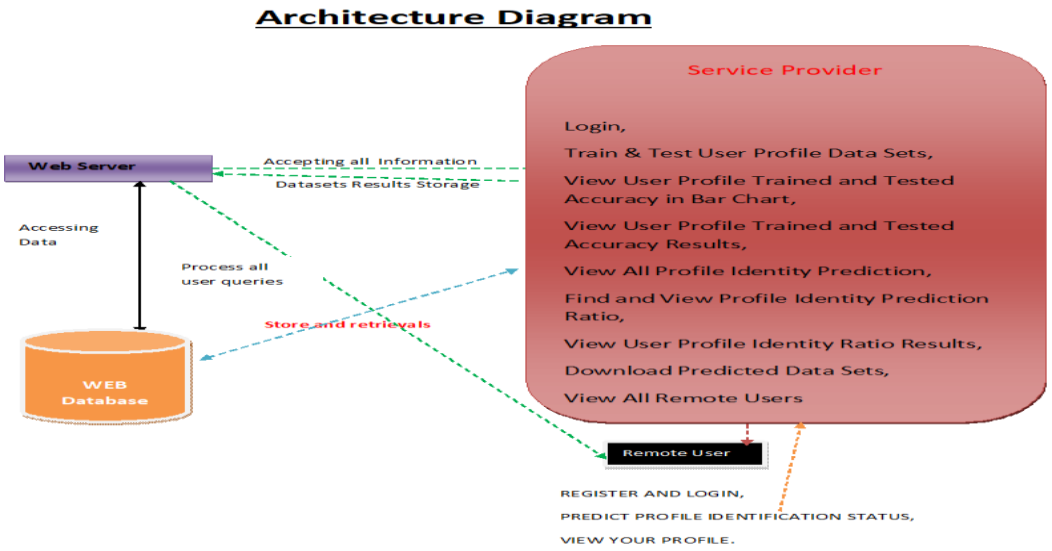
3.1 EXISTING SYSTEM

Chai et al. introduced a prototype approach utilizing Natural Language Processing (NLP) and human-computer interaction techniques for social networks. The study revealed that users, especially beginners, preferred natural language dialogue-based interactions over traditional menu-based systems. However, the study also highlighted that in an e-commerce environment, sophisticated dialogue management was more important than handling complex natural language sentences.

3.2 PROPOSED SYSTEM

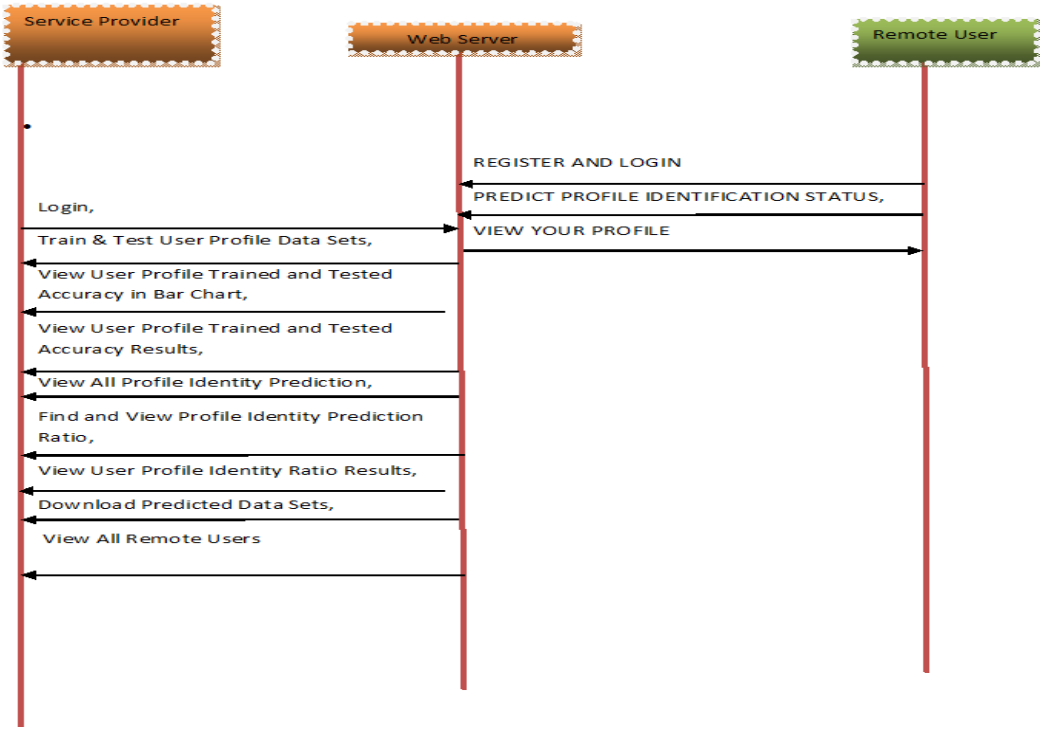
In this paper, we propose an AI-based system that integrates Machine Learning, Natural Language Processing (NLP), and Deep Learning techniques to detect fake profiles in online social networks. Our approach enhances detection accuracy by combining traditional classifiers like Support Vector Machine (SVM) and Naïve Bayes with a Convolutional Neural Network (CNN) model.

3.3 SYSTEM DESIGN

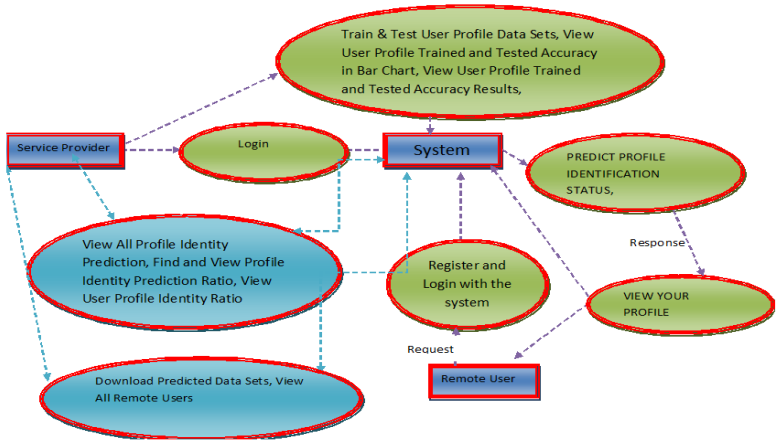


International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3.4 SEQUENCE DIAGRAM



3.5 DATA FLOW DIAGRAM



3.6 INPUT AND OUTPUT DESIGN

3.6.1 INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed

document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

3.6.2 OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2.It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

3.6.3 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

4. IMPLEMENTATION

4.1 Modules

4.1.1 Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Train & Test User Profile Data Sets, View User Profile Trained and Tested Accuracy in Bar Chart, View User Profile Trained and Tested Accuracy Results, View All Profile Identity Prediction, Find and View Profile Identity Prediction Ratio, View User Profile Identity Ratio Results, Download Predicted Data Sets, View All Remote Users

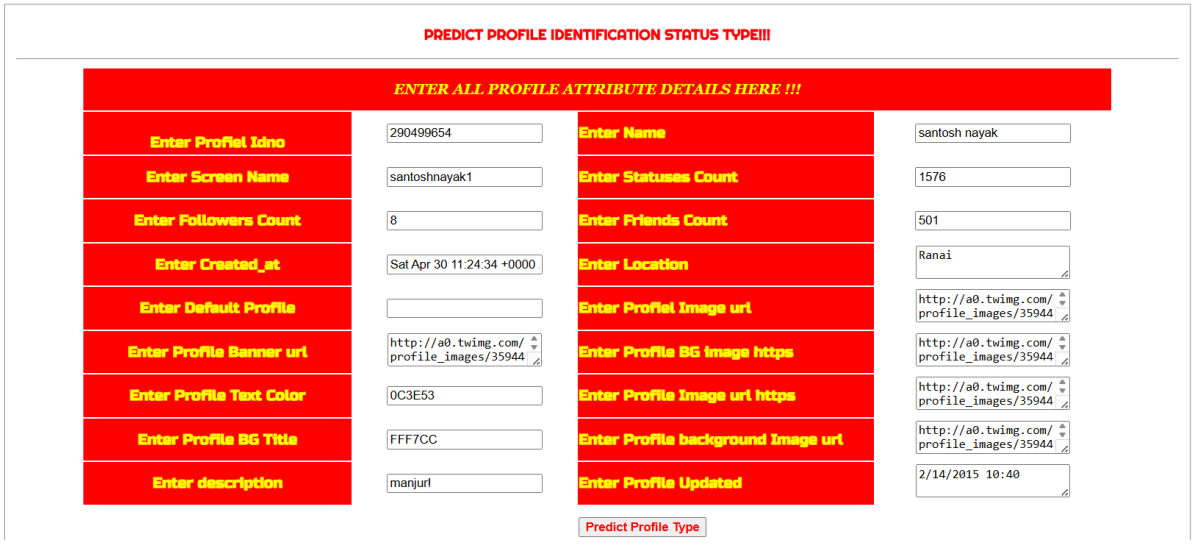
4.1.2 View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

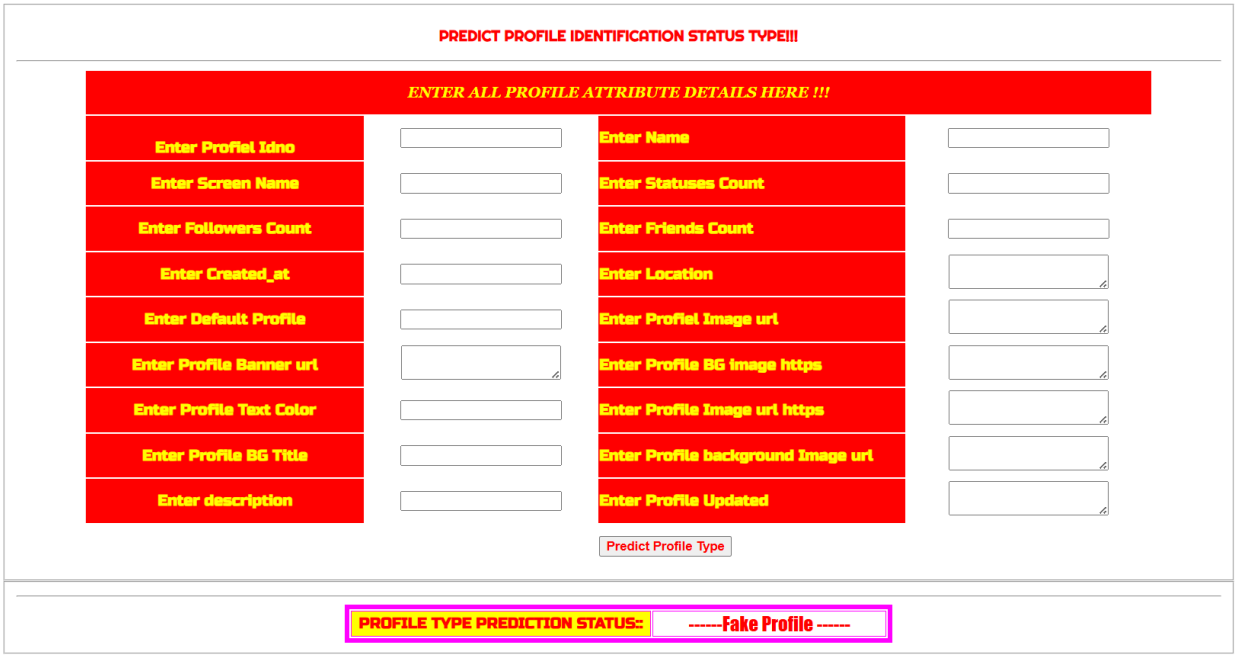
4.1.3 Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PROFILE IDENTIFICATION STATUS, VIEW YOUR PROFILE.

4.1.4 SCREEN SHOTS



International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354



5. CONCLUSIONS & FUTURE ENHANCEMENT

5.1 CONCLUSION

In this paper, we proposed machine learning algorithms along with natural language processing techniques. By using these techniques, we can easily detect the fake profiles from the social network sites.

In this paper we took the Face book Data set to identify the fake profiles. The NLP pre-processing techniques are used to analyse the dataset and machine learning algorithm such as SVM and Naïve Bayes are used to classify the profiles. These learning algorithms are improved the detection accuracy rate in this paper.

5.2 FUTURE ENHANCEMENT

While the proposed hybrid model leveraging NLP, Deep Learning (CNN), and traditional classifiers has shown significant improvements in detecting fake profiles on social networks, several avenues remain for future enhancement to further improve accuracy, scalability, and adaptability.

One key direction is the incorporation of **real-time detection capabilities**, allowing the system to identify suspicious activity as it occurs. This would enhance responsiveness and could be vital in mitigating potential threats before they escalate. Additionally, expanding the system to analyze **multimodal data**, such as profile images, shared multimedia content, and connection patterns, can significantly boost classification performance. Integrating **computer vision techniques** for image verification and **Graph Neural Networks (GNNs)** for network behaviour analysis offers a comprehensive approach to identifying coordinated fake accounts.

REFERENCES

[1] Kalai Selvi T, Abirami S, Aravind S, Ariharan M.(2025).Fake Profile Identification in E-Learning Platform using Machine Learning.

[2]Dr. P. Shanthakumar1, S. Jeyasri Pooja2, R.Jenifer2(2023).Fake Profile Identification in Online Social Networks Using Machine Learning

[3]Putra Wanda(2022).fake profile classification using novel nonlinear activation in CNN

[4] Dr. S. Kannan, Vairaprakash Gurusamy, "Preprocessing Techniques for Text Mining", 05 March 2015.

[5] Shalinda Adikari and Kaushik Dutta, Identifying Fake Profiles in LinkedIn, PACIS 2014 Proceedings, AISeL

[6] Michael Fire et al. (2012). "Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies." Human Journal 1(1): 26-39.Günther, F. and S. Fritsch (2010). "neuralnet: Training of neural networks." The R Journal 2(1): 30-38

[7] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,"Malicious users' circle detection in social network based on spatiotemporal co-occurrence," in Computer Networks and Information Technology (ICCNIT),2011 International Conference on, July, pp. 35–390.

[8] Stein T, Chen E, Mangla K," Facebook immune system. In: Proceedings of the 4th workshop on social network systems", ACM 2011, pp

[9] Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi, "Malicious and Spam Posts in Online Social Networks," Computer, vol.44, no.9, IEEE2011, pp.23– 28.

[10] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, B. Zhao, Understanding latent interactions in online social networks, in: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, ACM, 2010, pp. 369–382

[11] Kazienko, P. and K. Musiał (2006). Social capital in online social networks.Knowledge-Based Intelligent Information and Engineering Systems.