e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

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

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707100 |

Fake Profile Identification in Social Network

Rohith M[1], Shwethashri K[2]

Student, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: At present social network sites are part of the life for most of the people. Every day several people are creating their profiles on the social network platforms and they are interacting with others independent of the user's location and time. The social network sites not only providing advantages to the users and also provide security issues to the users as well their information. To analyse, who are encouraging threats in social network we need to classify the social networks profiles of the users. From the classification, we can get the genuine profiles and fake profiles on the social networks. Traditionally, we have different classification methods for detecting the fake profiles on the social networks. But, we need to improve the accuracy rate of the fake profile detection in the social networks. In this paper we are proposing Machine learning and Natural language Processing (NLP) techniques to improve the accuracy rate of the fake profiles detection. We can use the Support Vector Machine (SVM) and Naïve Bayes algorithm.

KEY WORDS: SVM, NLP, Machine Learning, Fake Profile, Social Networks

I. INTRODUCTION

Currently, long-distance informal conversation has become a significant online diversion, attracting a large number of users who spend billions of minutes using these services. Web-based social networks (Facebook, MySpace, etc.) and knowledge-sharing networks (Twitter, Google Buzz, etc.) are examples of online informal communities (OSN) services. Social media trademarks are used to launch applications such as Glint. Upgraded security issues, on the other hand, protect OSN privacy and represent a major bottleneck and saw goal.

Using their Social Networks (Sns), exceptional people disclose different levels of their private knowledge. Because of our unique ability, which is either completely or partially disclosed to the public, we are excellent targets for many different kinds of attacks, the most heinous of which may be identifying evidence theft. Fraud occurs when someone manipulates a character's skill for personal gain or other ulterior motive. Because it has affected a great number of people worldwide, online identification theft has been a major problem in recent years. Victims of distinctive proof robbery may face unusual sanctions, such as time or money loss, placement in a reformatory, destruction of their public image, or damage to their relationships with friends, family, and lovers. Currently, the vast majority of SNs do longer verify typical users' requirements and have completely helpless privacy and wellness policies. Actually, the majority of SN applications have their privacy settings set to a trivial degree by default, which has made SNs an ideal platform for deception and abuse. Long-distance unofficial communication contributions have helped both major and innocent aggressors deal with fraud and pantomime attacks. Clients are expected to have the necessary understanding to create a record on person-to-person communication sites, which exacerbates the dilemma. Merely keeping an eye on what customers post online may lead to terrible consequences, not to mention if those bills had been compromised.

II. LITERATURE SURVEY

Chai et al granted on this thesis is a proof-of motivation gain information on. Despite the fact that the model methodology has utilized best typical frameworks in ordinary language handling and human-pc exchange, the outcomes acknowledged from the client giving a shot are critical. By utilizing contrasting this straightforward model methodology and a completely sent menu technique, they've found that clients, mainly novice clients, emphatically pick the normal language exchange based approach. Additionally, they've learned that in an online business climate refinement in exchange organization is generally significant than the possibility to oversee complex ordinary language sentences. Likewise, to give easy admittance to information on internet business sites, normal language exchange based route and menu-pushednavigation ought to be keenly joined to meet individual's unique needs. Not very far in the past, they have achieved improvement of another emphasis of the methodology that remembers gigantic upgrades for

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707100 |

language handling, exchange organization and data the executives. They accepted that normal language casual connection points present strong customized options to customary menupushed or search-based connection points to web sites.LinkedIn is enormously liked through the people who're in the genuine occupations. With the rapid advancement of informal communities, people are probably going to abuse them for exploitative and unlawful behaviors. Production of a bogus profile transforms into such enemy results which is mind boggling to distinguish without well-suited research. The ongoing arrangements which were essentially community ties of the individual's social profile. Nonetheless, according to LinkedIn such social perceptions are massively prohibitive in openly to be had

III. SYSTEM DESIGN

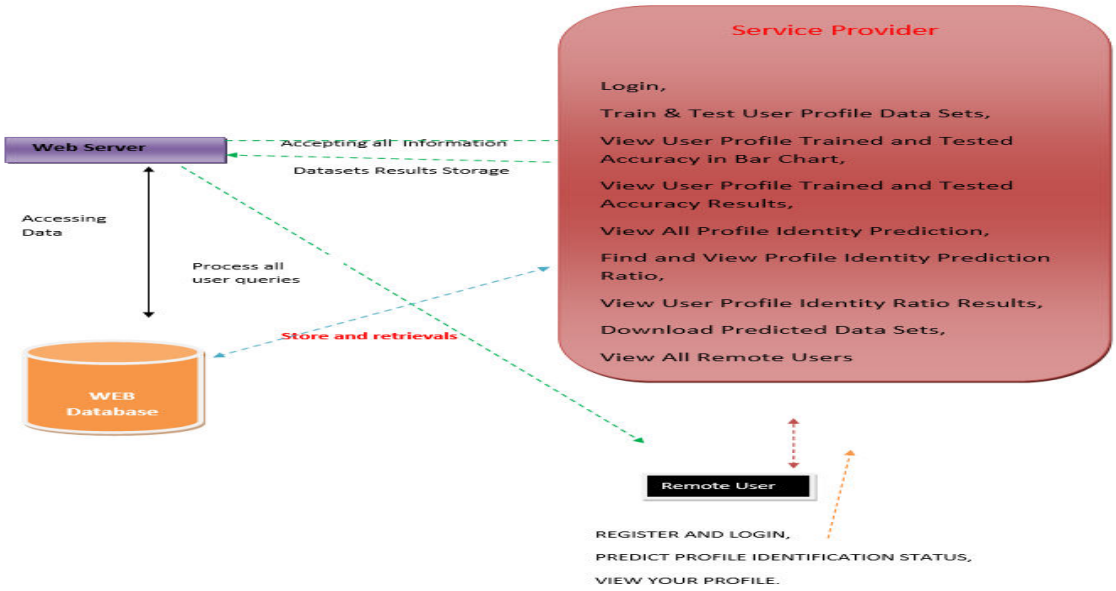

Fig 1: System Architecture

IV. PROPOSED METHODOLOGY

We introduced a machine learning and natural language processing method in this study to detect fraudulent profiles in online social networks. Furthermore, we are including the SVM classifier and the naive bayes method to improve the detection accuracy of bogus profiles.

An SVM classifies data by locating the exceptional hyperplane that divides all information aspects of one type from those of the other. The optimum hyperplane for an SVM algorithm is the one with the longest line connecting the two classes. An SVM classifies data by identifying the exceptional hyperplane that distinguishes all knowledge aspects of one category from those of the other. The assistance vectors are the information aspects that are closest to the separating hyperplane.

The Naive Bayes algorithm learns the likelihood of an object with certain qualities belonging to a specific crew/category. In a nutshell, it is a probabilistic classifier. The Naive Bayes algorithm is dubbed "naive" because it believes that the presence of a certain characteristic is independent of the presence of other factors. For example, suppose we want to identify fraudulent profiles based on their time, date of publication or posts, language, and geolocation. Even though these points are dependent on one another or on the existence of other aspects, all of these features, in my opinion, add to the possibility of a misleading profile.

Profile information in online networks will also be static or dynamic in the proposed system. The information provided by the user at the time of profile creation is referred to as static knowledge, whilst the information relayed by the system inside the network is referred to as dynamic knowledge.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707100 |

V. OBJECTIVES

To foster a powerful framework for grouping informal community profiles to recognize certified and counterfeit profiles. To use AI (ML) and Normal Language Handling (NLP) methods to upgrade the precision pace of phony profile location on interpersonal organizations. To execute and look at the viability of Help Vector Machine (SVM) and Gullible Bayes calculations in recognizing counterfeit profiles. To give a solid and dependable device

VI. IMPLEMENTATION

Service Provider: The Service Provider must login to this module using a valid user name and password. He can do various actions after successfully logging in, such as Login, User Profile Data Sets must be trained and tested. View User Profile Trained and Tested Accuracy Results, View All Profile Identity Prediction, and more. Locate and view the Profile Identity Prediction Ratio. View Predicted Data Sets, View User Profile Identity Ratio Results, View Every Remote User

View and Authorize Users: The admin may view a list of all registered users in this module. The admin may examine the user's data such as user name, email, and address, and the admin can approve the users.

Remote User: There are a n number of users in this module. Before doing any activities, the user must first register. When a user registers, their information is saved in the database. After successfully registering, he must login using his permitted user name and password. Once logged in, the user may do the following actions: REGISTER AND LOGIN, PREDICT PROFILE IDENTIFICATION STATUS, and VIEW YOUR PROFILE

Fig 2: User Login

Fig 3: User Registration

Fig 4: Admin Login

Fig 5: View All Profile Status Prediction Type

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707100 |

VII. CONCLUSION

In this thesis, we proposed AI calculations alongside normal language handling methods. By utilizing these procedures, we can undoubtedly distinguish the phony profiles from the informal organization destinations. In this thesis we took the Face book Informational collection to recognize the phony profiles. The NLP pre-handling procedures are utilized to investigate the dataset and AI calculation, for example, SVM and Credulous Bayes are utilized to arrange the profiles. These learning calculations are further developed the identification exactness rate in this thesis.

REFERENCES

[1] Michael Fire & colleagues (2012). "Other people infiltration detection-detecting spam & fake profiles in social networks by using topological deviations." The human race's Journal 1(1): 26–39. Fritsch & F. Günther (2010). "Neural net: Training of neural networks." R 2(1) The journal: 30-38
[2] "Preprocessing Methods for Text Mining," by Vairaprakash Gurusamy and Dr. S. Kannan, posted March 5, 2015.
[3] Recognizing Authentic Profiles on LinkedIn Kaushik Dutta and Shalinda Adikari, PACIS 2014 Proceedings, AISeL
[4] "Evil people's circles discovery in social media sites based on temporally co-occurrence," in Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz, eds., 2011 July International Conference on (ICCNIT), pp. 35–390.
[5] "Analyzing Facebook privacy settings: Client demands vs. reality," Proceedings of the 2011 ACM SIGCOMM meeting on Online measure event, ACM, pp. 61–70, Liu Y, Gummadi K, Krishnamurthy and B, and Mislove A.
[6] Muhammad, S., and Desmedt, Y. "Poster: initial safety analysis of Google." In: Transactions from the eighteenth ACM Symposium on Compute and Internet Privacy, ACM the year 2011, pp. 809–812.
[7] Yousef Abu-Nimeh, T. M. Chen, who is & D. Alzubi, "Malicious and Spam Posts in Online Social Networks," IEEE Computer, which is the volume.44, no.9, pp. 23–

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com