Unmasking Deceptive Profile: A Supervised Approach To Spotting Fake Identities On Social Networks

B.Raja kumar chittoor[1], V Aashritha[2], P Rahul Kumar[2], T Shivaji Naidu[2], B Balu[2], K Sathwick[2]

[1] Assistant Professor, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India
[2] Research Scholar, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India

ABSTRACT

In present times, social media plays a key role in every individual life. Everyday majority of the people are spending their time on social media platforms. The number of accounts in these social networking sites has dramatically increasing day-by-day and many of the users are interacting with others irrespective of their time and location. These social media sites have both pros and cons and provide security problems to us also for our information. To scrutinize, who are giving threats in these networking sites we need to organize these social networking accounts into genuine accounts and fake accounts. Traditionally, we are having different classification methods to point out the fake accounts on social media. But we must increase the accuracy rate in identifying fake accounts on these sites. In our project we are going with Machine Learning technologies and Natural Language processing (NLP) to increase the accuracy rate of detecting the fake accounts. We opted for Support Vector Machine algorithm.

Keyword: - *Social Media, Fake, Accounts, ML, 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 Facebook 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. When making use of Social network's (SN's), one of a kind men and women share one-of-a-kind quantities of their private understanding. Having our individual know-how entirely or in part uncovered to the general public, makes us excellent targets for unique types of assaults, the worst of which could be identification theft. Identity theft happens when any individual uses character's expertise for a private attain or purpose. During the earlier years, online identification theft has been a primary problem considering it affected millions of people's worldwide. Victims of identification theft may suffer unique types of penalties; for illustration, they would lose time/cash, get dispatched to reformatory, get their public image ruined, or have their relationships with associates and loved ones damaged. At present, the vast majority of SN's does no longer verifies ordinary users‟ debts and has very susceptible privateness and safety policies. In fact, most SN's applications default their settings to minimal privateness; and consequently, SN's became a best platform for fraud and abuse. Social Networking offerings have facilitated identity theft and Impersonation attacks for serious as good as naive attackers. To make things worse, users are required to furnish correct understanding to set up an account in Social Networking web sites. Easy monitoring of what customers share on-line would lead to catastrophic losses, let alone, if such bills had been hacked. 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

2. LITERATURE SURVEY

Today's social networks are plagued by numerous types of malicious profiles, ranging from bots to sexual predators. We present a novel method for the detection of these malicious profiles by only using the social network's own topological features. The algorithm has been evaluated on several social networks and was found to be effective in detecting several types of malicious profiles. We believe this method is an important step towards making social networks less vulnerable to spammers, socialbots and sexual predators. [1]

Online social networks have witnessed massive increase from the point of view of users during last decade. However, it is also becoming center of attraction for spammers. It is a complex problem to trace spammers on a large scale. Since spammers communicate covertly so by analyzing simple graph of social network, they cannot be identified. In order to find the circle of people involved in the malicious messaging, we associate people on the basis of their spatio-temporal co-occurrence i.e. people frequently communicating with each other. In this paper, we associate people on the basis of their spatio-temporal co-occurrence and find the users involved in malicious communications.[2]

The sharing of personal data has emerged as a popular activity over online social networking sites like Facebook. As a result, the issue of online social network privacy has received significant attention in both the research literature and the mainstream media. Our . In this paper, we focus on measuring the disparity between the desired and actual privacy settings, quantifying the magnitude of the problem of managing privacy. We deploy a survey, implemented as a Facebook application, to 200 Facebook users recruited via Amazon Mechanical Turk. We find that 36% of content remains shared with the default privacy settings. We also find that, overall, privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected. We find that these have significant correlation with the social network, suggesting that information from the social network may be helpful in implementing new tools for managing privacy. [3]

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. The attackers have vast resources at their disposal. As of March 2011, this is 25B checks per day, reaching 650K per second at peak. The system also generates signals for use as feedback in classifiers and other components. We believe this system has contributed to making Facebook the safest place on the Internet for people and their information. This paper outlines the design of the Facebook Immune System, the challenges we have faced and overcome, and the challenges we continue to face [4]

This paper examines the politics behind algorithmic ordering in social media, focusing on the advertising logic behind them. This is explored through a practice I call rhythmedia – the way media companies render people, objects and their relations as rhythms and order them for economic purposes. This anti-spam algorithm shows that it is important for Facebook to understand people as rhythms and assemble a dynamic database from their mediated experiences, to convince advertisers that they know when and where people do things. People's rhythms become a product that advertisers pay and bid for through Ad Auction to intervene in specific moments and shape people's experience. Thus, the company can shape, manage, and filter specific rhythms to order sociality that brings more value.[5]

3. METHODOLOGY

3.1EXISTING SYSTEM

In an existing system for fake profile identification in social networks using machine learning (ML) and natural language processing (NLP) Collect data from social networks, including profile information, post content, and interaction patterns. Use NLP techniques to extract features from the text, such as sentiment analysis, word frequency, and syntactic analysis. Analyze the network structure, including the connections between users and the behavior of fake profiles compared to genuine ones.

Train ML models, such as logistic regression, decision trees, or deep learning models, on the extracted features to classify profiles as fake or genuine. Validate the models using labeled data or cross-validation to ensure their accuracy and generalization ability. Deploy the trained models to automatically detect fake profiles in real-time or in batch processing. Incorporate feedback from users or moderators to continuously improve the models and adapt to new types of fake profiles. Provide reports on the identified fake profiles, including their characteristics and the reasons for their classification.

3.1.1DISADVANTAGES OF EXISTING SYSTEM

- Limited Accuracy
- Complexity and Scalability
- Over Fitting

3.2 PROPOSED METHODOLOGY

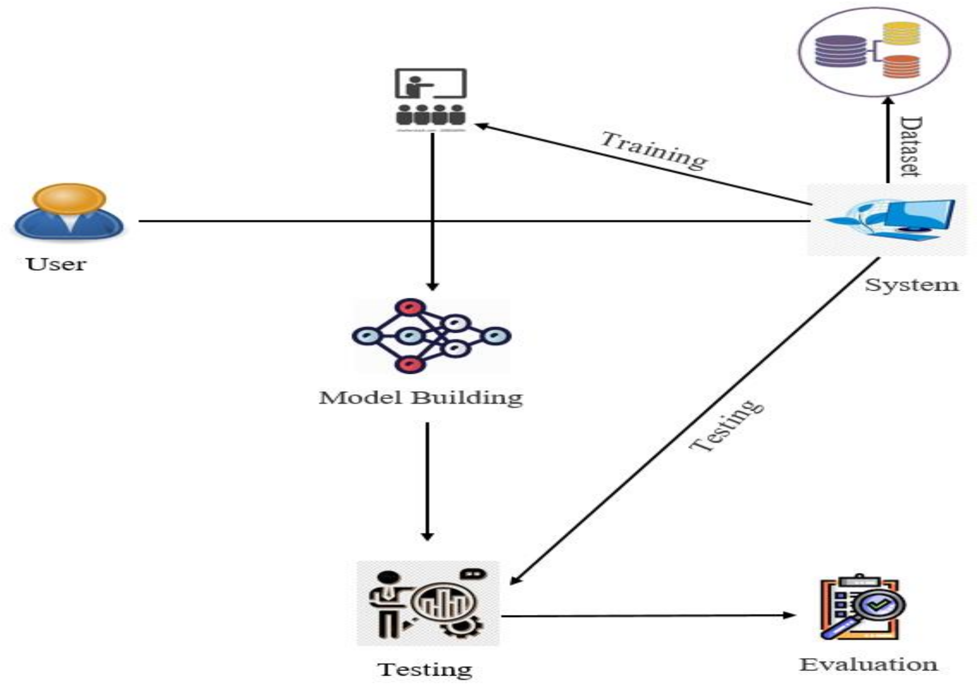
A proposed methodology for fake profile identification in social networks using machine learning (ML) and natural language processing (NLP) Collect data from social networks, including profile information, post content, and interaction patterns. This data will be used to train the ML models. Use NLP techniques to extract features from the text, such as sentiment analysis, word frequency, and syntactic analysis. These features will help differentiate between fake and genuine profiles. Analyze the network structure, including the connections between users and the behavior of fake profiles compared to genuine ones. This can help identify suspicious patterns of interaction. Clean and preprocess the data to remove noise, handle missing values, and standardize the format for input into the ML models. Train ML models, such as logistic regression, decision trees, or deep learning models, on the extracted features to classify profiles as fake or genuine. Use labeled data for training, where fake profiles are labeled as such. Validate the models using labeled data or cross-validation to ensure their accuracy and generalization ability. This step helps to identify and address any issues with the models. Deploy the trained models to automatically detect fake profiles in real-time or in batch processing. This step involves integrating the models into the social network platform's backend infrastructure

4. SYSTEM DESIGN

It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently.

.

4.1 SYSTEM ARCHITECTURE



4.2 MODULES

In this proposed system, there are Three modules. They are:

- Service Provider
- Remote user
- Dataset Administrator

4.2.1.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

4.2.2.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.

4.2.3.DATA ADMINISTRATOR

In this module, the functionalities are as : Process and train datasets

5. RESULTS AND PERFORMANCE

EXECUTION PROCEDURE

The Execution procedure is as follows:

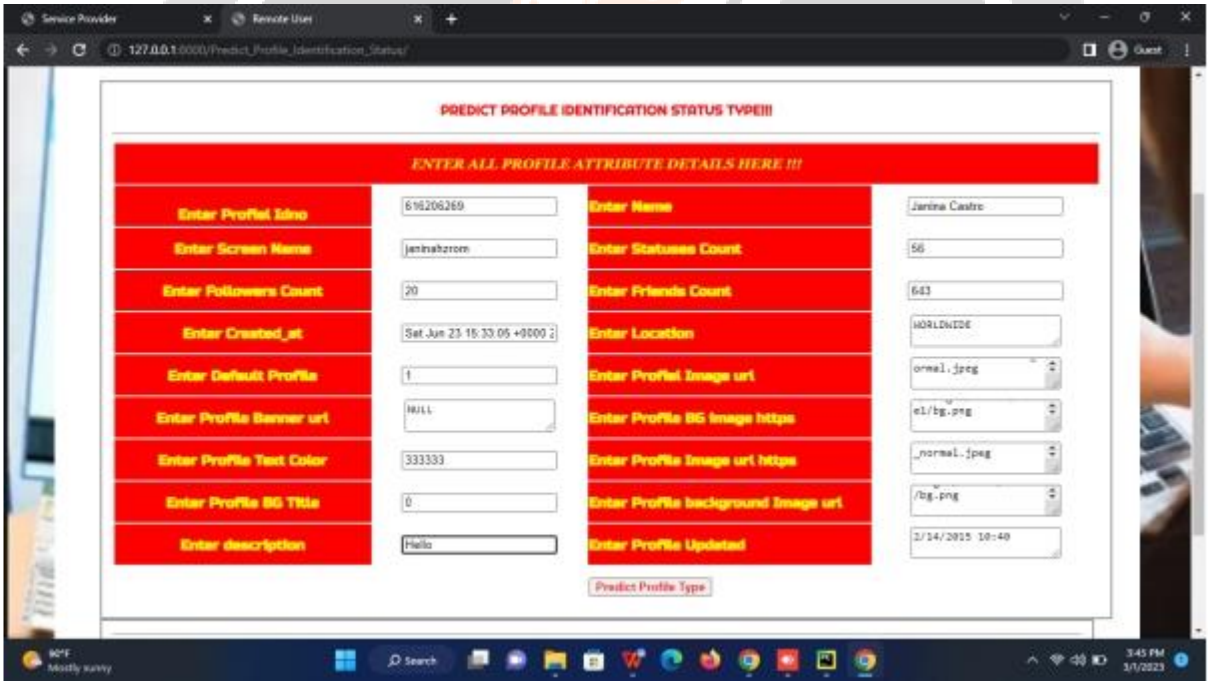
1. In this research work with data with attributes are observable and then all of them are floating data. And there's a decision class/class variable. This data was collected from Kaggle machine learning repository.

2. In this research 70% data use for train model and 30% data use for testing purpose.

3. SVM is used as Classifier .

4. In the classification report we were able to find out the desired result

5. In this analysis the result depends on some part of this research. However, which algorithm gives the best true positive, false positive, true negative, and false negative are the best algorithms in this analysis.



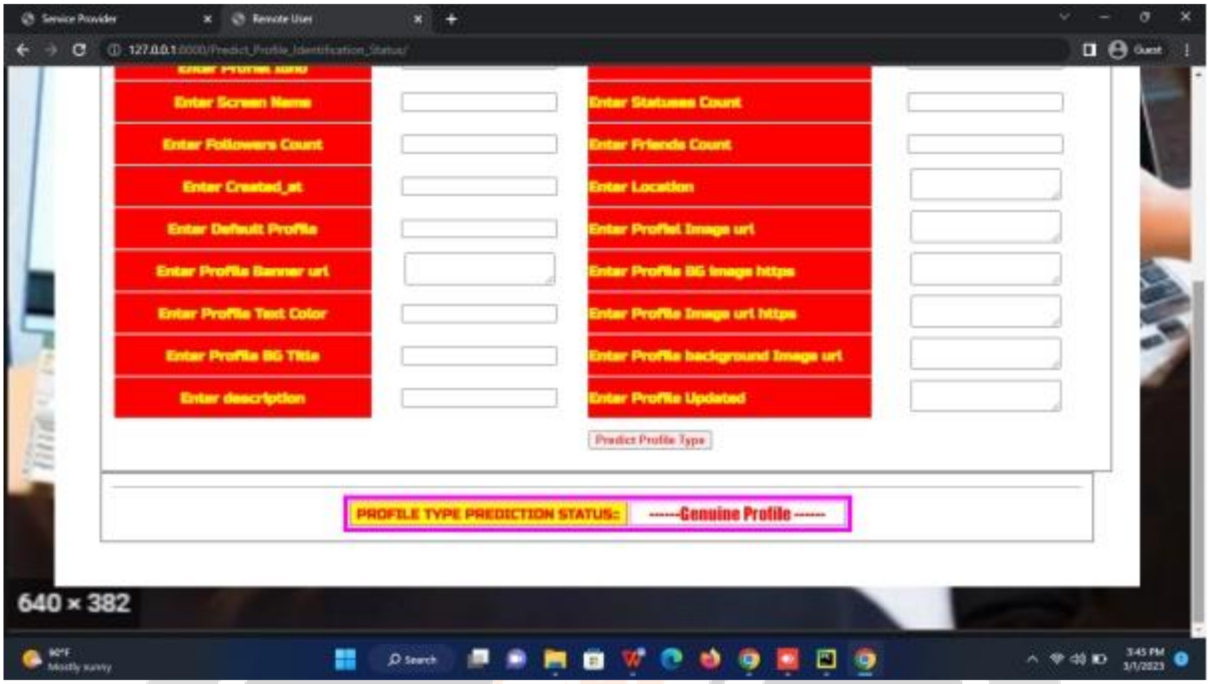
PREDICT PROFILE IDENTIFICATION STATUS TYPE!!!

ENTER ALL PROFILE ATTRIBUTE DETAILS HERE !!!

Enter Profiel Idno	616206269	Enter Name	Janina Castro
Enter Screen Name	janinahzrom	Enter Statuses Count	56
Enter Followers Count	20	Enter Friends Count	643
Enter Created_at	Sat Jun 23 15:33:05 +0000 2	Enter Location	WORLDWIDE
Enter Default Profile	1	Enter Profiel Image url	ormal.jpeg
Enter Profile Banner url	NULL	Enter Profile BG Image https	el/bg.png
Enter Profile Text Color	333333	Enter Profile Image url https	_normal.jpeg
Enter Profile BG Title	0	Enter Profile background Image url	/bg.png
Enter description	Hello	Enter Profile Updated	2/14/2015 10:40

Predict Profile Type

Fig . Enter Profile Attribute Values



Enter Screen Name | Enter Statuses Count
Enter Followers Count | Enter Friends Count
Enter Created_at | Enter Location
Enter Default Profile | Enter Profiel Image url
Enter Profile Banner url | Enter Profile BG Image https
Enter Profile Text Color | Enter Profile Image url https
Enter Profile BG Title | Enter Profile background Image url
Enter description | Enter Profile Updated

Predict Profile Type

PROFILE TYPE PREDICTION STATUS:: ------Genuine Profile ------

Fig . Prediction Status

6. CONCLUSION

In this project, 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 project, we took the Data set to identify the fake profiles. The NLP pre-processing techniques are used to analyze 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 project.

7. REFERENCE

[1] 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).

[2] Dr. S. Kannan, Vairaprakash Gurusamy, “Preprocessing Techniques for Text Mining”, 05 March 2015.

[3] ShalindaAdikari and Kaushik Dutta, Identifying Fake Profiles in LinkedIn, PACIS 2014 Proceedings, AISeL

[4] 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.

[5] Liu Y, Gummadi K, Krishnamurthy B, Mislove A,” Analyzing Facebook privacy settings: User expectations vs. reality”, in: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,ACM,pp.61–70.

[6] Mahmood S, Desmedt Y,” Poster: preliminary analysis of google?’s privacy. In: Proceedings of the 18th ACM conference on computer and communications security”, ACM 2011, pp.809–812.

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