IJASEM INTERNATIONAL JOURNAL OF APPLIED
SCIENCE ENGINEERING AND MANAGEMENT

DETECTING FAKE PROFILES IN SOCIAL NETWORKS USING MACHINE LEARNING AND NATURAL LANGUAGE PROCESSING

[1]LAKKIREDDY PRIYANKA, [2]GREESHMA PEDDAPELLI

[1]Assistant Professor,[2]Student

Department of CSE

Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Most individuals use social networking sites in their daily lives these days. On social networking sites, a number of individuals create accounts every day and engage with others regardless of their time and place. Social media platforms not only provide benefits to its users, but they also raise security concerns for their data. We must categorise user profiles on social networks in order to analyse who is promoting dangers there. We can distinguish between real and phoney social network accounts based on categorisation. Traditionally, there have been a variety of categorisation techniques used to identify phoney social network accounts. However, we must raise the accuracy rate of social network phoney profile detection. In order to increase the accuracy rate of the false profile identification, we propose machine learning and natural language processing (NLP) approaches in this research. The Naïve Bayes method and Support Vector Machine (SVM) may be used.

1. INTRODUCTION

Nowadays, social networking has become a well-known online pastime, drawing hundreds of thousands of users who log on for billions of minutes each year. The range of online social network (OSN) services includes social interaction-focused platforms like Facebook and MySpace, comprehension-focused platforms like Twitter and Google Buzz, and social interaction features integrated into current systems like flicker. On the other hand, strengthening security issues and safeguarding OSN privacy continue to be recognised as a primary bottleneck and purpose.

One of a kind men and women communicate one-of-a-kind volumes of their private knowledge via social networks (SNs). Because our personal knowledge is either fully or partially disclosed to the public, we are prime candidates for some kinds of attacks, the worst of which may be identity theft. Identity theft occurs when someone appropriates a character's knowledge for their own gain or agenda. In previous times, millions of individuals worldwide were impacted by online identity theft, making it a major issue. Identity theft victims may face special punishments, such as losing money or time, being sent to reformatory, having their reputation harmed, or experiencing problems in their relationships with friends and family. Nowadays, the great majority of SNs have extremely shaky privacy and security standards and do longer verify the debts of regular customers. In actuality, the majority of SN apps have low privacy settings by

default, which has made SNs an ideal venue for fraud and abuse. Social networking platforms have made identity theft and impersonation attempts easier for both skilled and unsuspecting attackers. To exacerbate matters, users must provide accurate information in order to create an account on social networking websites. Simple oversight of what users post online might result in disastrous losses, never mind if these bills were compromised.

Online networks will also include static or dynamic profile data. Static knowledge refers to the information that may be provided by the user during the profile construction process, while dynamic knowledge refers to the fine print that is narrated by the network system. A person's realtime behaviours and location within the network are examples of dynamic knowledge, while demographic information and interests about the individual make up static knowledge. Most of the research being done now relies on both static and dynamic data. This isn't applicable to many social networks, however, since only a small percentage of static profiles are seen and dynamic profiles are often hidden from the human network. A unique researcher has presented a number of methods to identify fraudulent information and false identities in online social networks. Every procedure has strengths and drawbacks of its own.

social networking issues, including those related to privacy, cyberbullying, abuse, trolling, and many more. are several occasions when fraudulent accounts on social networking platforms are used. Unspecific profiles are known as false profiles. These are the fictitious profiles of men and women. False Facebook identities often engage in harmful and undesired behaviour, which disrupts users of social media networks. False profiles are made by people for social engineering, online impersonation to harm a person, and campaigning and supporting a persona or group of people. Facebook has its own security system in place to protect user credentials from phishing, spam, and other threats. It's also often referred to as the Facebook Immune System (FIS).

The FIS hasn't been prepared to see more and more phoney Facebook accounts made by users.

2. LITERATURE SURVEY

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). IEEE Conference on Machine Learning and IOT,

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. They can even launch threats like phishing, stalking, spamming etc. Fake profile is the creation of profile in the name of a person or a company which does not really exist in

social media, to carry out malicious activities. In this paper, a detection method has been proposed which can detect Fake and Clone profiles in Twitter. Fake profiles are detected based on number of abuse reports, number of comments per day and number of rejected friend requests, a person who are using fake account. For Profile Cloning detection two Machine Learning algorithms are used. One using Random forest Classification algorithm for classifying the data and Support Vector Machine algorithm. This project has worked with other ML algorithms, those training and testing results are included in this paper.

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

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. The user's need for information is represented by a query or profile, and contains one or more search terms, plus some additional information such as weight of the words. Hence, the retrieval decision is made by comparing the terms of the query with the index terms (important words or phrases) appearing in the document itself. The decision may be binary (retrieve/reject), or it may involve estimating the degree of relevance that the document has to query. Unfortunately, the words that appear in documents and in queries often have many structural variants. So before the information retrieval from the documents, the data preprocessing techniques are applied on the target data set to reduce the size of the data set which will increase the effectiveness of IR System The objective of this study is to analyze the issues of preprocessing methods such as Tokenization, Stop word removal and Stemming for the text documents Keywords: Text Mining, NLP, IR, Stemming.

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

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. As this value increases, so does the temptation to misuse the network for unethical purposes. Fake profiles have an adverse effect on the trustworthiness of the network as a whole, and can represent significant costs in time and effort in building a connection based on fake information. Unfortunately, fake profiles are difficult to identify. Approaches have been proposed for some social networks; however, these generally rely on data that are not publicly available for LinkedIn profiles. In this research, we identify the minimal set of profile data necessary for identifying fake profiles in LinkedIn, and propose an appropriate data

mining approach for fake profile identification. We demonstrate that, even with limited profile data, our approach can identify fake profiles with 87% accuracy and 94% True Negative Rate, which is comparable to the results obtained based on larger data sets and more expansive profile information. Further, when compared to approaches using similar amounts and types of data, our method provides an improvement of approximately 14% accuracy.

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.

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. The informal organization an urgent piece of our life is tormented by online pantomime and phony records. Fake profiles are for the most part utilized by the gatecrashers to complete malevolent exercises, for example, hurting individual, data fraud, and security interruption in online social network (OSN). Hence, recognizing a record is certified or counterfeit is one of the basic issues in OSN. Right now, propose a model that could be utilized to group a record as phony or certified. This model uses random forest method as an arrangement strategy and can

process an enormous dataset of records on the double, wiping out the need to assess each record physically. Our concern can be said to be a characterization or a bunching issue. As this is a programmed recognition strategy, it very well may be applied effectively by online interpersonal organizations which have a large number of profiles, whose profiles cannot be inspected physically.

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

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. They are well-funded, with full-time skilled labor, control over compromised and infected accounts, and access to global botnets. Protecting our users is a challenging adversarial learning problem with extreme scale and load requirements. Over the past several years we have built and deployed a coherent, scalable, and extensible real time system to protect our users and the social graph. This Immune System performs real time checks and classifications one very read and write action. As of March 2011, this is25B 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 as 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.

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.

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. In addition to providing users with advantages, social networking sites also present security concerns to them and their information to them. We need to classify the social network profiles of the users to figure out who is encouraging threats on social networks. From the classification, we can figure out which profiles are genuine and which are fake. As far as detecting fake profiles on social networks is concerned, we currently have different classification methods. However, we must improve the accuracy of detecting fake profiles in social networks. We propose the use of a machine learning algorithm and Natural Language Processing (NLP) technique in this paper so as to increase the detection rate of fake profiles. This can be achieved using Support Vector Machines (SVM) and Naïve Bayes algorithms.

3. **EXISTING SYSTEM**

Chai et al awarded on this paper is a proof-of inspiration gain knowledge of. Even though the prototype approach has employed most effective normal systems in normal language processing and human-pc interplay, the results realized from the user trying out are significant. By using comparing this simple prototype approach with a wholly deployed menu procedure, they've discovered that users, principally beginner users, strongly pick the common language dialog-based approach. They have additionally learned that in an ecommerce environment sophistication in dialog administration is most important than the potential to manage complex typical language sentences.

In addition, to provide effortless access to knowledge on ecommerce web sites, natural language dialog-based navigation and menu-pushed
navigation should be intelligently combined to meet person's one-of-a-kind wants. Not too long ago, they have got accomplished development of a new iteration of the approach that includes enormous enhancements in language processing, dialog administration and information management. They believed that average language informal interfaces present powerful personalized alternatives to conventional menupushed or search-based interfaces to web sites.

LinkedIn is greatly preferred through the folks who're in the authentic occupations. With the speedy development of social networks, persons are likely to misuse them

for unethical and illegal conducts. Creation of a false profile turns into such adversary outcomes which is intricate to identify without apt research. The current solutions which were virtually developed and theorized to resolve this contention, mainly viewed the traits and the social network ties of the person's social profile. However, in relation to LinkedIn such behavioral observations are tremendously restrictive in publicly to be had profile data for the customers by the privateness insurance policies. The limited publicly available profile data of LinkedIn makes it ineligible in making use of the existing tactics in fake profile identification. For that reason, there is to conduct distinctive study on deciding on systems for fake profile identification in LinkedIn. Shalinda Adikari and Kaushik Dutta researched and identified the minimal set of profile data that are crucial for picking out false profiles in LinkedIn and labeled the appropriate knowledge mining procedure for such project.

Z. Halim et al. Proposed spatio-temporal mining on social network to determine circle of customers concerned in malicious events with the support of latent semantic analysis. Then compare the results comprised of spatio temporal co incidence with that of original organization/ties with in social network, which could be very encouraging as the organization generated by spatio-temporal co-prevalence and actual one are very nearly each other. Once they set the worth of threshold to right level, we develop the number of nodes i.e. Actor so that they are able to get higher photo. Total, scan

indicate that Latent Semantic Indexing participate in very good for picking out malicious contents, if the feature set is competently chosen. One obvious quandary of this technique is how users pick their function set and the way rich it's. If the characteristic set is very small then most of the malicious content material will not be traced. However, the bigger person function set, better the performance won.

Disadvantages

- The system is not implemented Learning Algorithms like svm, Naive Bayes.
- The system is not implemented any the problems involving social networking like privacy, online bullying, misuse, and trolling and many others.

4. **PROPOSED SYSTEM**

• On this paper we presented a machine learning & natural language processing system to observe the false profiles in online social networks. Moreover, we are adding the SVM classifier and naïve bayes algorithm to increase the detection accuracy rate of the fake profiles.

An SVM classifies information by means of finding the exceptional hyperplane that separates all information facets of 1 type from those of the other classification. The best hyperplane for an SVM method that the one with the biggest line between the two classes. An SVM classifies data through discovering the exceptional hyperplane that separates all knowledge facets of one category from those of the other class. The

help vectors are the info aspects which are closest to the keeping apart hyperplane.

Naive Bayes algorithm is the algorithm that learns the chance of an object with designated features belonging to a unique crew/category. In brief, it's a probabilistic classifier. The Naive Bayes algorithm is called "naive" on account that it makes the belief that the occurrence of a distinct feature is independent of the prevalence of other aspects. For illustration, if we're looking to determine false profiles based on its time, date of publication or posts, language and geoposition. Even if these points depend upon each and every different or on the presence of the other facets, all of these properties in my view contribute to the probability that the false profile.

Advantages

- In the proposed system, 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.
- In the proposed system, Social Networking offerings have facilitated identity theft and Impersonation attacks for serious as good as naïve attackers.

ARCHITECTURE

Architecture Diagram
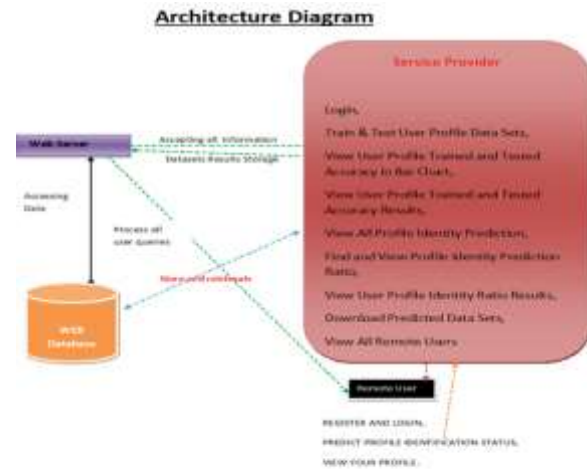
5. ALGORITHIM
Naïve Bayes

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .

Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).

While the Naive Bayes classifier is widely used in the research world, it is not

widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they does not understand the interest of such a technique.

Thus, we introduce in a new presentation of the results of the learning process. The classifier is easier to understand, and its deployment is also made easier. In the first part of this tutorial, we present some theoretical aspects of the naive bayes classifier. Then, we implement the approach on a dataset with Tanagra. We compare the obtained results (the parameters of the model) to those obtained with other linear approaches such as the logistic regression, the linear discriminant analysis and the linear SVM. We note that the results are highly consistent. This largely explains the good performance of the method in comparison to others.

SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an *independent and identically distributed* (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point x and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. From a geometric perspective, learning a classifier is equivalent to finding the equation for a multidimensional surface that best separates the different classes in the feature space.

SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to *genetic algorithms* (*GAs*) or *perceptrons*, both of which are widely used for classification in machine learning. For perceptrons, solutions are highly dependent on the initialization and termination criteria. For a specific kernel that transforms the data from the input space to the feature space, training returns uniquely defined SVM model parameters for a given training set, whereas the perceptron and GA classifier models are different each time training is initialized. The aim of GAs and perceptrons is only to minimize error during training, which will translate into several hyperplanes' meeting this requirement.

6. IMPLEMENTATION

Modules

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

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.

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.

7. **SCREEN SHOTS**

8. CONCLUSION

In this research, we combined natural language processing methods with machine learning algorithms. These methods make it simple to identify fraudulent personas on social media platforms. In order to identify the phoney profiles, we used the Facebook Data Set in this research. The dataset is analysed using NLP pre-processing methods, and the profiles are classified using machine learning algorithms like SVM and Naïve Bayes. In this research, the detection accuracy rate is increased using these learning techniques.

REFERENCES

[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). "neuralnet: Training of neural networks." The R Journal 2(1): 30-38

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

[3] Shalinda Adikari 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

[8] 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.

[9] 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

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