CLASSIFICATION OF FAKE AND CLONE PROFILES USING SIMILARITY MEASURING IN TWITTER

G. Praveen Kumar Associate Professor, Department of CSE, Narayana Engineering College Gudur, SPSR Nellore, AP
P. Tejaswini,, **P. Srilakshmi** , **S. Priyanka**, UG student, Department of CSE, Narayana Engineering College Gudur (Autonomous), SPSR Nellore, AP

ABSTRACT
Over the years major social networks such as Facebook or Twitter have admitted that on their networks there are strong and duplicate accounting accounts. Through these accounts, their creators will spread false information, support, or attack the idea, product, or qualification person, influencing network users once they have decided. They exploit trusting relationships between users in order to capture their hateful intentions, for example, generating hateful links between posts / tweets. To investigate Twitter accounts, we tend to create the use of a variety of new options, that rating unit is simpler and stronger than the options used (e.g., type of users / followers / followers, etc.). We often test a set of proposed options using advanced machine configuration algorithms, particularly Support Vector Machine (SVM) and Neural Networks (NN). Their recommendation is semiconductor on various issues such as the creation of faux accounts and the spread of information hypocrisy in addition to creating malicious content. Such things can damage real-world events that square steps related to people, business organizations, study camps, etc. With this paper, we tend to give our system a build with the aim of identifying fraudulent users of the Twitter social network.
Keywords - Fraud Detection, Separation, Online Social Network.

INTRODUCTION
People use Twitter to share their feelings, news, events and post their daily activities like taking, drinking, traveling like that. Therefore, malicious users will check everyone's activities from their timeline and twitter becomes a regional site for hateful hackers[7]. These malicious unit-level users generate fake accounts and expose many false stories, false links, and images. Most of the highway users' details do not seem to remember those fake accounts; they accepted requests and suffered within the framework[8]. Therefore, finding false accounts on twitter is mandatory for everyone who uses them.

Over the past few years, social networking sites (e.g., Facebook, Twitter, and Instagram) have become one of the leading platforms for internet surfers to talk to friends, express ideas, and have conversations about events and appreciate memories. Twitter, a small blogging service launched in 2006, is one of the most popular social networking sites, where users send about 140 text messages, called "tweets[3]". Twitter has 330 million active users who send 500 million tweets each day. This huge rumor attracts the eye of spam users who use twitter for hostile purposes, including spreading hateful URLs within tweets, spreading rumors, sending unsolicited messages to other users.

Social Networks (OSNs) have also attracted the interest of mining investigators and analyzed their vast amount of data, assessing, and studying the behavior of users alike to find their pre-existing jobs. best understanding that predicts customer status.

LITERATURE SURVEY
In paper [1], a review of the number of mining routes that typically find slopes. An unusual guide is being developed in the investigation of informal public identification programs that are properly directed at initiation, formation, and conceptualization. All of these combinations include many of the processes discussed in the paper. This paper is closed with a variety of future topics and areas of research that can be addressed and worked on.

In the paper , it is intended that the Twitter trend is protected from the use of hateful users. We collect 69 million tweets from 5 million records. We use collected tweets, first directing information investigations, and finding evidence of Twitter pattern control. At that point, we read at the title level

and discover the key factors that can determine whether the issue you need is starting to decline because of its spread, inclusion, transmission, potential inclusion, or thunderstorm. What we find is that apart from the transmission, all of the above factors are firmly identified in the trend. Finally, we continue our research on trend control from the total number of sold and false records and discuss counter-measures.

In paper [3], social media users build trust relationships with subsequent accounts. This conviction can create a combination of reasons. For example, a client may know the owner of a credible record face to face or the record may be used even by a part that is considered trustworthy, for example, a general news office. Alternatively, if the ability above the record consists of digital violation controls, he can hope without much sacrifice this trust to make it his own. It shows how we can use similar methods to compare victims of certain high-profile accounts. High profile accounts often have a single trademark that produces a strong site that reflects reliable behavior after your time. We show that our framework, if it had been submitted, would have chosen to separate and oppose the real attacks on well-known organizations and media trials. Moreover, our framework, as opposed to the well-known media, would not have fallen into the formal trade that filled the US café network for reasons of attention.

In paper [4], they proposed a reliability analysis system to test the information officer on Twitter to prevent the spread of false or harmful information. The proposed framework consists of 4 integrated components: a component based on respect, a suitable classification vehicle, a user experience component, and a feature-level algorithm.

In Paper [5], they forwarded the research discussed in this paper and applied these same engineering features to a host of fake personal accounts in the hope of furthering the successful acquisition of man-made fake identity in SMPs. Various thanks to the thought-provoking handle on Twitter: they look to show how the word calling trend influences the choice of micro blog creators. During the survey, the creator indicated the link between the word calling the trend and therefore the number of followers. As such, it is difficult to determine the client's performance in these programs and to evaluate his or her posts. As online corporations have evolved to become increasingly useful in disseminating data to a wider audience, in the face of the aforementioned difficulties in determining customer legitimacy in OSNs requires the development of best practices for client rating and credibility.

They investigated the behavior of spam users on Twitter with the aim of improving existing spam detection methods. To find Twitter spam, they need the use of several new features, simpler and more powerful than existing features.

Based on the expected results from machine learning models[6], the features available and machine learning models that typically obtain fraudulent accounts are not sufficient to obtain fraudulent social media accounts.

We did an analysis of the smuggling concept used by Twitter spam. They have noticed that Twitter spammers often change their performance to avoid spam detection strategies, in order to suggest designing a replacement feature that could improve spam and make it harder for them to avoid it. That they have incorporated their new features into the machine learning algorithm and compared the use with other existing methods.

PROPOSED SYSTEM

In this paper, our aim is to use machine learning class algorithms to select account authenticity as real or false, those algorithms were vector support, neural Network, and our newly developed algorithm, SVM-NN. The proposed algorithm (SVM-NN) uses a small number of features, while still having the ability to fine-tune the accounts of our training database.

Figure 1 shows the proposed system configuration for non-Twitter account acquisition. Input traffic data is used for twitter datasets with specific features. The training database consists of data processing that involves two steps: the output feature and the machine learning method. After use, the two are sorted by an override model, which was used to select several features. Then install the

Support Vector machine to separate our data and use the neural network to train our model. After using the algorithms, it predicts whether our model account is inaccurate or not.

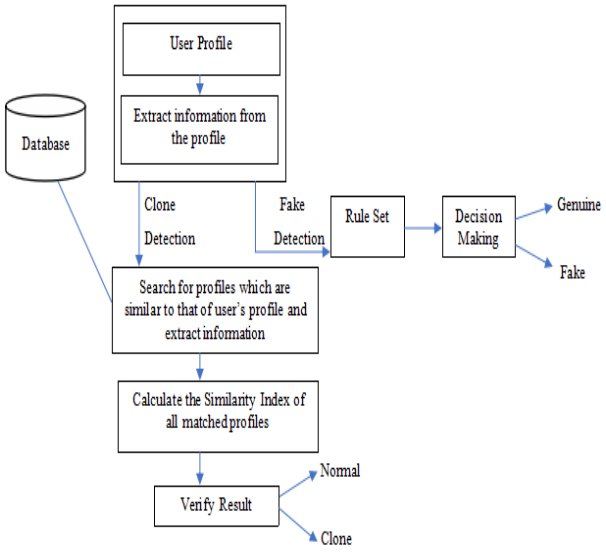

Fig. 1: Proposed System

A. Fake Profile Detection

This module is employed to detect fake Twitter profiles. Here fake profiles are detected supported rules that effectively distinguish fake profiles from genuine ones. A number of the principles that are accustomed detect fake profiles are - usually fake profiles do not have profile name or image. They are doing not include any description about the account. The geo-enabled field are going to be false as they are doing not want to reveal their location in tweets. They typically make substantial number of tweets or sometimes the profiles wouldn't have made any tweets etc. The principles are applied on the profile, for every matching rule, a counter is incremented, if the counter value is bigger than pre-defined threshold, then the profile is termed as fake

B. Clone Profile Detection using Similarity Measures

This module detects clones supported Attribute and Network similarity. User profile is taken as input. User identifying information are extracted from the profile. Profiles which are having attributes matching thereto that of user's profile are searched. Similarity index is calculated and if the similarity index is bigger than the edge, then the profile is termed as clone, else normal [1].

i) Attribute Similarity

Attribute similarity is calculated supported the similarity of attribute values between the profiles. The attributes that are considered for similarity measurement are Name, Screenname, Language, Location and zone. Two similarity measures are wont to measure the similarity between the attributes – Cosine similarity and Levenshtein distance. Cosine similarity is employed to seek out similarity between words and Levenshtein distance is employed to search out similarity between two sequences.

Two vectors have a cosine similarity of 1 if they're with the same orientation; have a similarity of 0 if they're at 90° and -1 if they are diametrically opposed [9][10]. Levenshtein distance may be a similarity measuring metric to seek out similarity between two sequences.

If two sequences are given, the Levenshtein distance between them is that the minimum number of inserts, delete or substitution operations required to alter one sequence into another.

ii) Network Similarity

Network similarity is calculated supported network relationships [1]. Here, Followers_ids attribute is employed to seek out the network similarity between the profiles. Followers_ids give the list of accounts which follows the user. The clone profile always tries to attach to same set of users as that of legitimate owner to indicate that it's genuine one. So, by comparing the Followers_ids of two

profiles, we are able to find whether or not they are similar with relevance network relationships or not.

iii) Clone Profile Detection using C4.5 algorithm

In this module, C4.5 algorithm is employed to detect whether the given profile may be a clone or not. C4.5 could be a decision tree algorithm used for classification. It builds a choice tree supported given data. At each node of tree, the attribute that the majority effectively splits the sample sets into subsets is chosen. The splitting factors employed in C4.5 are information gain and entropy. The attribute with highest information gain is chosen to form decision so its re-curses over the partitioned sub-trees.

iv) Evaluation Metrics

To evaluate the performance of the system, various evaluation metrics are used supported following four standard indicators

- True Positive (TP): True positives are records that are correctly detected with expected vectors.
- True Negative (TN): True negatives are records correctly detected expected as Neutral.
- False Positive (FP): False positives are records that were detected by the system needless to say but are listed within the other vectors.
- False Negative (FN): False negatives are records not detected by the system.

The evaluation metrics considered are

1. Accuracy which supplies the ratio of number of correct results to the whole number of inputs
2. Precision which supplies the proportion of positive detection that was correct
3. Recall which provides the proportion of actual positives that was detected correctly
4. F1 Score which considers both precision and recall to compute the score. F1-score is given by harmonic mean of precision and recall. If F1-score is 1, then it's best value and worst is 0.

CONCLUSION

Fake and clone profiles have become a profoundly severe problem in online social networks. We hear some or the other threats caused by these profiles in everyday life. So, a detection method has been proposed which can find both fake and clone Twitter profiles. For fake detection, a set of rules were used which when applied can classify fake and genuine profiles. Clone detection was carried out using Similarity Measures and C4.5 algorithm and a comparison was made to check the performance. Clone detection using Similarity Measures worked better than C4.5 and was able to detect most of the clones which were fed into the system.

REFERENCES

[1] Sowmya P and Madhumita Chatterjee," Detection of Fake and Cloned Profiles in Online Social Networks", Proceedings 2019: Conference on Technologies for Future Cities (CTFC)

[2] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P.Markatos, "Detecting Social Network Profile Cloning", 2013

[3] Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile CloningDetection in Social Networks", 2014 European Network IntelligenceConference

[4] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, AngelloSpognardi, Maurizio Tesconi, "Fame for sale: Efficient detection of fakeTwitter followers", 2015 Elsevier's journal Decision Support Systems,Volume 80

[5] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set", World Academy of Science, Engineering and Technology, International Journal of Computer, and Information Engineering Vol:10, 2016

[6] Sucharita, V, Jyothi, S.,Rao,P.V Comparison of machine learning algorithms for classification of Penaeid prawn species 2016 Proceedings of the 10th INDIA.com 2016 ,pp.1610

[7] Kiruthiga. S, Kola Sujatha. P and Kannan. A, "Detecting CloningAttack in Social Networks Using Classification and ClusteringTechniques" 2014 International Conference on Recent Trends inInformation Technology

[8] Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, Ceyhun Akyol, "Twitterfake account detection", 2017 International Conference on ComputerScience and Engineering (UBMK)

[9] Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A.S, "Pythonbased Machine Learning for Profile Matching", International ResearchJournal of Engineering and Technology (IRJET), 2018

[10] Olga Peled, Michael Fire, Lior Rokach, Yuval Elovici, "Entity Matchingin Online Social Networks", 2013 International Conference on SocialComputing