RESEARCH ARTICLE OPEN ACCESS

IMPROVED AND DYNAMIC DISTANCE MEASURE ALGORITHMS TO DETECT FAKE AND CLONE SOCIAL NETWORKING ACCOUNTS

1.Dr K Jayarajan, 2.Muppaneni Yukthika, 3. Murari Bhargavi, 4.Musku Samskruthi

1(Professor and Head, Information Technology, Malla Reddy Engineering College for Women, Hyderabad-500100
Email: bvsr79@gmail.com)
2, 3, 4 (Student, Information Technology, Malla Reddy Engineering College for Women, Hyderabad-500100.
Email: mahalaxmiracha19@gmail.com)

Abstract:

Online Social Network (OSN) is a network hub where people with similar interests or real world relationships interact. As the popularity of OSN is increasing, the security and privacy issues related to it are also rising. 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.

I. INTRODUCTION

ONLINE Social Networks (OSN) like Face book, Twitter, LinkedIn, Instagram etc are used by billions of users all around the world to build network connections. The ease and accessibility of social networks have created a new era of networking. OSN users share a lot of information in the network like photos, videos, school name, college name, phone numbers, email address, home address, family relations, bank details, career details etc. This information if put into hands of attackers, the after effects are very severe.

Most of the OSN users are unaware of the security threats that exist in the social networks and easily fall prey to these attacks. The risks are more dangerous if the victims are children. In Profile Cloning attack, the profile information of existing users are stolen to create duplicate profiles and these profiles are misused for spoiling the identity of original profile owners. There are two types of Profile Cloning namely - Same Site and Cross Site Profile Cloning. If user credentials are taken from one Network to create a clone profile in same Network then it is called Same Site profile cloning.

In Cross Site profile cloning, attacker takes the user information from one Network to create a duplicate profile in other Network in which the user is not having any account. As the registration process in social networks have become very simple in order to attract more and more users, the creation of fake profiles are also increasing in an alarming rate. An attacker creates a fake profile in order to connect to a victim to cause malicious activities. And also to spread fake news and spam messages. The paper organized as below. Section II describes the literature survey. Section III explains the proposed methodology. Section IV discusses the results. At last, Section V concludes the paper with the conclusion.

II. LITERATURE REVIEW

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P Markatos [2] have proposed a prototype to check whether the users have become victim to cloning attack or not. Information is extracted from user profile and a search is made in OSN to find profiles which match to that of user profile and a similarity score is calculated based on commonality of attribute values. If the similarity score is above the threshold value then the particular profile is termed as clone.

Brodka, Mateusz Sobas and Henric Johnson in their paper [3] have proposed two novel methods for detecting cloned profiles. The first method is based on the similarity of attribute values from original and cloned profiles and the second method is based on the network relationships. A person who doubts that his profile has been cloned will be chosen as a victim. Then treating name as primary key, a search is made for profiles with the same name as that of victim, using query search. Potential clone (Pc) and the Victim profile (Pv) are compared and similarity S is calculated. If S(Pc, Pv) > Threshold, then profile is suspected to be a clone. In the verification step, the user does it manually as he knows which is his original profile and which one is a duplicate.

III. EXISTING SYSTEM

Today, Fake and Clone profiles have become a very serious threat in social networks. So, a detection method is very much necessary to find these frauds who use people’s faith to gather private information and create duplicate profiles. Many authors have worked in this area and have proposed methods to identify these type of profiles in social networks. Some of these methods are discussed below.

Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny [5], have proposed a classification method for detecting fake accounts on Twitter. They have collected some effective features for the detection process from different research and have filtered and weighted them in first stage. Various experiments are conducted to get minimum set of attributes which gives accurate results. From 22 attributes, only seven attributes were selected which can effectively detect fake accounts and have applied these factors on classification techniques. A comparison of the classification techniques based on results are made and the one which provides most accurate result is selected.

DISADVANTAGES

- In the existing work, the system doesn't calculate fake accounts due to lack of Attribute similarity finding.
- This system less effective due to absence of Attribute similarity which is not calculated based on the similarity of attribute values between the profile.

IV. PROPOSED SYSTEM

Fake and clone profiles have become a very serious social threat. As information like phone number, email id, school or college name, company name, location etc are readily exposed in social networks, hackers can easily hack this information to create fake or clone profiles. They then try to cause various attacks like phishing, spamming, cyberbullying etc. They even try to defame the legitimate owner or the organisation. So, a detection method has been proposed which can detect both fake and clone profiles in order to make the social life of the users more secure. The architecture of proposed system is as shown in the proposed system.

A. Fake Profile Detection : This module is used to detect fake Twitter profiles. Here fake profiles are detected based on rules that effectively distinguish fake profiles from genuine ones. Some of the rules that are used to detect fake profiles are - usually fake profiles do not have profile name or image. They do not include any description about the account. The geo-enabled field will be false as they do not want to expose their location in tweets.

B. Clone Profile Detection using Similarity Measures : This module detects clones based on Attribute and Network similarity. User profile is taken as input. User identifying information are extracted from the profile. Profiles which are having attributes matching to that of user's profile are searched. Similarity index is calculated and if the similarity index is greater than the threshold, then the profile is termed as clone, else normal.

ADVANTAGES

- Accuracy which gives the ratio of number of correct results to the total number of inputs.
- Precision which gives the proportion of positive detection that was actually correct. Recall which gives the proportion of actual positives that was detected correctly.

MODULES

- Service Provider
- View and Authorize Users
- Remote User

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 View All Tweet Data Set Details, Search Tweet Data Set Details, View Fake Accounts, View All Remote Users, View Clone Account, View Account Type Ratio Details, View Tweet Score Results, View Fake and Clone Account Ratio Results.

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 ADD TWEET DATA SETS, SEARCH ON TWEET DATA SET DETAILS, and VIEW YOUR PROFILE.

V. RESULTS

A. Datasets Used

The datasets used in the experiment are collected from MIB projects. It consists of Genuine and Fake Twitter datasets. The Genuine accounts dataset contains accounts of people who came forward to be part of academic study for detecting fake accounts on Twitter and it is mostly a mixture of accounts of researchers, social experts and journalists from Italy, US and other European countries. The fake accounts were purchased from three different Twitter online markets namely fastfollowerz.com, intertwitter.com and twittertechnology.com.

B. Evaluation Metrics

In order to evaluate the performance of the system, various evaluation metrics are used based on 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 as expected but actually are listed in the other vectors.

• False Negative (FN): False negatives are records not detected by the system. The evaluation metrics considered are 1. Accuracy which gives the ratio of number of correct results to the total number of inputs 2. Precision which gives the proportion of positive detection that was actually correct 3. Recall which gives the proportion of actual positives that was detected correctly 4. F1 Score which takes into account 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 is best value and worst is 0.

VI. CONCLUSION

Fake and clone profiles have become a very serious 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.

VII.FUTURE WORK

For the future scope, a more complex algorithm for the skin detection can be implemented. The natural language processing techniques can be implemented to detect fake accounts more accurately. The new features will be certainly introduced by the Facebook, and these features can also be included while analyzing the fake accounts. In future researches, a new method will be presented; which can recognize the legitimate or fake account before any activity of the user in the network or at the time of registration.

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 Cloning Detection in Social Networks”, 2014 European Network Intelligence Conference.

[4] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angello Spognardi, Maurizio Tesconi, “Fame for sale: Efficient detection of fake Twitter 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] M.A.Devmane and N.K.Rana, “Detection and Prevention of Profile Cloning in Online Social Networks”, 2014 IEEE International Conference on Recent Advances and Innovations in Engineering.

[7] Kiruthiga. S, Kola Sujatha. P and Kannan. A, “Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques” 2014 International Conference on Recent Trends in Information Technology.

[8] Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, Ceyhun Akyol, “Twitter fake account detection”, 2017 International Conference on Computer Science and Engineering (UBMK).

[9] Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A.S, “Python based Machine Learning for Profile Matching”, International Research Journal of Engineering and Technology (IRJET), 2018.

[10] Olga Peled, Michael Fire, Lior Rokach, Yuval Elovici, “Entity Matching in Online Social Networks”, 2013 International Conference on Social Computing.

[11] Aditi Gupta and Rishabh Kaushal, “Towards Detecting Fake User Accounts in Facebook”, 2017 ISEA Asia Security and Privacy (ISEASP).

[12] Michael Fire, Roy Goldschmidt, Yuval Elovici, “Online Social Networks: Threats and Solutions”,

JOURNAL OF LATEX CLASS FILES, VOL. 11, NO. 4, DECEMBER 2012, IEEE Communications Surveys & Tutorials.

[13] Ashraf Khalil, Hassan Hajjdiab and Nabeel Al-Qirim, “Detecting Fake Followers in Twitter: A Machine Learning Approach” 2017 International Journal of Machine Learning and Computing.

[14] Mohammad Reza Khayyambashi and Fatemeh Salehi Rizi, “An approach for detecting profile cloning in online social networks” 2013 International Conference on e-Commerce in Developing Countries: with focus on e-Security.

[15] Mauro Conti, Radha Poovendran and Marco Secchiero, “FakeBook: Detecting Fake Profiles in On-line Social Networks”, 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.