Predicting Identity Clone Attacks in Online Social Networks

Using Machine Learning Techniques

[1]Anusha K.G, [2]Mahalakshmi, [3]Manasa J, [4]Siri S,[5]Chandru A.S

[5]Assistant Professor
[1,2,3,4,5]Department of Information Science and Engineering,
[1,2,3,4,5]NIE Institute of Technology, Mysuru, India
(affiliated to VTU Belagavi)

Abstract : Online social networks (OSNs) are becoming increasingly popular and Identity Clone Attacks (ICAs) that aim at creating fake identities for malicious purposes on OSNs are becoming a significantly growing concern. Such colluding attacks affect the reliable relationships. The purpose of this paper is to overcome such attacks by matching the user profiles across many OSNs by analyzing and characterizing the behaviors of ICAs. Then, we propose a prediction framework that focuses on identifying suspicious identities. Towards predicting suspicious identities, we propose two approaches for attribute similarities and User activities. The first approach deals with building a classifier based on semi supervised techniques for attribute extraction and matching; and the second one focuses on tracking the user activities. Experimental results are demonstrated to validate the accuracy of our prediction approach.

***Index Terms* – OSN, ICA, semi supervised techniques**

I. INTRODUCTION

As Online Social Networks (OSNs) such as Facebook and Google+ are becoming part of people's daily lives, personal information becomes easily available for attackers. Information harvesting, by the OSN operator, malicious users, and third party commercial companies has recently been identified as subjected to many security issues. Recently, a new attack called Identity Cloning Attack (ICA), which focuses on forging user profiles on OSNs, has been introduced. In this attack, the attacker first tries to gather the target user's information such as name, location, occupation, gender from his profile in the OSNs and creates a similar or identical profile on OSN sites. Later, the attacker sends the friend request to the victim's contacts. Once the friend request is accepted, he builds the friend network and gains the access to the profiles of the victim's friends. In order to overcome ICAs, we need to educate users to reduce sharing sensitive information on the OSNs.

However, prediction of fake identities is a challenging task. One such challenge is several people have similar names on the online social networks so, it's possible that their identities on the OSNs might be identical. So we cannot conclude all the similar identities as faked identities. This paper proposes a two step approach to detect the ICA attackers on OSNs, first step is based on semi supervised technique that matches the user profiles from two different OSNs using attribute similarity and the second step deals with the creation of the frequent patterns by tracking the user activity. Later, we present the experimental results to demonstrate that the prediction schemes are effective and more accurate.

II. LITERATURE REVIEW

Several researches have been made for prediction of fake accounts in OSNs. One such work [1] "A new approach for finding Cloned Profiling in OSN" was carried out in 2014, under this work a new approach for detecting clone identities was proposed by defining profile similarity and strength of relationship measures. The accuracy of this prediction is less. Another work [2] 8th ICECE paper on "Community Recommendation in Social network using strong friends and Quasi -Clique approach" was published in 2014, Graph Mining technique is used to find strong friends from user's friend list and Clique Technique is used to recommend the communities who share the similar interests. In this approach the database is represented in a graph format so it is easy to understand but involves use of complex algorithms.[3] "Detecting Social Network Profile Cloning" is another work done in 2015 for investigating whether the victim has been subjected to clone attack by using architectural design and implementation details of prototype system. It can be implemented only in one social network. In the year 2017 [4] an IEEE paper named "Preventing Colluding Identity Clone Attack in OSN" , in this work a classifier based on features and text that are extracted form user's profile is built in order to overcome colluding attacks. The accuracy of this approach is less.

Since the accuracy of predicting the fake profiles in most of the proposed approaches is less, therefore, we are enhancing the existing approaches using another level of filtration by tracking the user activities, which is more accurate and effective.

III. PROPOSED METHODOLOGY

The main purpose of the proposed approach is based on predicting the Identity Clone Attacks on the multiple Social networking sites. The attackers impersonate as friend of the legitimate users and send friend request to them and gain access to sensitive information. In order to avoid these colluding attacks we proposed a two step approach to predict the fake and genuine user accounts.

A. Data Initialization

In order to detect the clone profiles, large number of datasets from multiple OSNs is required. It is very hard to find the datasets with the textual information based on ICA to validate our framework hence, Two social networking sites similar to Facebook and Twitter and a synthetic dataset of 1000 user profiles with the profile attributes and their activities in the social network is created.

B. Training Dataset

In this phase the aim is to identify which users belong to both the OSNs. Each user profile attributes are extracted from both the networks and are classified by using one of the semi supervised learning technique called FuzzySim Classifier and next we checked each matched pair of user profiles to see whether it belongs to same genuine user. The remaining unmatched profiles will be classified as fake accounts.

C. Structure of the Model

In this phase of our proposed approach, we built a model that consists of two step filtration. In that, the first step focuses on calculating the attribute similarities of two profiles from multiple OSNs. The calculated attribute similarity value is compared with the fixed threshold value to classify the profile is genuine or fake. To carry out this step we use a semi supervised machine learning technique. If the profile similarity value is greater than the fixed threshold value then we go to the next level of filtration. Under this level of filtration the patterns are created by tracking user activities. Next, we classify the account as genuine or fake based on the patterns of the user activity.

C.1 Attribute Similarity

We review the existing similarity metrics and then formulated the FuzzySim similarity. It is one of the powerful similarity metrics which is a character based similarity. Consider an example where a particular user has a profile attributes set T_1 {name, date of birth ,age, city, gender} in first OSN and another set of profile attributes T_2 second OSN. The attribute similarity is calculated using cosine method as follows:

Cosine Similarity : FCOSINE = $|T_1 \cap T_2| / \sqrt{} |T_1| \cdot |T_2|$

ALGORITHM 1: FuzzySim(Cosine Method)

```
Step 1: Extract the constraints (first name,last name,age…)

Step 2: Calculate the similarity using Cosine method
        FCOSINE = $|T_1 \cap T_2| / \sqrt{} |T_1| \cdot |T_2|$

Step 3: S(1,2)=No. of characters of matching/Total no of
        Characters in a constraint

Step 4: If {value > 0.5} consider these constraint
       //set the no of constraint to match for fake account
        Prediction -min_rec=8 constraints

Step 5: Check if(constraint matching count > min_rec)
            Genuine
       Else
            Fake
```

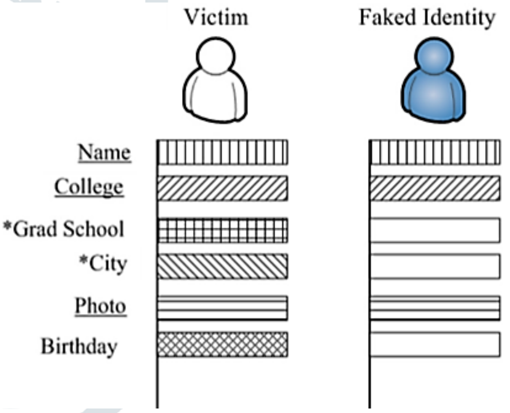

Fig.1 Attributes characteristics of the Genuine and Fake Identities

The computed similarity value is compared with the fixed threshold value 0.5 ,if it is greater than this value it is considered as the genuine account otherwise fake.

C.2 Tracking User Activity

In order to get the more accurate classification of the profiles into genuine or fake accounts, in this approach we propose a Predictive FP growth algorithm. Under this algorithm we will extract the user activity information from the user profile from OSN1 then Tokenization technique is applied. It tokenizes string into token sets (e.g., using white spaces) and quantifies the similarity based on the token sets. For example, given string “BLUE SKY”, its token set is{‘BLUE’,’SKY’}.It’s a keyword extraction method where the stop words are removed and only keywords are retrieved. Based on the predefined set of keywords in the database the clusters are formed. Based on the cluster the Area of Interest of the user is identified for the OSN1. The similar approach is followed for the user profile in the OSN2. If the AOI of both the OSNs match then the particular user account is classified as genuine otherwise fake.

ALGORITHM 2: Predictive FP-Growth

```
Step 1: Retrieve shared information from the database(User1-OSN1)

Step 2: Tokenization(Keyword extraction method -removing the stop words and retrieving
          the key words)

Step 3: Clustering the messages shared by the users(grouping of similar objects)
                  By comparing with the predefined dataset(set of keywords)

Step 4: Check if(matching count>min_rec)

Step 5:Identify the user OSN1 area of interest(AOI) / patterns(priority wise)

Step 6: Retrieve the shared information from other database(User2-OSN2)

Step 7:For each entry Mi(messages) in buffer(storage server) do
         Trace user (OSN2) AOI, using following steps
             → Tokenization
             → Clustering the messages shared by the users
                  By comparing with the predefined dataset(set of keywords)
             → Check if(matching count>min_rec)

Step 8:Compare the present user AOI(OSN1) with the previous user AOI(OSN2)

Step 9: If( AOI Matches)
             Genuine
           Else
             Fake
```

IV. SYSTEM DESIGN

In this section, we proposed a framework for the ICA prediction on OSNs. In our proposed system there are mainly three user requirements namely Admin, Member and Visitor. Member is the registered user who receives the services from the OSN. Admin maintains the application and has the complete authority. He/She can track the registered users details and can also view and list the fake user accounts which the system predicts. Visitor has the limited accessibility who can view the basic information related to the application and can access only the registration page and login page.

As shown in the Fig.2, in the proposed system the user can update the profile, send friend requests, search for the users and share information. All the information shared by the users will be stored in the server through Internet. These datasets will be managed by the Admin and manages the Keyword datasets which are required for the fake account prediction. In our framework, the system is trained in such a way that whenever the user send the request, it will extract the profile attributes of that user from both the OSNs and will predict whether the account is fake or genuine. If the account is genuine, the system will track the user activity of the particular user from both the OSNs and will form the pattern based on the keywords stored in the predefined keyword database(like education, sports, politics). This information will be updated to the recipient and the Admin end. The admin can also get the details about the accuracy of account prediction for the given datasets.

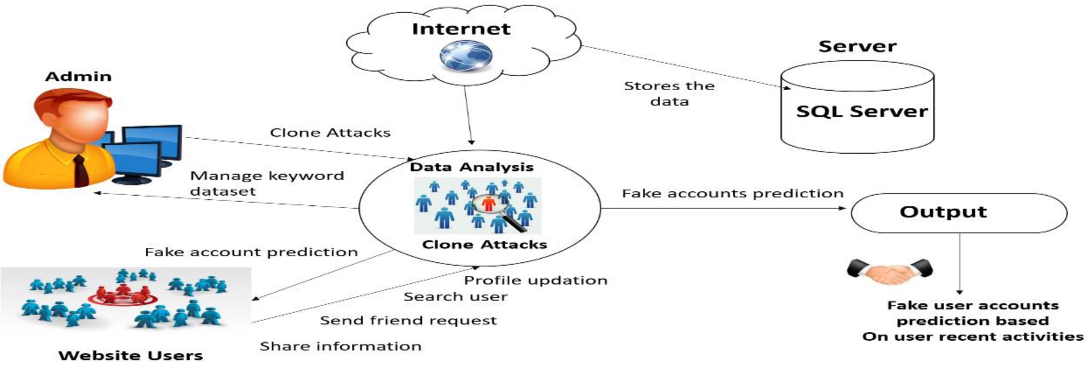

Fig 2. Clone attacks in Social networks

V. EXPERIMENTAL RESULTS

Relationship between fake accounts and registered accounts

For the experimental purpose of the proposed approach, we have used model datasets and generated a graph to visualize the relationship between the no. of registered accounts and the no. of fake accounts. In the Fig 4, the experimental result shows the Prediction of no of fake accounts among the registered accounts in the particular period of time.

Comparison Between the Prediction Accuracy of FuzzySim vs Naive Bayes

In the research we tested the prediction accuracy of the accounts using two different types of classifiers i.e. FuzzySim and Naive Bayes. As shown in the Fig 3, the best prediction results are achieved using the FuzzySim classifier. On reduced set of attributes and instances that classifier correctly classified 79.87 % of instances whereas, Naive Bayes classifier classified 76.33 % of instances.

Correct classification of 79.87 % of all instances in the best case can be considered as relatively good result. Further improvements can be made possible by using some other classifiers.

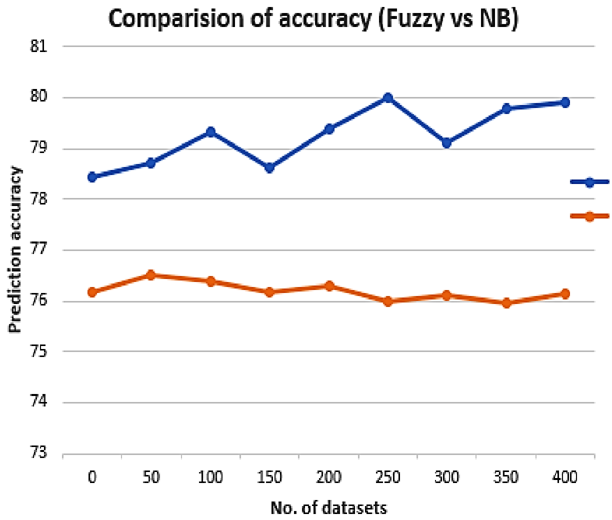

Fig 3. Comparison of Prediction Accuracy

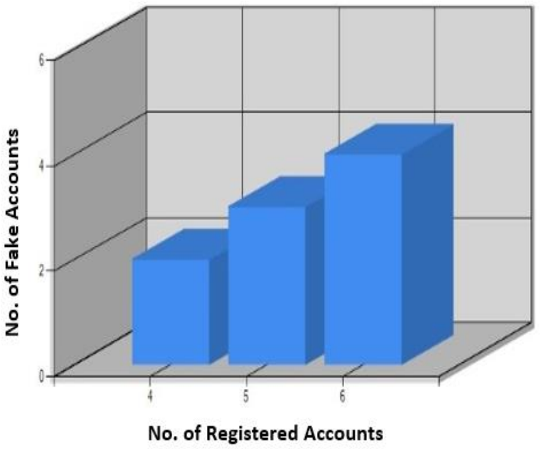

Fig 4. Fake Accounts Prediction in given dataset

CONCLUSION

OSNs have become part of our daily life and most of the users spend more time on social networking sites .OSNs are generally used to interact with other people through the sharing experiences, images, videos. However ,OSNs are subjected to various threats from hackers, fraudsters and online predators, all of whom are capable of stealing sensitive data from various target users. ICA are becoming the significant threat in OSNs. It affects the trust equations among various users and exposes the personal information .In this paper we proposed a two-step approach to predict the fake profiles on multiple OSNs. In the first step we perform matching of user profiles based on attribute similarity using FuzzySim .If the profile matching occurs up to 80%, we go to the next level of filtration. Second step involves the frequent pattern creation based on user activity to predict if the account is fake or genuine. The experimental results gives accuracy of 79.87% for the given instances. Our proposed approach gives more effective and accurate results.

REFERENCES

[1] Fatemah Salehi Rizi,Mohammmad Reza Khayyambashi. “A new approach for finding Cloned Profiling in OSN” ACEEE(April 2014).

[2] Anjum Ibna Matin,Sawgath Jahan. “Community Recommendation in Social network using strong friends and Quasi -Clique approach” 8th ICECE (Dec 2014).

[3] Georgios Kontaxis, Iasonas Polakis. “Detecting Social Network Profile Cloning”.

[4] Georges A. Kmhoua, Niki Pissinou, S.S.Iyengar. “Preventing Colluding Identity Clone Attacks in Online Social Networks” 2017 IEEE 37th International Conference on Distributed Computing Systems.

[5] Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online social networks: threats and solutions." IEEE Communications Surveys & Tutorials 16.4 (2014): 2019-2036.

[6] Wang, Jiannan, Guoliang Li, and Jianhua Fe. "Fast-join: An efficient method for fuzzy token matching based string similarity join." In Data Engineering (ICDE), 2011 IEEE 27th International Conference on, pp. 458-469. IEEE, 2011.

[7] He, Bing-Zhe, Chien-Ming Chen, Yi-Ping Su, and Hung-Min Sun. "A defence scheme against identity theft attack based on multiple social networks." Expert Systems with Applications 41, no. 5 (2014): 23452352.

[8] L. Jin, Y. Chen, T. Wang, P. Hui, A. V. Visalakos, “Understanding User Behavior in Online Social Networks: A Survey”, IEEE Communication Magazine, September 2013, pp. 144-150.