International Journal of Engineering & Technology, 7 (3.10) (2018) 83-87

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Advance Identification of Cloning Attacks in Online Social Networks

Megha Renuka Prasad[1], Santhosh Kumar B J[2]

[1, 2] Department of Computer Science
[1, 2] Amrita Vishwa Vidyapeetham
[1, 2] Amrita School of Arts and Sciences
Mysore, India
[*]Corresponding author E-mail: meghaprasad.mp1@gmail.com[1]

Abstract

Online social networks (OSN) have changed the way individuals collaborate and convey to reconnect with old companions, acquaintances and set up new associations with others considering leisure activities, interests, and fellowship circles. Shockingly, the member's lamentable acknowledgment of reckless conduct in sharing data, often worthless safety efforts from part of the framework heads and, at last, take advantage of the distributed data in Online Social networks as an intriguing objective to attackers. As OSN is becoming increasingly popular and identity cloning attacks (ICA) mechanism designed to fake the identity of users on OSN is becoming one significant growth concerns. This attack has been seriously affected the victims and other users to establish the relationship of trust, if there is no active application defense.

In this paper, the first step analyzes the member constraints and characterize the profiles based on their behavior. Then focusing on the categorized profiles of the framework and verify each of them using their area of interests. To detect suspicious identities, two methods are followed based on attribute similarity of profiles and by verifying similar profiles in a cross-site environment by their area of interests.

Keywords: *Area of Interest; Clone Attacks; Fake Profiles; Frequent Pattern; Online Social Network;*

1. Introduction

In today's world, the Internet is the center of information sharing. The social networking represents a strong part called Web 2.0. It is the most convenient place for people to connect with friends or to discuss new ideas with people of similar interests. Basically, a social network is an interactive network of mutual networks, which shares one another's interest and receives interactive information sharing through the service.

Social networking sites come in different facets. Some OSNs are robust in certain localities like Ren-Ren (China), Facebook (India), Mixi (Japan) or VKontakte (Russia). Globally well-known sites are Facebook and Twitter. Depending on the user base, there are dedicated or focused groups - LinkedIn and Xing have focus on business, enabling people to share business connections and job offerings. Other networks focus on keeping in touch with your old friends.

Regularly, when utilizing social networking services, programs that are unapproved may abuse the corporate computers, unapproved access to physical and network services, password abuse, and exchange of personal data between computers and work, as a rule faces different dangers. In any case, over the top trust in the social networks, the users may experience different assaults and information leaks.

In this work, the initial step is to check the similarity of text-based attribute comparisons to find the matching user profiles in a cross-site environment. Secondly, the matching user profiles are observed in one OSN and compared the same with another OSN based on the latest info shared by the user. Thirdly, to distinguish between the users in the OSNs, by recognizing the area of interest of each member using clustering technique.

Finally, the uncommon behaviors of the users are diagnosed. The experimental results and effectiveness of methods are presented.

2. Related Works

Naruchitparames et al. As of recently, the separating strategy has represented basic properties of the interpersonal organization. The Facebook Graph API bunches the shared likes and shared music together. Potential companions will rank higher as the quantity of shared general interests increment. In the exploration, different levels of detail relating to training (secondary school, undergrad, and graduate and expert instruction) were assembled. This range is sufficiently extraordinary differential to decide the probability of collaboration among people [1].

Sebastiani et al. To help the content-based separating in online social networks, examined divider engineering is presented. Content mining strategies are utilized to order the approaching messages. Conventional content grouping strategies have real deficiency in characterizing the short instant message. A mechanized framework called separated divider is composed in the paper to channel undesirable messages from client dividers. In the framework, Machine Learning based content classification procedures are utilized to consequently assign each short instant message with set of classifications in view of the substance [2].

Thilagavathi et al. Short Text Classifier is worked to exact extraction and set of segregating highlights in the message. Neural learning model is utilized for the proficient content characterization. [3]

Fortunato et al. A subset of clustering calculations is considered with different information. The mutual data portrays people as hubs and their companionships as connections. Calculations with this contribution as data are called auxiliary calculations. The element-based calculations utilize highlights and credits of the hubs to separate gatherings. These highlights can be age, sexual orientation, and instruction of individuals in OSNs. The last classification joins the thoughts as system structure and hubs' highlights [4].

Eslami et al. utilizing the element-based calculations requires mining extra information from a long range interpersonal communication site. This outcomes in higher processing time which makes controlling investigations in a constrained time in the lab, troublesome or relatively incomprehensible [5].

Labade et al. The proficient calculation for visit item-set mining is the FP-Growth Algorithm which goes for wiping out the holdups of the Apriori-Algorithm in creating and testing competitor set. As a substitute of putting away everything in the database, it stores the certifiable exchanges from the database in a tree structure and everything has a connected rundown going through all exchanges that contain that. This new structure is implied by FP-tree. Essentially, all exchanges are put away in tree-like structure. [6]

Devmane, M. A. et al. Each Record store is analyzed with respect to the client's unique profile. An examination is made between the first profile and the looked record and after the correlation a similarity list is ascertained. The profile having the higher similarity record might be the cloned profile. The profiles having low similarity are pronounced as fake profiles. The cloned and fake profiles are affirmed with the honest to goodness proprietors of the separate profile. [7]

Hasan, M. et al. essentially, they don't just consider the well-known or individuals having regular interests to be prescribed as a companion, yet individuals having exceptional or one of a kind interests ought to be suggested as companions. They have expected another framework for recommendation of friends (FRF) in view of client's online conduct and the primary commitment relates the meaning of client's online conduct and calculation to suggest a companion. [8]

L Jin et al addressed the difficulties and propose a dynamic location system to recognize existing pseudo-personalities on OSNs. By researching and describing a fake character. They have proposed two techniques for figuring the closeness between forms in view of trait comparability and companion organize similarity. In this view, a structure to recognize false characters on the OSN. In our testing procedure, we utilize an arrangement of adaptable parameters to alter the casualty and its clones to precisely recognize distinctive OSNs, where the produced personality may have diverse conduct [9].

G Kontaxis et al present an automatic search tool and identify clone personal data in social networks. Key rationale behind its idea is that it utilizes client (Or client recognizable proof) data, gathered from the client the first interpersonal organization design document to find a comparative setup Cross-informal community. Any reappearance to the result depends on Common personal information is considered how rare, is considered suspicious and carries on further examination [10].

Z Shan et al proposed two distinct possible results. First, the snowball-sampling and then the iterative attacks. The idea of examining the clone attacks and introduced a new detector, CloneSpotter. This new system utilizes detailed log IP records and present the location of field evidence, to regulate whether a suspicious account is being manipulated by a real user or an attacker. Adding to that, a content-based protection to the user is provided which is easy to the distributed client [11].

M Conti et al in this article, they initially attempted to ponder and give a location structure OSA in FPA, the subject does not have an online profile. In view of the advancement rate of social network's outlines for average clients with their systems; a foe should endeavor to get away from the location structure. It is essentially on Experimental examination joined with unmistakable structures in Social-arrange collaboration and its insights. [12]

3. Methodology

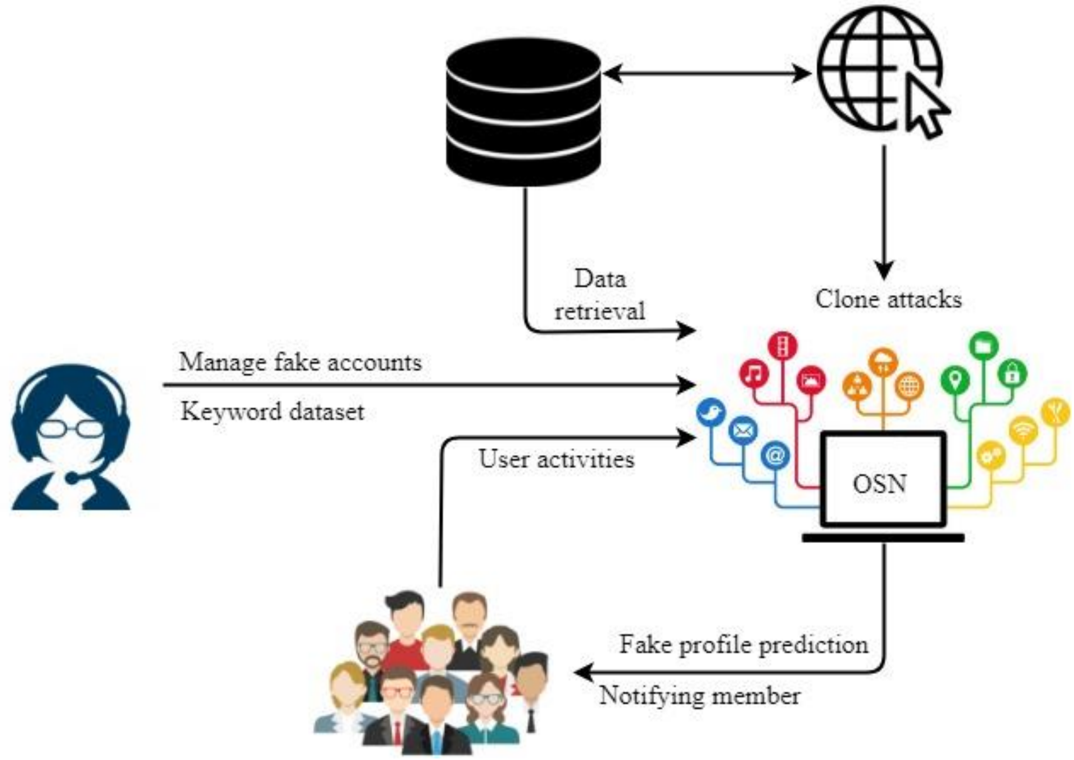

Fig. 1: Architectural Diagram

3.1. Computing the Similarity Index to Classify the Cloned Profile

In this article, the underlying development is to tackle with a straightforward representation of content-based attribute comparisons to locate the coordinating member profiles in a cross-site condition. Each record is analysed concerning the member's unique profile. An assessment is made between the first profile and the looked record in two OSNs and after the comparison the similarity is computed. The profile having the greatest similarity, that record might be the real profile. The profiles having low comparability are expressed as fake profiles [7] [12].

3.1.1. Member's Profile Matching

Step 1: Extract the constraints of a user in OSN1 and OSN2.

Step 2: Calculate the similarity index using cosine similarity method

$$Sim(OSN1, OSN2) = \frac{No.of\ Constraints\ Matching}{Total\ Constraints} \quad (1)$$

$$If\ (value > Threshold) \quad (2)$$

Step 3: Consider those constraints and check if the constraints matching count is greater than minimum support

$$If(count > support) \quad (3)$$

Then, Genuine. Else, Fake

Step 4: If Genuine, then track the user activities

3.2. Tracking the Member's Frequent Activities

Secondly, the matching user profiles are observed in one OSN and compared the same with another OSN based on the latest information shared by the user. Thirdly, to distinguish between the users in the OSNs we recognize the area of interest of each user by constraint-based clustering technique.
We should consider three sets: users/members (U), activities (A) and Area of interests (I).

$$U = \{u \mid users\ in\ OSN = \{u1, u2, u3, \dots, un\}$$

$$A = \{a \mid activities\ of\ the\ users\ in\ OSN\} = \{a1, a2, a3, \dots, am\}$$

$$I = \{i \mid subset\ of\ activities\ any\ user\ in\ OSN\}$$

The conduct of the part is exclusively related to the activities of the members. Members can share diverse activities. In any case, the conduct will be those activities which are performed by the member indicated as I. The equation for the behavior could be given as:

$$B: U \rightarrow I \quad (4)$$

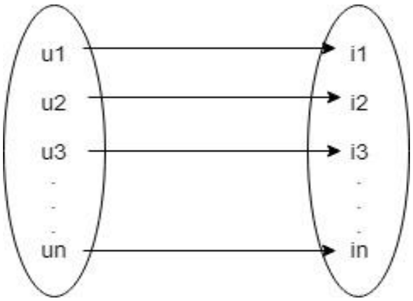

Fig 2: User related to area of interest

I is a proper subset of A: I ⊆ A (5)

3.2.1. User Activities

Scan the User (OSN1 and OSN2) in the Database

OSN 1

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

Step 2: Tokenization

Step 3: Clustering the information shared by the users (grouping of similar objects i.e., Area of Interests) by comparing with the predefined dataset (created by the admin).

Step 4: Check if (matching count > minimum_support) [number of contents to compare]

Step 5: Identify the user (OSN1) area of interest (priority wise). (Cluster [AOI] with more number of objects)

OSN 2

Step 1: Retrieve shared information from the other database (User2 - OSN2)

Step 2: Trace user (OSN2) AOI, using the following steps:

Step 3: Tokenization

Step 4: Clustering the messages shared by the users (grouping of similar objects i.e., Area of interests) by comparing with the predefined dataset (created by the admin)

Step 5: Check if (matching count > minimum_support) [number of contents to compare]

Step 6: Compare the present user AOI (OSN1) with the previous user AOI (other OSN2).

$$If\ (AOI\ Matches) then\ Genuine, Else\ Fake$$

Finally, the uncommon behaviors of the users are diagnosed. The experimental results and effectiveness of methods are presented in the upcoming sections.

4. Experimental Results

Table 1: Member related constraints

Sl no.	Constraints	Possibilities
1	Email ID	Unique ID for a member
2	First Name, Last Name	Name
3.	Gender	Female, Male
4.	Date of Birth	Day, Month, Year
5.	Education information	School, College, Employment
6.	Location	City, State, Nationality
7.	Relationship status	Married, Single
8.	About you	Member's traits
9.	Language	English, Hindi, Native Language
10.	Religion	Hindu, Christian, Muslim
11.	Contact Number	Phone number
12.	Content type (Area of Interest)	Education, Sports, Art, Music etc.

For experimental motivation behind the proposed calculation, a model dataset having the comparable highlights of association and connections like an ordinary social networking site has been considered. Postings database has content-type as an imperative. The Content-Type database keeps every one of the interests of a member. The Postings database tracks all the client activities and in addition the frequencies of activities, consecutively. The member database contains the data of the client.

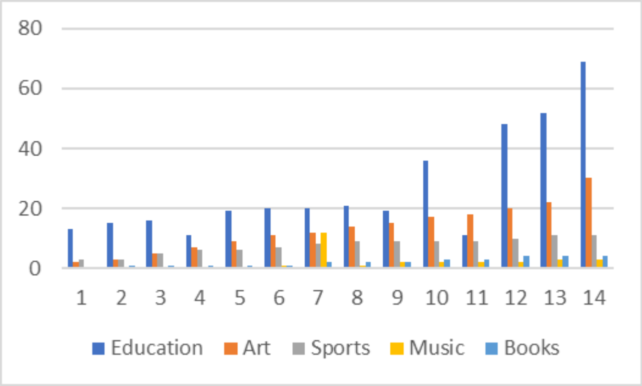

Fig 2: Member's Area of Interest.

The fig. 2 represents the member's area of interest according to the total frequency of the messages that has been shared in the OSN. Thus, it helps in understanding the common behaviors of the member in the cross-site environment.

The modified FP Growth calculation is executed on the association of the considerable number of information and the calculation yields the uncommon practices which are utilized for fake profile forecast. The system demonstrates exactness for the model dataset with a few restrictions. On the off chance that two members have many interests in common is predictively to be a fake profile in the same-site however can be anticipated as either real or fake profile in cross site environment, again members having a couple of activities in common possibly be distinct profiles.

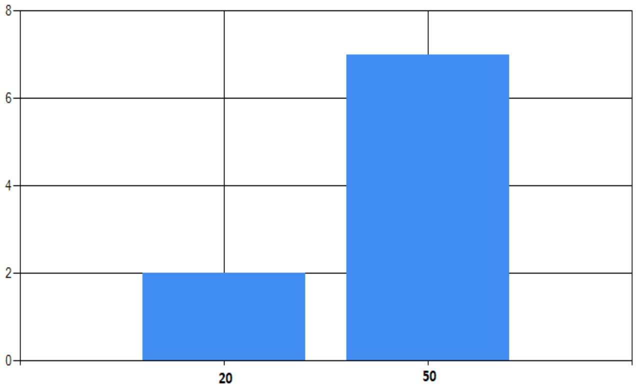

Fig 3: Total number of users (x-axis), Number of Fake profiles predicted (y-axis).

The fig. 3 shows the results of the prediction of the fake profiles by analyzing the uncommon behavior of a member in cross-site environment.

5. Conclusion

Primarily, the similarity between member profiles that can be impersonated is calculated. The core idea behind the mechanism is to recognize the fake profiles according to the frequent user activities which exclusively identifies the members' area of interest.

To filter the impersonation of member accounts from OSNs, the component accomplishes a classifier to implement adaptable content dependent filtering rules. The adaptability of the component as far as filtering alternatives is upgraded through the expectation of member activities example of a part.

In that light, the results are presented from a study regarding the type and amount of information exposed by social network users which allows an invader to clone a profile also supports us in identifying the clone.

Acknowledgement

As a matter of first importance, I'm obliged to Mata Amritanandamayi Devi for her motivation and direction in many ways.
Sincerely, I thank our Director, Br. Sunil Dharmapal and Correspondent Br. Venu Gopal for giving the important condition, framework and consolation for doing my exposition work at Amrita Vishwa Vidyapeetham University, Mysuru Campus, and Mysuru.
I offer my genuine thanks to Prof. Vidya Pai C, Principal, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru for the consistent help and encouragement.

References

[1] Naruchitparames, J., Güneş, M. H., & Louis, S. J. (2011, June). Friend recommendations in social networks using genetic algorithms and network topology. In Evolutionary Computation (CEC), 2011 IEEE Congress on (pp. 2207-2214). IEEE.

[2] Sebastiani, F. (2002). Machine learning in automated text categorization. ACM computing surveys (CSUR), 34(1), 1-47.

[3] Thilagavathi, N., & Taarika, R. (2014, March). Content based filtering in online social network using inference algorithm. In Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference on (pp. 1416-1420). IEEE.

[4] Fortunato, S. (2010). Community detection in graphs. Physics reports, 486(3), 75-174.

[5] Eslami, M., Aleyasen, A., Moghaddam, R. Z., & Karahalios, K. (2014, November). Friend grouping algorithms for online social networks: preference, bias, and implications. In International Conference on Social Informatics (pp. 34-49). Springer, Cham.

[6] Labade, S., & Kini, S. N. (2006). A survey paper on frequent item set mining methods and techniques. International Journal of Science and Research. Jia, YW, Wang, H., and Yan, DH, 534-542.

[7] Devmane, M. A., & Rana, N. K. (2014, May). Detection and prevention of profile cloning in online social networks. In Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1-5). IEEE.

[8] Hasan, M. M., Shaon, N. H., Al Marouf, A., Hasan, M. K., Mahmud, H., & Khan, M. M. (2015, December). Friend recommendation framework for social networking sites using user's online behavior. In Computer and Information Technology (ICCIT), 2015 18th International Conference on (pp. 539-543). IEEE.

[9] Jin, L., Takabi, H., & Joshi, J. B. (2011, February). Towards active detection of identity clone attacks on online social networks. In Proceedings of the first ACM conference on Data and application security and privacy (pp. 27-38). ACM.

[10] Kontaxis, G., Polakis, I., Ioannidis, S., & Markatos, E. P. (2011, March). Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on (pp. 295-300). IEEE.

[11] Shan, Z., Cao, H., Lv, J., Yan, C., & Liu, A. (2013, January). Enhancing and identifying cloning attacks in online social networks. In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication (p. 59). ACM.

[12] Conti, M., Poovendran, R., & Secchiero, M. (2012, August). Fakebook: Detecting fake profiles in on-line social networks. In Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on (pp. 1071-1078). IEEE.

[13] Matin, A. I., Jahan, S., & Huq, M. R. (2014, December). Community recommendation in social network using strong friends and quasi-clique approach. In Electrical and Computer Engineering (ICECE), 2014 International Conference on (pp. 453-456). IEEE.

[14] Banerjee, S., & Niyogi, R. (2015, August). A method for community recommendation for social networks. In Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on (pp. 2341-2347). IEEE.

[15] Brandes, P., & Wattenhofer, R. (2012, October). On finding better friends in social networks. In Symposium on Self-Stabilizing Systems (pp. 266-278). Springer, Berlin, Heidelberg.

[16] Raju, E., & Sravanthi, K. (2012). Analysis of social networks using the techniques of web mining. International Journal, 2(10).

[17] Kharaji, M. Y., Rizi, F. S., & Khayyambashi, M. R. (2014). A new approach for finding cloned profiles in online social networks. ArXiv preprint arXiv: 1406.7377.

[18] Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, 16(4), 2019-2036.

[19] Kamhoua, G. A., Pissinou, N., Iyengar, S. S., Beltran, J., Kamhoua, C., Hernandez, B. L., ... & Makki, A. P. (2017, June). Preventing Colluding Identity Clone Attacks in Online Social Networks. In Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on (pp. 187-192). IEEE.

[20] Kiruthiga, S., & Kannan, A. (2014, April). Detecting cloning attack in Social Networks using classification and clustering techniques. In Recent Trends in Information Technology (ICRTIT), 2014 International Conference on (pp. 1-6). IEEE.

[21] Wang, Z., Liao, J., Cao, Q., Qi, H., & Wang, Z. (2015). Friendbook: a semantic-based friend recommendation system for social networks. IEEE transactions on mobile computing, 14(3), 538-551.

A. Asok, Jisha, T. J., S. Ashok, and Dr. M.V. Judy, "Integrated framework using frequent pattern for clustering numeric and nominal data sets", Advances in Intelligent Systems and Computing, vol. 408, pp. 523-530, 2016.

[22] M. S. Pallavi, Hegde, V., Anushadevi, H. G., and Ambika, V., "Automated spam detection in e-mail using SVM", International Journal of Applied Engineering Research, vol. 10, pp. 25219-25228, 2015.