



International Journal of Emerging Technologies in Computational and Applied Sciences(IJETCAS)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

An Assessment of Algorithms to Detect the Profile Cloning in Social Networks

Naresh Kumar¹, Poonam Dabas², Komal³

Department of Computer Science and Engineering

University Institute of Engineering and Technology (UIET),

Kurukshetra University, Kurukshetra-136119, Haryana, INDIA

Abstract: The social network is a medium that tries to simulate the social interaction of the users by providing a construct to create and manage different relationships. In the present age, people of almost all age groups are active on different kinds of Social Media to connect and explore their relationship with different people. This has led to a large amount of information available on social sites openly which may include personal data and sensitive stuff and has given rise to the problem of Profile Cloning. Profile Cloning is a practice in which a person makes a profile in name of some other person by capturing their information provided on social networking platforms. It results in stealing a lot of personal information. In this paper an attempt has been made to review various algorithms developed to detect the cloned as well as fake profiles along various social sites.

Keywords: Social Networks, Profile Cloning, Fake Profile, Facebook, Instagram, Google+

I. INTRODUCTION

Online social network is an e-service for simulating how humans interact with each other and helps in maintaining the relations of human life. This interaction is not limited to any boundaries of age. People of almost all age group are active on various different social media. Social Networking Platforms have become a way of entertainment for people of every age group. Social Networking Sites have provided a way to share believes, ideas and thoughts of every individual. In today's modern age, existence of life without social networks seems to be impossible. People spent a large segment or portion of their time on various social media such as Facebook, Instagram, Google+, etc. [1].

History of different social media can be tracked to 1995 when first social networking site Classmate.com was developed. It was a site developed for variety of users to connect to their previous classmates. Currently this site has more than 40 millions user registered. But this site lacks the feature of users connecting directly to each other; they can only communicate through the school they have attended together. First site having the feature of users directly connecting and communicating with each other came into being in 1997 with the name SixDegrees.com. In fact, SixDegrees.com is the first site that qualifies the criteria of social networking platform.

As the time passed, Social Networks started to gain popularity as the number of users active on social media was getting increased. As the 21st century started to approach, a number of sites having the capability of finding friends, thus fulfilling the general purpose started to establish. Friendster was one such social media which gain popularity in early 2000. The major focus of Friendster was to allow friends-of-friends to connect to each other and thus came into being as a rival to online dating site called Match.com. Various other social networking sites like LinkedIn, CyWorld and Ryze came into being during the same time period.

In 2003, another social networking platform called MySpace.com came into existence and served as an alternative to Friendster and several other sites. Soon after coming into existence, MySpace gained a lot of popularity and became the largest social networking platform as it provided the capability of customizing the profile appearance, a feature that became very popular with almost all set of users. Currently, MySpace is known to have more than 247 million user accounts, more than twice the number of users on next largest and popular social network, Facebook [2].

With time, as social sites started to gain popularity, various other different kinds of social networking sites started to come into being. Examples include blogging sites (Live-Journal and BlogSpot), multimedia content sharing sites (Flickr, YouTube, and Zoomr), and professional networking sites (LinkedIn and Ryze). All of the above social sites are developed to serve the different kind of intent but they all are having the same feature of exploitation of social networks to continuously improve their work. This list of social sites is keep on increasing as more and more time is passing [3].

A. Architecture of Social Networks

The underlying architecture of Social Networks consists of 3 layers mainly:

- Application Layer: This layer is GUI based and designed for interaction with the end user. It includes functions like Creating a Profile, Sharing Information, Interacting etc.

- Service Layer: Service layer basically serves as an interface between the other two layers of Social Networks i.e. Application Layer and Data Layer and helps in execution of the things with the help of data layer.
- Data Layer: This layer is what serves as a repository of data and its function is to give services to other layers [4].

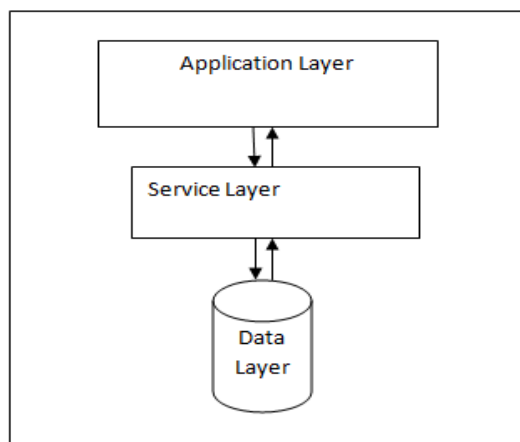


Figure 1: Basic architecture of Social Networks [4]

II. PROFILE CLONING

Online Social Networking Sites are rage of today as they provide a network to connect and communicate with a variety of people whether they are known or not in real world. People from almost every age group are active on social media leading to a large number of users across various social platforms. Facebook alone has more than 1.2 Billion users. This gives rise to a large amount of data and personal information being shared over the internet which is not a good thing as it leads to cloning of profiles.

Profile Cloning also called as Identity-Theft Attack is an attack in which a person steals information from other people's profile to use the information in fulfilling his/her goals. All these have become possible because a large amount of user's data and personal information is available on the social sites which can be intercepted very easily. Main aim of Identity Theft Attacks also called as Profile cloning attack is to create a duplicate or fake identity of already registered users in an online social network so that their friends can be tricked into thinking the fake profile as the authenticated one and establishing links with them and using these links to get the private information from the victim's friend which is generally not shared in their public profiles [5].

Profile Cloning is basically of two types:

- Same-Site Profile Cloning: In this type of profile cloning, adversary steals information and data from a social networking platform and clones his/her profile across the same platform. After creating a cloned profile, adversary may try to send the connection request to original user's connections and using them to execute his/her malicious intentions.
- Cross-Site Profile Cloning: In this type of profile cloning, adversary steals credentials from a social networking platform and uses it to create or develop a profile on some other social network where the user might not be present. In this type of profile cloning, adversary tries to gather as much amount of information as possible and try to create a profile having maximum resemblance to the legitimate user. This type of cloning is really very hard to detect both by the user and the network provider [6].

III. RELATED WORK

In this section, a review of the work so far done in the field of detection of Cloned Profile across various networking platforms is presented. Various advantages and shortcomings of the technique developed so far are studied.

Rizi *et al.* [7] proposed a Identity Clone Attack (ICA) mechanism by defining strength of relationships and profile similarity. It works by collecting attributes that are similar to each other and defining strength of the relationship among different users and then deciding whether the profile is legitimate or cloned by setting a predetermined threshold and comparing the values with the threshold. The researchers used the offline dataset of Facebook to validate their work. There were around 63,731 users in the used dataset and 16,34, 115 links among them.

Devmane and Rana [8] on the other hand, used similarity index based approach to identify cloned profile as well as fake profile across a social networking platform. The researchers also worked on Facebook dataset to validate their work. They used attributes like name, profile, birth date, workplace, education and places and assigned them weight according to how much they affect the detection process. Using these values, a similarity index is calculated which decides whether the profile is fake profile or cloned profile or legitimate one.

Conti *et al.* [9] however used the graph based approach to detect the profile cloning across various social networks. They analyzed the dynamic behavior of social network graphs in context of privacy threats. The idea was to research on temporal evolution of Online Social Networks and characterize real user profile.

Erlandsson *et al.* [10] studied various types of privacy threats that are associated with the user's active on social media and classified them into six categories. The privacy threat identified were a) OSN Information Leakage b) Friend-in-the-middle Threat c) Public Information Harvesting d) Trojan Application e) Friend-in-the-middle Trojan Application f) Socialbot. They also proposed various protection mechanisms against each kind of attack.

Faisal *et al.* [11] highlighted in their paper the need of information security awareness in various social networking sites. Their emphasis was on the importance of various information security measures to protect this information by maintaining the confidentiality, availability and integrity (CIA). Their survey was based on the dataset of Facebook. They presented an Islamic point of view on security and privacy awareness to minimize privacy issues in Facebook.

Fang *et al.* [12] proposed in their paper an automated approach to manage Facebook privacy. They used three predefined levels: basic, medium and advanced to manage privacy concerns over Facebook. They developed an application to automate the process and to provide wide usability and platform independency, two versions were developed: a PHP application and a Firefox add-on.

Fire and Elovici [13] provided a thorough review of all the privacy and security risks present in various social networks and an overview of existing solutions to the above problems is presented. They also provided in their work various Network Provider Solution, Commercial Solutions and Academic Solution to the security and privacy concerns.

Hashimoto *et al.* [14] suggested that network policy management services like Intrusion Prevention System (IPS), Firewall and antivirus, etc are not sufficient to prevent against security and privacy issues present in various social networking sites. They proposed a security framework composed of five blocks: sustain and commitment, then design, after that implementation, then monitoring and finally continual improvement. Each block performs a series of steps to provide the privacy and security across various networking sites.

Li *et al.* [15] discussed the policy for preserving the privacy of social networks that is based upon some logics and rules having three levels: object level, system level and user level. The privacy settings across various attributes can be set to either one of the above levels. This policy is very fine-grained and flexible so as to maintain the dynamics and diversity of social applications.

Bilge *et al.* [16] investigated in their paper two types of profile cloning attacks and showed how much easy and feasible these types of attack are. In the first kind, attackers steal the identity of existing users and then send friend request to their users and connect with them to get the sensitive information. In the second type, it was shown how to easily launch a cross-site cloning attack by creating a fake profile of victim in other social networking platforms where user is not present and thereby using it.

Malhotra *et al.* [17] in their paper created Digital Footprints of the users by extracting information about user identities on various social media through Friend Feed, Social Graph API and Profilactic. Digital Footprints play a very important role in protecting users from security and privacy risks arising due to availability of a very large amount of data on social networking sites. Lastly, analysis and results are presented by applying automated classifiers for disambiguating profiles of users across various social media.

Cuttillo *et al.* [18] proposed Safebook, a privacy protecting and decentralized online social networking application designed as a solution to two issues: violation of users' privacy by the service provider and capitalizing the trust that exists between different users that are connected to each other on social network and know each other in real life so as to deal with privacy-concerning issues. Preliminary results of the approach showed a realistic compromise between performance and privacy is possible.

Cuttillo *et al.* [19] further extended their Safebook application by creating a peer-to-peer architecture so that there would be no centralized control that exists over data. In peer-to-peer connections, Safebook makes use of the trust that is available in order to build a network of trusted peers that can store user's data. Messages between a requester's node and friend's node route through several hops to hide a user's social links that can be reflected by graphs.

Gao *et al.* [20] provided a survey of comprehensive study of security issues in online social networks. They organized attacks into four categories: viral marketing, privacy breaches, malware attacks and network structural attacks and also provided solutions to each type of attack.

Shah Mahmood [21] discovered six new privacy leaks in Facebook and Twitter: a) How an attacker can map email address to real names b) Curse of the timeline c) Reconstruction of a friend's friend list d) Curse of Social Plugins e) Permanent takeover of Facebook account f) Social Network Relay Attacks and provided solutions to each kind of problem.

Kontaxis *et al.* [22] proposed a methodology which can detect cloned profiles in a social networking site. This prototype can be used to check whether users have fallen for any such type of attack. Their prototype basically consists of three components: Information Distiller, Profile Hunter and Profile Verifier. Information Distiller identifies some unique features in users' profiles that can identify them uniquely. Profile Hunter hunts for the

profiles that may be similar to the given user's profile and Profile Verifier calculates the similarity based on the Similarity Score.

Majedi *et al.* [23] believed to extend SQL so that it can be used to support user privacy in social networks. They proposed to extend data manipulation and data definition language to capture privacy preserved mandatory and discretionary access controls.

IV. CONCLUSION AND FUTURE WORK

Profile Cloning is stealing of someone's identity to fulfill some malicious goals. Profile Cloning is becoming very popular across various Online Social Networking Sites. Large amount of personal information shared on social sites have attracted adversaries to capture the information and use it to fulfill their desired goals. In this paper, a review of the various techniques and methodologies developed and devised so far is presented. In some of the research, similarity index based approach is used while other focused on dynamics of social graphs to detect the cloned profile in social networks. All the techniques work well for social networks having their own advantages and disadvantages. We would like to continue our studies further by taking the Similarity Index based approach for Online Social Networks. We would work upon improving the results by increasing the number of attributes in calculation of similarity index and analyzing our proposed architecture by using the dataset of Facebook to produce the improved research.

V. REFERENCES

- [1] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History and Scholarship," *Journal Of Computer-Mediated Information*, vol. 13, no. 1, pp. 210-230, 2007.
- [2] Joan DiMicco, David R. Millen, Werner Geyer, Casey Dugan, Beth Brownholtz and Michael Muller, "Motivations for Social Networking at Work," in *ACM conference on Computer supported cooperative work*, San Diego, CA, USA, November 08 - 12, 2008.
- [3] Danah Boyd, "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life," *MIT Press, Cambridge, MA*, vol. 12, no. 4, pp. 23-35, 2007.
- [4] Brian L. Wilcox, Eric M. Vernberg, Irwin G. Sarason and Barbara R. Sarason, "Social Support: Theory, Research and Applications," *Springer Netherlands*, vol. 24, no. 1, pp. 73-94, 1985.
- [5] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning," in *proceedings of IEEE International Conference on Pervasive Computing and Communications Workshop*, 2011
- [6] Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang and Yen Chen, "Security Issues in Online Social Networks," *IEEE Internet Computing*, vol:15, issue: 4, pp: 56-63, 2011.
- [7] Fatemeh Salehi Rizi, Mohammad Reza Khayyambashi and Morteza Yousefi Kharaji, "A New Approach for Finding Cloned Profiles in Online Social Networks," *International Journal of Network Security*, vol:6, pp:25-37, 2014.
- [8] M. A. Devmane and N.K. Rana, "Detection and Prevention of Profile Cloning in Online Social Networks," in *proceedings of IEEE International Conference on Recent Advances and Innovations in Engineering*, Jaipur, India, 2014.
- [9] Mauro Conti, Radha Poovendran and Marcco Secchiero, "Facebook: Detecting Fake Profiles in On-Line Social Networks," in *proceedings of IEEE International Conference on Advances in Social Networks Analysis and Mining*, 2012.
- [10] Fredrik Erlandsson, Martin Boldt and Henric Johnson, "Privacy Threats Related to User Profiling in Online Social Networks," in *proceedings of IEEE International Conference on Social Computing*, 2012.
- [11] Ammy Amelia Faisal, Bsek Salihatun Nisa and Jamaludin Ibrahim, "Mitigating privacy Issue on facebook by Implementing Information Security Awareness with Islamic Perspectives," in *proceedings of International Conference on Information and Communication Technology for the Muslim World*, 2013.
- [12] Sheh Wei Fang, Dhananjaya Rajamanthry and Mohammad Hussain, "Facebook Privacy Management Simplified," in *proceedings of IEEE International conference on Information Technology-New Generations*, 2015.
- [13] Michael Fire and Yuval Elovici, "Online Social Networks: Threats and Solutions," *Journal of Latex Class Files*, vol:11, issue: 4, 2012.
- [14] Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho and Tadeu Machado, "A Security Framework to Protect Against Social Networks Services Threats," in *proceedings of IEEE International Conference on Systems and Network Communications*, 2010.
- [15] Ma Li, HUO Yingyu and ZHONG Yong, "A Rule Based Privacy Preserving Policy for social networks," in *proceedings of International Conference on Intelligent Systems Design and Engineering Applications*, 2015.
- [16] Leyla Bilge, Thorsten Strufe, Davide Balzarotti and Engin Kirda, "All Your Contacts Are Belong To Us: Automated Identity Theft Attacks on Social Networks," in *ACM Conference of world wide web*, Madrid, Spain, 2009.
- [17] Anshul Malhotra, Luam Totti, Wagner Meira Jr, Ponnuram Kumaraguru and Virgilio Almeida, " in *ACM International Conference on Advances in Social Network Analysis and Mining*, Washington DC, USA, 2012.
- [18] Luecio Antonio Cutillo, Refik Molva and Thorsten Strufe, "A Privacy-Preserving Online Social Network leveraging on Real-Life Trust," in *Journal of IEEE Communications Magazine*, vol. 47, no. 12, pp. 94-101, 2009.
- [19] Luecio Antonio Cutillo, Refik Molva and Melek Onen, "Safebook: A Distributed Privacy Preserving Online Social Network," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Lucca, Italy, 2011.
- [20] Hongyu Gao, Jun hu, Tuo Huang, Jingnan Wang and Yan Chen, "Security Issues in Online Social Networks," in *IEEE Journal of Internet Computing*, vol. 15, no. 4, pp. 56-63, 2011.
- [21] Shah Mahmood, "New Privacy Threats for Facebook and Twitter Users," in *proceedings of IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2012.
- [22] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Networking Profile Cloning," in *IEEE International Conference on Pervasive Computing and Communications Workshop*, Seattle, WA, USA, 2011.