ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Prevention of Fake Profile Proliferation in Online Social Networks

S.Priyanga[1], V.M.Priyadharshini[2], N.Hariharan[3]

P.G. Student, Department of CSE, University College of Engineering, Anna University, BIT campus, Tiruchirappalli, India[1].

Assistant Professor, Department of CSE, University College of Engineering, Anna University, BIT campus, Tiruchirappalli, India[2].

U.G. Student, Department of CSE, University College of Engineering, Anna University, BIT campus, Tiruchirappalli, India[3].

ABSTRACT: Today, Online Social Networks (OSNs) are the most common platforms on the Internet, on which millions of users register to share personal facts with their friends. Online social network users are unaware of the numerous security risks that exist in these networks, like privacy violation, identity theft and sexual harassment etc. Many users disclose their personal information like phone no., date of birth, address etc. Leakage of personal information is a significant concern for social network users. Fake profiles are being created in all the sites and one's information is becoming more and more vulnerable in the past decade. Nowadays the Identity Clone Attack (ICA) is increased in the many social networking websites that causes the frustration between the peoples and social networking websites too. This attack is done by retrieving the information of the individuals profile by anonymous person i.e. individual information is leaked and clone or fake profile is created which shows as real one. Thus this leads to the ambiguity between the owner of the profiles and the person associated to their profile i.e. we cannot have control to create over creation of clone profiles in the OSN and impacts it to the person having his or her own profiles. Hence, a new way of protecting personal information on online social sites is being proposed in this paper.

KEYWORDS: Profile Cloning, ICA attack, Questionnaire

I. INTRODUCTION

1.1 ONLINE SOCIAL NETWORKS

A social network is a social structure made up of a set of social actors (such as individuals or organizations) and a set of the dynamicties between these actors. The social network perspective provides a set of methods for analysing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures. The study of these structures uses social network analysis to identify local and global patterns, locate influential entities, and examine network dynamics.

The social network is a theoretical construct useful in the social sciences to study relationships between individuals, groups, organizations, or even entire societies. The term is used to describe a social structure determined by such interactions. The ties through which any given social unit connects represent the convergence of the various social contacts of that unit. This theoretical approach is, necessarily, relational. An axiom of the social network approach to understanding social interaction is that social phenomena should be primarily conceived and investigated through the properties of relations between and within units, instead of the properties of these units themselves. Thus, one common criticism of social network theory is that individual agency is often ignored although this may not be the case in practice. Precisely because many different types of relations, singular or in combination, form these network configurations, network analytics are useful to a broad range of research enterprises.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

When most people hear the term social network, they automatically think of online social networks. That's because online social networks, also known as social-networking sites, have exploded recently in popularity. Sites like MySpace, Facebook and LinkedIn account for seven of the top 20 most visited Web sites in the world. For many users, especially the fully wired Net Generation, online social networks are not only a way to keep in touch, but a way of life. Several features of online social networks are common to each of the more than 300 social networking sites currently in existence. The most basic feature is the ability to create and share a personal profile. This profile page typically includes a photo, some basic personal information (name, age, sex, and location) and extra space for listing your favourite bands, books, TV shows, movies, hobbies and Web sites. Most social networks on the Internet also let you post photos, music, videos and personal blogs on your profile page. But the most important feature of online social networks is the ability to find and make friends with other site members. These friends also appear as links on your profile page so visitors can easily browse your online friend network.Each online social network has different rules and methods for searching out and contacting potential friends. MySpace is the most open. On MySpace, you're allowed to search for and contact people across the entire network, whether they're distant members of your social network or complete strangers. However, you'll only gain access to their full profile information if they agree to become your friend and join your network. Facebook, which began as a college social network application, is much more exclusive and group-oriented. On Facebook, you can only search for people that are in one of your established "networks." Those networks could include the company you work for, the college you attended, or even your high school. But you can also join several of the thousands of smaller networks or "groups" that have been created by Facebook users, some based on real-life organizations and some that exist only in the minds of their founders. LinkedIn, the most popular online social network for business professionals, allows you to search each and every site member, but you can only access the full profiles and contact information of your established contacts - the people who have accepted an invitation to join your network.

II. RELATED WORKS

Leakage of personal information is a significant concern for social network users. Besides information propagation, some new attacks on OSNs such as Identity Clone attack (ICA) have been identified. ICA attempts to create a fake online identity of a victim to fool their friends in order to reap their private information which is not shared in public profiles. There are some identity validation services that perform users' identity validation, but they are passive services and they only protect users who are informed on privacy concerns and online identity issues. This paper starts with an explanation of two types of profile cloning attacks in OSNs. Afterwards, a new approach for detecting clone identities is proposed by defining profile similarity and strength of relationship measures. According to similar attributes and strength of relationship among users which are computed in detection steps, it will be decided which profile is clone and which one is genuine by a predetermined threshold. Finally, the experimental results are presented to demonstrate the effectiveness of the proposed approach. Detecting profile cloning attacks using a more accurate approach causes to improve the active users' safety and motivate OSNs' service providers to raise the level of security and privacy of social networks services.

There are two kind of profile cloning in OSNs: profile cloning and cross site profile cloning. In profile cloning the adversary builds clone profile from victim profile in the same OSN and sends friend requests to victims friends. The first attack is called Identity Cloning Attack (ICA), where the personal OSN information of an existing profile is used to create one or more clone accounts, claiming the same identity as the victim in a given OSN.

Detection of faked identities is a challenging work. The key challenges are first it is quite common that several people have similar names in real world; and hence their identities on OSNs may be similar. We cannot arbitrarily infer all the similar identities that have similar names as faked identities. Second, the characteristics of a faked identity have not been analysed and summarized.

A framework for detecting profile cloning in OSNs is presented. First the parts of faked identity are defined, then an approach for comparing two profiles based on attribute equality and friend network equality is used. Profile cloning detection has 3 steps: In the first step information from individuals profile will be extracted, in the second step

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

matching profiles will be found by searching user's attributes. At the end step, symmetry of each profile will be calculated and evaluated and the fake profiles will be detected.

After successful creation of user account, OSN authenticate the person via user credentials such as user name and password. While accessing own profile, the person can search for the person that he or she knows him or her personally. Thus people can communicate with each other on the OSN regardless the geographical location of them. In the last decades these popular OSN websites as well as the people facing the problem of a fake profile of a person having all the details of the person having the real profile in the same or different OSN that leads to the conflict between the people and the genuine profile owner. The clone profile is created by any anonymous person, called as attacker, it might be any person in the world and this term is known as identity clone attacks (ICAs).

The attribute similarity measure is used for calculating the similarity of two profiles' attributes. Here by using rank-sum weighting formula, the weight of each attribute is identified, as per the rank of the groups of attributes; with respective to domain, it is possible to be expressed. The other similarity measure is friend network similarity where the groups of friends are present in OSNs of that profile. The victim profile and clone profiles, similarity measure is calculated according to friends list, excluded friends list and recommended friend list of both profiles.

Profile Similarity measurement is based on attribute similarity and friend network similarity measurement of both profiles.
The detection process is will be as follows:
-The victim profile information such attributes and friend's network is extracted.
- Profiles in OSN will be searched based on attributes such as name same as victims name.
- The result of search is a set of clone profiles.
- The attributes and friend network will be extracted from each clone profile.
- Based on similarity measures of victim and clone profiles, profile similarity will be calculated.
-According to the calculation and measurements, the decision will be taken that which profiles are clone and which is real.

One of the most important challenges of observing friends' information is threatening users' security and privacy. An adversary can cause many problems by exploiting users' information. This data may contain users' financial information which adversary can use them to do identity theft attacks, or may contain users' medical background such as healthy status, diagnosis or treatment records. Recently, a new kind of attack which is named Identity Clone Attack is detected on OSNs that makes fake identities of specific users. The basic goals of the adversary in this attack are obtaining victim's friends' personal information by forging real user profile, and increasing trust among mutual friends to do more defrauding in the future. Two kinds of these attacks are already defined: first one is Single-Site Profile Cloning, and the next one is Cross-Site Profile Cloning. In the first attack, adversary forges the real user profile in the same social network and use this cloned profile to send friend request to users' friends.

III. EXISTING SYSTEM

The existing systems use the attribute similarity between the original profile and the fake profile that is being generated in order to find the fake one. All the existing methods suggest only avoidance of fake profile creation from server side. A huge collection of users datasets are being analysed for every profile generation in order to find the fake profiles.

3.1 Disadvantages

The ultimate motto of fake profile proliferation is not yet completely eradicated. Since this involves server side computation from datasets of existing users, this process is time consuming. A new profile cannot be created by an existing user even if he/she has forgotten his/her account details.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

IV. PROPOSED SYSTEM

Here, we propose a system that will detect fake profiles from client side (i.e. by users). The users will authenticate the acquaintances by a new form of questionnaire which varies from user to user. If any user is subject to many hits then it is identified as a suspicious profile and a warning is also given to the respective user. When the hit rate reaches a certain limit for a profile then it is removed from the database.This enables the avoidance of fake profiled intruder from gaining information. The main objective of the paper is to create an environment in which users' information are secured and are not prone to identity clone attacks. The questionnaire idea proposed here is very much useful in detecting the fake profiles and is helpful in eradicating the fake profiles.

The users are signed up and logged in into the online social networks. Then if the user wants to add another person as a friend he/she needs to send friend request along with few personal questions which is answered by the other user and new questions are sent by the user. The answers are verified and according to the answers, the originality of the user is calculated

4.1 Advantages

The proposed system will eradicated the fake profiles from having a genuine relationship with an existing user and thereby protecting one's information on social sites. This system also allows existing user to create a new profile and still connected to his/her friends even if he/she has forgotten his/her account details.

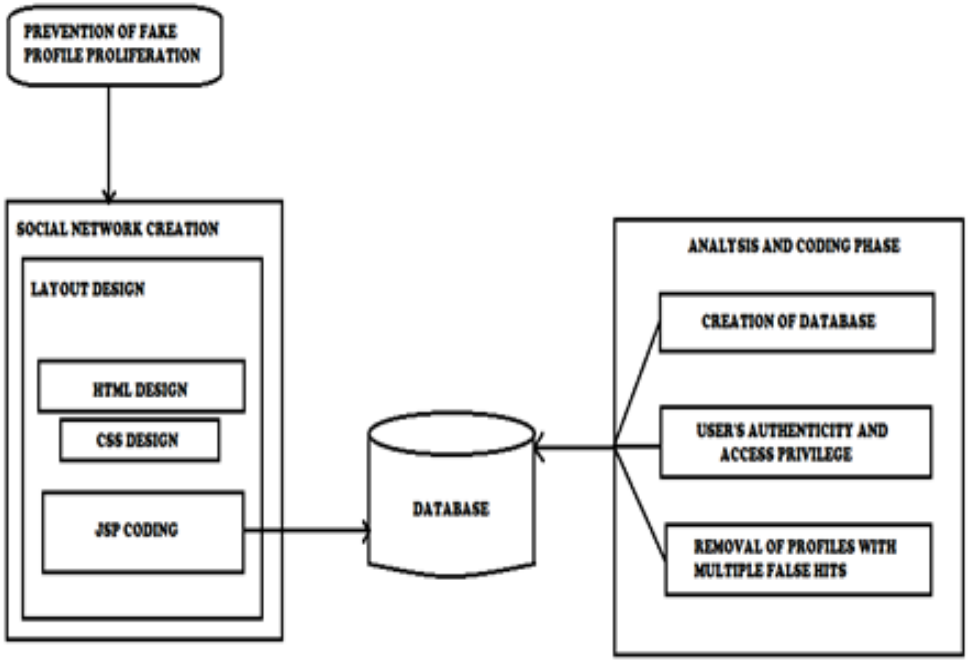

Figure 5.1 System Architecture

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

V.EXPERIMENTAL RESULTS

Figure 5.1 Login Page

Figure 5.2 Profile

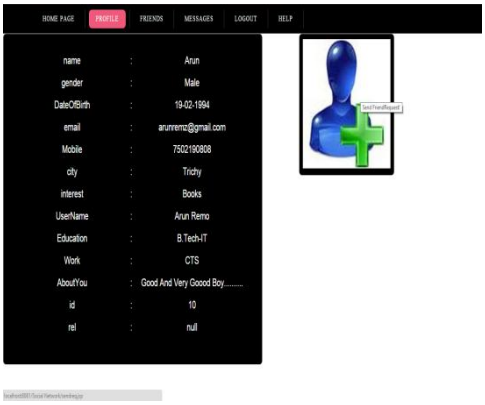

Figure 5.3 Send Friend Request

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Figure 5.4 Questions from user 1

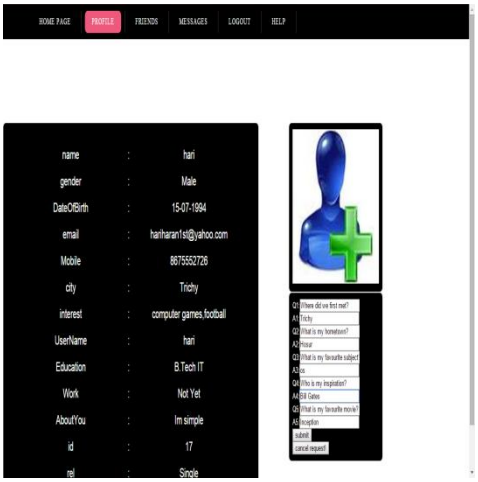

Figure 5.5 Answers from user 2

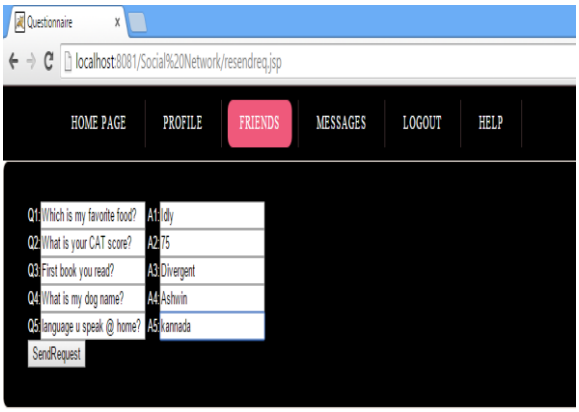

Figure 5.6 Questions from user 2

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

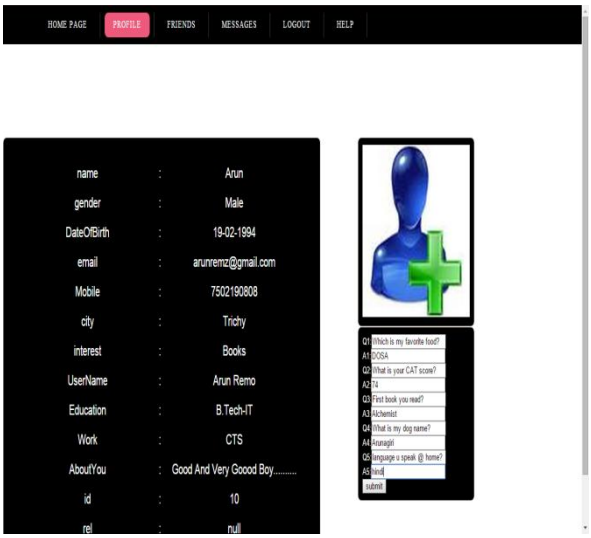

Figure 5.7 Answers from user 1

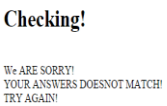

Figure 5.8 Warning for suspicious user

V. CONCLUSION

The proposed system overcomes the disadvantages present in existing system, that may include performance overhead in server side due to comparing the attributes of every new user with the whole database. This system concentrates more on prevention of fake profile proliferation than on prevention of fake profile creation.This system helps in identifying original users for creating another profile with same data existing in the server in case of them losing their password for their access, as the system does not takes attribute similarity into account.This system takes only questions as the authentication key. Future works may include pictures as authentication key and the comparison algorithm can be enhanced so that multiple varieties of answer, which are legitimate, can help in avoiding false positives which may occur in this proposed system.

REFERENCES

1. P. Joshi and C. Jay Kuo, "Security and Privacy in Online social network: A survey", In Proceeding of IEEE International Conference on Multimedia and Expo, pp.1-6, 2012.
2. L. A. Cutillo, R. Molva and T. Strufe, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real- Life Trust", IEEE Communication Magazine, pp. 94-101, 2013.
3. C. G. Akcora, B. Carminati and E.Ferrari, "Network and profile based measures for user similarities on social networks", In Proceedings of the 2012 IEEE 11th International Conference on Information Reuse and Integration (IRI), pp. 292-298, 2012.
4. C. Tanner, I. Litvin, A. Joshi, "Social networks: Finding highly similar users and their inherent patterns", Social Netw, 2012.
5. M.Conti, R.Poovendran, M.Secchiero ,"FakeBook: Detecting Fake Profiles in On-line Social Networks",2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.
6. Acquisti (2005), 'Information Revelation and Privacy in Online Social Networks.' Paper presented at of the ACM workshop on Privacy in the electronic society, November 7, Alexandria, USA.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

7. Bilge L, Strufe T., Balzarotti D., Kirda E.: All your contacts are belong to us: automated identity theft attacks on social networks. In: 18th international Conference on World wide web, Madrid, Spain (2009)
8. Kontaxis. G, I. Polakis, S. Loannidis and E.Markatos (2011). 'Detecting Social Network Profile Cloning.' Paper presented at the Ninth Annual IEEE International Conference on Pervasive Computing and Communications, March 21-25, in Seattle, WA, USA.
9. D. Boyd and N. Ellison, "Social network sites: Definition, history, and scholarship", IEEE Engineering Management Review Journal, vol. 38, no. 3, pp. 16-31, 2010.
10. L. Jin, H. Takabi and J. Joshi, " 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, 2011.
11. S. Schechter, S. Egelman, and R.W. Reeder, "It's not what you know, but who you know: a social approach to last resort authentication", In Proceedings of the 27th International Conference on Human Factors in computing systems,pp. 1983-1992, 2009.
12. Q. Cao, M. Sirivianos, X. Yang and T. Pregueiro, "Aiding the Detection of Fake Accounts in Large Scale Social Online Services", In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, pp. 15-29, 2012.