International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Providing Security to Social Media using Unique Identification

Pranav Jambare, Anup Kulkarni, Neha kharat, Prof. Suvarna Ghule
Department of Computer Engineering, Pune, Maharashtra, India

ABSTRACT
Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Facebook, Myspace, or Twitter), storing and sharing a wealth of personal information. This information, as well as the possibility of contacting thousands of users, also attracts the interest of cybercriminals. For example, cybercriminals might exploit the implicit trust relationships between users in order to lure victims to malicious websites.

This invention relates to the field of Social Media where a system is built to restrict scammers from creating fake profiles or pages. If misbehave is occurred by any account user the social media is able to track and identify the user easily as its information is stored in database. As there are many social media around us, but none of them assured to have verified user. To make the user verified or authenticate this system is implemented.

Keywords: *component; formatting; style; styling; insert*

I. INTRODUCTION

A. ***About social media.***

Over the last few years, social networking sites have become one of the main ways for users to keep track and communicate with their friends online. Sites such as Facebook, Myspace, and Twitter are consistently among the top 20 most-viewed web sites of the Internet. Moreover, statistics show that, on average, users spend more time on popular social networking sites than on any other site. Most social networks provide mobile platforms that allow users to Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. The tremendous increase in popularity of social networking sites allows them to collect a huge amount of personal information about the users, their friends, and their habits. Unfortunately, this wealth of information, as well as the ease with which one can reach many users, also attracted the interest of malicious parties. In particular, spammers are always looking for ways to reach new victims with their unsolicited messages. This is shown by a market survey about the user perception of spam over social networks, which shows that, in 2008, 83% of the users of social networks have received at least one unwanted friend request or message.

B. ***Problem to be solved.***

Now days everyone is using social media like Whatsapp, Facebook and Instagram etc. Many of us are feeling unsecure while using social media, some of them are facing harassment using social media. Creating fake profiles and pages is now days so easy as we able to provide fake information. The information which is provided by the user is not verified by anyone so it is not possible to trust anyone on social media. Scammers can used information and try to damage the image of the victim. Social media designed multiple technique for solving problem of the authenticate user, none of them are promised to give the verified users only. Mobile authenticate, Email authenticate etc. are the ways to authenticate user but this information can be stolen or can be used fake mobile no or email. With this system, a planned operation is designed where the drawbacks of the previous system related to fake ids, misbehavior and scamming have to be resolved. Here finger print is used for unique identification. Finger print is matched

to the database of adharcard, if the finger print matches to the database of the adharcard then only the user able to create the account on the social media.

C. Objective of project.

The aim of the invention is to offer a system, which eliminates drawbacks of the prior solutions and provide authenticate user to the society. The user's finger print will match using algorithm which is resent in the bit image for in the database. The objective of the project is to restrict the scammer to creating of the fake profiles or pages. It is very easy to create fake ids on the Facebook. Scammer can easily stole information and harass the user of the social media. As it is so easy for scammer to do this, to avoid scamming by the scammer the project is implemented. Further another objective of the project is the as we are using the finger print scanner, which is used as hardware device to store the finger print in the database. To make the device more feasible we can use the retina in future. It will be used for the authentication of the users.

The other objective is the categorized social media. In which it provides the users to choose in which category the user wants to be. Category can be 1.VIPs 2.FriendZone 3.Public which provides facility as we choose it. If the user having millions followers or celebrity it can be VIP account we provide some more feature. If the user wants to see only the things which are related to the friends of the user only then it will be in FriendZone.If the user loves to make friends from anywhere then the user can choose Public category.

II. RELATED WORK

The success of social networks has attracted the attention of security researchers. Since social networks are strongly based on the notion of a network of trust, the exploitation of this trust might lead to significant consequences. In 2008, a Sophos experiment showed that 41% of the Facebook users who were contacted acknowledged a friend request from a random person . Bilge et al. show that after an attacker has entered the network of trust of a victim, the victim will likely click on any link contained in the messages posted, irrespective of whether she knows the attacker in real life or not. Another interesting finding was reported by Jagatic et al. . The authors found that phishing attempts are more likely to succeed if the attacker uses stolen information from victims' friends in social networks to craft their phishing emails. There are also botnets that target social networks, such as koobface .Brown et al. showed how it would be possible for spammers to craft targeted spam by leveraging the information available in online social networks. As for Twitter, Krishnamurthy et al. studied the network, providing some characterization of Twitter users . Yardi et al. ran an experiment on Twitter spam. They created a popular hashtag on Twitter, and observed that spammers started using it in their messages. They also discuss some features that might allow one to distinguish a spammer from legitimate users, such as node degree and frequency of messages. Another work that studied social network spam using honey-profiles was conducted by Webb et al. in 2008 . For this experiment, 51 profiles were created on MySpace, which was the largest social network at the time. The study showed a significant spam activity. The honey-profiles were contacted by 1,570 spam bots over a five-month period. Compared to their work, our study is substantially larger in size and covers three major social networks, and the honeypot population we used is representative of the average population of these networks, both from an age and nationality point of view. Moreover, we leverage our observation to develop a system able to detect spammers on social networks. This system has detected thousands of spam accounts on Twitter, which have been subsequently deleted.

D. Background of social networks

Social networks offer a way for users to keep track of their friends and communicate with them. This network of trust typically regulates which personal info rmation is visible to whom. In our work, we looked at the different ways in which social networks manage the network of trust and the visibility of information between users. This is important because the nature of the network of trust provides spammers with different options for sending spam messages, learning information about their victims, or befriending someone (to appear trustworthy and make it more difficult to be detected.

CONCLUSION

Social networking sites have millions of users from all over the world. The ease of reaching these users, as well as the possibility to take advantage of the information stored in their profiles, attracts spammers and other malicious users.

In this paper we have solved the problem of spam accounts by preventing the creation of spam accounts

REFERENCES

1) J. Alqatawna, "An adaptive multimodal biometric framework for intrusion Detection in online social networks," *IJCSNS International Journal of Computer Science and Network Security*, vol. 15, no. 4, pp. 19–25, 2015.

2) F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida, "Detecting spammers on Twitter", *Proc. Collaboration +Electron. Messaging Anti-Abuse Spam Conf. (CEAS)*, vol. 6, pp. 12, 2010.

3) X.Hu,J.Tang,Y.Zhang,H.Liu,Socialspammerdetect ioninmicroblogging,in: Proceedings oftheTwenty-ThirdInternationalJointConferenceonArtificial Intelligence,AAAIPress,Beijing,China,2013,pp.26 33–2639.

4) C. M. Bishop, Pattern recognition and machine learning, New York, NY, USA: Springer, 2006.

5) Mccord Michael, M. Chuah, "Spam detection on twitter using traditional classifiers" in Autonomic and trusted computing, Berlin Heidelberg: Springer, pp. 175-186, 2011.

6) S. N. Yanushkevich, "Synthetic Biometrics: A Survey," in International Joint Conference on Neural Networks, 2006. IJCNN '06, 0-0 0, pp. 676-683.

7) B. Amberg and T. Vetter, "GraphTrack: fast and globally optimal tracking in videos".proc of IEEE International Conference on Computer Vision and Pattern Recognition, 2011.

8) L. Hong, Y. Wan, A. K. Jain, "Fingerprint image enhancement: Algorithms and performance evaluation", *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777-789, 1998

9) Reza Nejatpour, Ali Asmari Sadabad, Ali Akbar Akbari, "Automated weld defects detection using image processing and cad methods", *2008 ASME International Mechanical Engineering Congress and Exposition*, October 31-November 6, 2008.

10) Beach, M. Gartrell, R. Han, "q-Anon: Rethinking Anonymity for Social Networks", *IEEE Second International Conference on Social Computing*, 2010.

11) F. Beato, R. Peeters, "Collaborative joint content sharing for online social networks", *IEEE International Workshop on Pervasive Computing and Communications*, 2014.

12) D. M. Boyd, N. B. Ellison, "Social Network Sites: Definition History and Scholarship", *J. Comp.-Mediated Commun.*, vol. 13, no. 1, pp. 210-230, Oct. 2007.

13) S. Kanika, R. S. Chadha, "Captcha Generation for Secure Web Services", *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 10, April 2013.

14) H. Gao, J. Hu, T. Huang, J. Wang, Y. Chen, "Security Issues in Online Social Networks", *IEEE Computer Society*, vol. 15, pp. 56-66, 2011.

15) Evmorfia N. Argyriou, Aikaterini A. Sotiraki, Antonios Symvonis, "Occupational Fraud Detection Through Visualization", *Proc. of the 11th IEEE Intelligence and Security Informatics (ISI 2013)*, pp. 4-7, 2013.