ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 06, pp.32435-32438, June, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

DETECTING DECEPTION IN ONLINE SOCIAL MEDIA USING PHYSICAL CHECK MECHANISM

***,[1]Alka and [2]Harjot Kaur**

[1]Student (M.TECH), Department of Computer Science, GNDU RC, Gurdaspur, Punjab, India
[2]Professor, Department of Computer Science, GNDU RC, Gurdaspur, Punjab, India

ARTICLE INFO

Article History:
Received 23rd March, 2016
Received in revised form
20th April, 2016
Accepted 06th May, 2016
Published online 15th June, 2016

Key words:

Deception Detection, Social Media,
Physical Check Mechanism.

ABSTRACT

The technology is allowing the users to communicate with each other. One of the most common way is to use the social networking like Facebook. The social networking sites will allow the users to create the account without any verifications and validation. As more and more user communicate with each other also causing the problem like deception. This is caused due lack of standards followed by the social networking sites. In the proposed paper a physical check mechanism is introduced with the help of which deception is going to be detected. This mechanism is also termed as background check mechanism.

Citation: Alka and Harjot Kaur, 2016. "Detecting deception in online social media using physical check mechanism", *International Journal of Current Research*, 8, (06), **32**435-**32**438.

INTRODUCTION

The people now days do not have time. They communicate with each other by the use of internet. Internet provides number of mechanisms by which users can communicate with each other. Most common mechanisms which are used involve social media. Social media will help in establishing linkage between the different communities of users. The social media has allowed many users to share their views and also help the users around. But with the advent of the technology problems also start to appear. The main problem which is caused with the social media is deception. The deception model is then created in order to detect the problems with the online user accounts. Some users can have multiple accounts or some wrong information is provided by them. This paper describe that the deception is deliberate attempt to mislead the others. The deception will be such that the other user will not able to detect the falsifying information provided by the malicious users. The privacy of the users will be at stake if deception takes place.

Online deception

The deception will cause falsifying information to be transmitted from source to the destination. Deception can be at the smaller scale or at the large level. Deception can cause damages both at physical and mental level. With the advent of the technology large number of users is using the internet. There are number of social networking sites which user use in order to interact with each other. They share their thoughts, feelings, experience etc. some information which they share may be sensitive in nature. Also there is some private information which is presented over the social media. Deception which takes place over the internet is under the category of Online Deception.

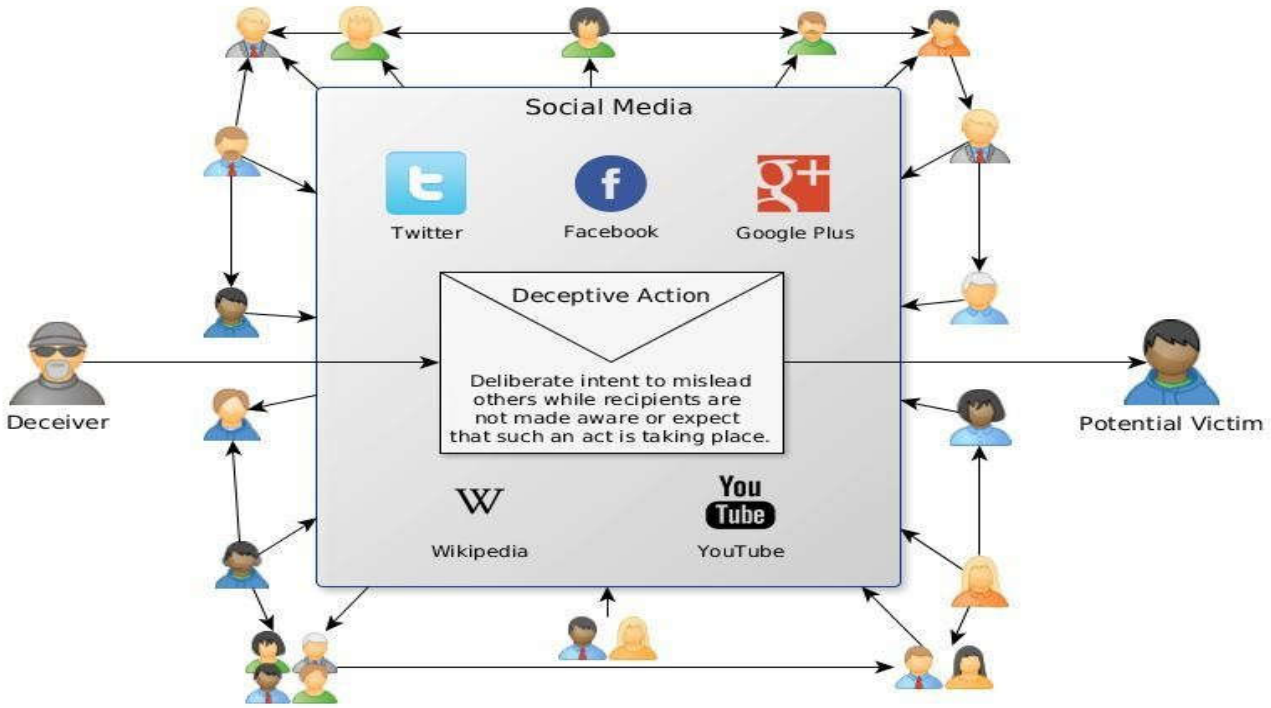
Potential victim

When falsifying information is provided by the users then the other users which are affected by the deception are potential victims. General technology behind the deception will be online social media. The sites like Facebook are just concentrating on increasing the size of their database. They have less focus on the information provided by the users rather they are more concerned about the size of the database. This is causing more and more deception on the network. The users who are suffering from the falsifying information are known as victims.

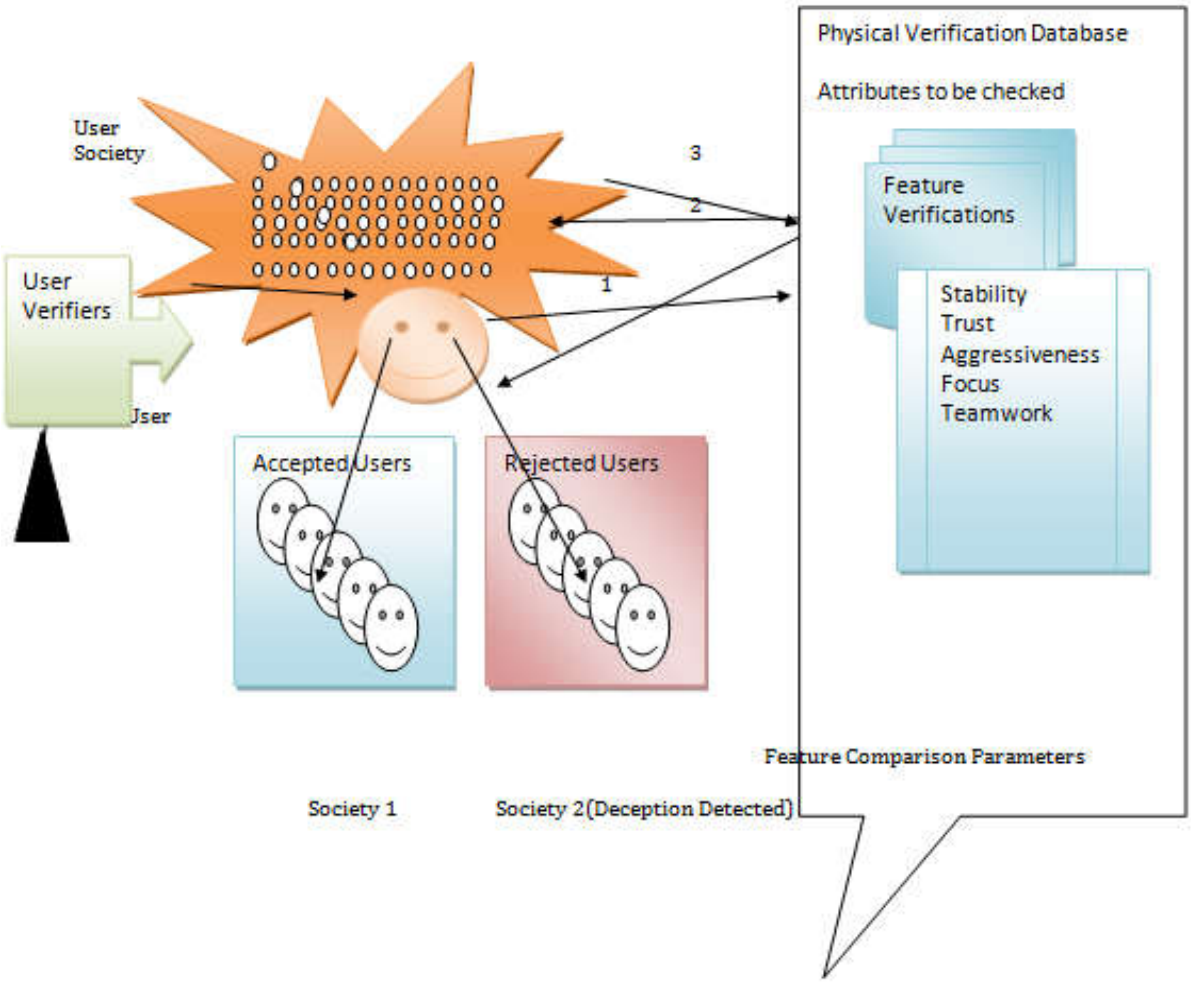
Proposed model

The proposed model helps in reducing the deception over the Online Social Media. It is close to impossible to remove the deception over the social media. But it is possible to reduce the deception over the social media. The proposed model is as shown as follows

Corresponding author: Alka,
[1]Student (M.TECH), Department of Computer Science, GNDU RC, Gurdaspur, Punjab, India.



Entities involved in online deception



The user of the online social network will create their accounts in order to access the networks. The account verification process is not hard. This will cause deception in the social networks. The proposed model try to resolve the problem associated with the social network users. There are following steps which are associated with the proposed system.

1) In the proposed system first of all user will appear. The information about the user will be passed to the user verifier.
2) There exist user societies with which the information which presented by the user will be compared. If the user already exists then user is not further created. User has to go through the process of user verification again.
3) After the second step user has to go though physical verification process. The list of attributes is listed with which user information is validated. This information is used if the malicious activity is detected.
4) On the basis of the information two groups are formed. First group indicate the validated users and the second group indicates the deception which is caused by the users.

Proposed algorithm

The proposed algorithm will reduce the deception over the social media. The physical check mechanism is used in this case. If the falsifying information is provided then concept of jailed will be used. Which means is falsifying information is provided then legal action can be taken against that user. Also validity of user can be checked by verifying the information physically by calling or through the e-mail.

The algorithm is step by step representation of the steps required to solve the problem. The proposed algorithm is as follows

Algo Check()
// This algorithm build a network in which information is received from the user(I_u) and then validation mechanism verify the data
1)Record Length of the Record(R_f) in I.
2)Loop until I>0
a)Make user pass through the series of Questions(Q).
b)If InValid(Q) then
B1) Declare user falsifiy(F) and return
Else
B2) Goto c
End if
c)Perform Background(B) Check
d)If IsValid(B) then
D1) Declare user Valid and goto step e.
Else
D2) Declare user invalid.
End of if
e)I=I-1
End Loop
3)Stop
The above algorithm suggests that the user has to go through series of steps before user will be able to create account over the network. The questionnaires are also used so that validity of the user can be verified.

Conclusion and Future work

The proposed model concentrates on the mechanism for reducing the deception over the social media like Facebook. In order to do so background check mechanism or physical verification mechanism will be used. User will provide the information and that information will be verified against the certain checks. Phone calls and emails can be sent to the appropriate college or schools or the firm in which user works. This mechanism will takes time which can be the disadvantage of the system but deception over the social media can be significantly reduced using the above said mechanism. In the future time consumption can be reduced by fully automating the system of verification.

REFERENCES

Brenner J. and Smith A. 2013:15. 72% of Online Adults are Social Networking Site Users.; Available at: http://pewinternet.org/Reports/2013/social-networking-sites.aspx.

Buller DB. and Burgoon, JK. 1996. Interpersonal Deception Theory. *Commun Theory*, 6(3):203–242.

Burgoon J, Adkins M, Jensen JKML, *et al*. 2005. An Approach for Intent Identification by Building on Deception Detection. *Syst Sci 2005 HICSS '05 Proc 38th Annu Hawaii Int Conf.*, 21a–21a.

Castelfranchi C, Tan Y-H. 2001. The role of trust and deception in virtual societies. *Syst Sci., Proc 34th Annu Hawaii Int Conf*, 8 pp.

Dai C, Rao F-Y, Truta TM, Bertino E. 2012. Privacy-preserving assessment of social network data trustworthiness. *Collab Comput Networking, Appl Work (CollaborateCom), 8th Int Conf*, 97–106.

Damphousse KR, Pointon L, Upchurch D, Moore RK. 2007. *Assessing the validity of voice stress analysis tools in a jail setting.*

Dando CJ, Bull R. 2011. Maximising Opportunities to Detect Verbal Deception: Training Police Officers to Interview Tactically. *J Investig Psychol Offender Profiling*, 8(2):189–202. Available at: http://dx.doi.org/10.1002/jip.145.

Donath JS. 1999. Identity and deception in the virtual community. In: Smith MA, Kollock P, eds. *Communities in Cyberspace*. Routledge.

Ekman P. Deception, Lying and Demeanor. 1997. In: Halpern DF, Voiskounsky AE, eds. *States of Mind : American and Post-Soviet Perspectives on Contemporary Issues in Psychology: American and Post-Soviet Perspectives on Contemporary Issues in Psychology*. Oxford University Press, 93–105.

Galanxhi H, Nah FF-H. 2007. Deception in cyberspace: A comparison of text-only vs. avatarsupported medium. *Int J Hum Comput Stud*., 65(9):770–783.

Grazioli S, Jarvenpaa SL. 2000. Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *Syst Man Cybern Part A Syst Humans, IEEE Trans*, 30(4):395–410.

Hirschberg J, Benus S, Brenier JM, *et al*. 2005. Distinguishing deceptive from non-deceptive speech. In: *Interspeech,* Proceedings of Eurospeech'05; 1833–1836.

Hoglund G, McGraw G. 2007. *Exploiting Online Games: Cheating Massively Distributed Systems*. First. Addison-Wesley Professional.

Humpherys SL, Moffitt KC, Burns MB, Burgoon JK, Felix WF. 2011. Identification of fraudulent financial statements using linguistic credibility analysis. *Decis Support Syst*., 50(3):585–594.

Kaplan AM, Haenlein M. 2011. The early bird catches the news: Nine things you should know about micro-blogging. *Bus Horiz*., 54(2):105–113.

****