Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A Survey on detecting Identity Deception in Social Media Applications

Antu Mary Kuruvilla[1], Saira Varghese[2]
[1]*Computer Science, Toc H Institute of Science & Technology*
[1]*Computer Science, Toc H Institute of Science & Technology*

Abstract—Today the current landscape of the internet where there is a large number of social networking sites and also collaborative websites like Wikipedia concern about fake users keeping multiple accounts is of mainly give importance. Many of all those sites which allow users easily create an account and start collecting the content. Social media system such as collaborative project's single user constantly creates many accounts with different account names not long after a block has been applied. Then the blocked deceiver who login again with multiple accounts is called sockpuppet. Current mechanism for detecting deception is based on human deception detection such as text. Mainly these methods have large detection accuracy, but it cannot be applied in huge databases with large data's. So they are computationally inefficient and unsecured. There should be an efficient method for detecting identity deception by using Nonverbal in the social media framework. Thus all these methods increase high detection accuracy and they data's are secured. Close examination and monitoring of data's on these methods which finds out that it can be applied to any social media framework.

Keywords- Deception, sockpuppet, security, nonverbal behavior, verbal behavior

I. INTRODUCTION

Social Networking sites and open collaborative websites are having become much admired in present time. There should be an unmatched flow of transmission of data through these online media through chats, blogs and collaborative conservation of data's. Social media is shows a powerful tool while considering its potential of reaching a group of people at a single place at very brief duration. The outcome of social media for people is that, it is a medium for people to show their ideas and thoughts to a large mass of people at very short time. Social media can be defined as a group of Internet applications that developed on the intellectual and scientific foundations of web and that allow the user creation and also the exchange of user designed content. So there should be always a malicious threat occurs to such sources from malicious minds like hackers, information vandalizes and hate dealer.

An example for collaborative project is Wikipedia, which emerged as the world's largest crowd-sourced encyclopedia. At a time any user can easily register with Wikipedia by providing fewer details. All users can edit articles in Wikipedia and also make comments on discussion pages and also report abuse about the malicious users. This type of broadcast collaborative project is extremely vulnerable to vandalism and malicious behavior [1].

Some Wikipedia users create multiple accounts and use them for various malicious purposes such as creating fraudulent articles, damaging existing article text etc. So these deceptions cannot easily detected by any authority. Numerous methods have been proposed that can help in detecting multiple accounts owned by the same persons but their victory varies in terms of computational efficiency depending on the availability of the suitable data [1][2], additionally the past methods have mainly

focused on detecting deception through human deception detection mechanism, which shows positive result in offline sites[3].

The proposed method for detecting identity deception by a single user is based on using Nonverbal behavior. The rest of the work is organized as follows. In Section II, explains related work of survey. In Section III, conclusion of the survey conducted.

II. RELATED WORKS

The social networking users are increasing exponentially from the upcoming years. As stated to Wikipedia's scheme, single user is generally to create only single user account. Whenever, Wikipedia does not impose the single user single account rule through technical means. Thus the results of users who login to system are free to create multiple accounts they want to create. When a user produces a new account for spiteful activities it is called a sockpuppet. This effort of producing single user accounts has led malicious attacker to create multiple accounts and use them for diverse motive, vary from block shirking, false most belief objection and ballot pile [4].

One of the crucial applications of the sockpuppet table is to develop an automated tool for sockpuppet detection in Wikipedia. At the present, the process for identifying sockpuppets is human detection mechanism and involves major experience from the chief. In many occasion, special Wiki chief with IP-address verifying privileges such as check users have to be involved to check user IP addresses of the spurious articles. Without knowing the IP addresses, the head of media need to trust on their occurrences in dealing with sockpuppets to manually detect sameness in text (writing style) and behavior.

Deception is serious problems which are mainly occurring in networking sites. It can be mainly in variety purposes and it is highly viable to provide false information not only about the contents of a text but also the background or beginning. Taking an example, a friendly invitation can become sexual harassment when sent from the malicious person, and very few abnormal notes are signed by some authors. Latest research into stylometry has explains that it is practical method to detect authors based on their writing pattern such as text, but it is same as practical for authors to use a knowing deceptive style, either bewildering their own style or copying that of any writer, with a big chance of deleting recognition [5].

Stylometry authorship attribution judging the author of a document by statistical perusal of its contents has its origins in the 19th century (Mendenhall, 1887; de Morgan, 1851), but has experienced gigantic rebirth since the work of (Mosteller and Wallace, 1964) and the dawn of the data uprising. With the speedy extension of digital texts and the increasing need to prove or test the refusal of questioned digital data's this is clearly an area with many probable applications.

2.1 Online Deception

Online deception is one of the serious complications in social media websites. Social media organizers can also be sorted based on social presence or media richness and self presentation or self memorandum. Social presence can again be influence by the affinity and excitement of the medium in which the transmission takes place while media richness describes the quantity of information that can be rely at a given time. Self presentation describes the power that users have in representing themselves whereas self memorandum determines revealing one's information whether willingly or by unwillingly. It is not amazingly that many level of difficulty in attaining online deception properties is described by using many factors such are associated mainly with the attacker, the social

media services, the deceptive act and the potential sufferer. These entire elements will also describe how easy and difficult it is for a deceiver to capture in online deception media's. High difficulty in reaching deception may discourage potential deceivers while low difficulty may be seen as an easy method to deceive others [6].

2.2 Cyber bullying

Cyber bullying or bullying through information and transmission technology tools such as the internet and mobile phones is a serious problem of developing concern with students. Cyber bullying performance is not taking place on school sites, but dangerous effects are knowledgeable by users of cyber bullying in schools zone [7]. Cyber bullying tools are email, constant messaging, pictures etc. Cyber bullying actions may include the wide distribution of degrading information about each and every individuals, also their families and friends, secret values are calculated for the sender only and also pictures taken with or without accord of the subject, videos clips taken without accord or made by the users for a select audience and social prohibition can also be practiced on users by cyber bullies affecting groups to block someone from their list of friends.

A method for detecting deception is by using blob analysis of head and hand. A behavioral signal of deception and behavioral state are extremely tough for users to investigate and makes an output. Blob analysis is a method for investigating the actions and variation of the head and also hands based on the recognition of skin color is presented. This approach also is updated with numerous skin tones [8]. Blob analysis may extracts hand and face parts using the color spreading from an image order.

A Look-Up-Table called LUT with three color ingredients such as red, green, and blue is also been developed root on the color spreading for body parts. This three-color LUT, defined as 3D LUT, it is used for any analysing and is formed using skin color examples. After withdrawing the body regions such as hand and face from an image sequence then the system figured out elliptical blobs identifying candidates for the face and hands. The 3-D LUT can also be incorrectly recognizing candidate regions which are similar to body color. All these candidates are not taken into account through great segmentation and differentiating the sub part of the face and also hand candidates. Then the most face and hand field in a video part are to be identified.

Mainly in every framework each comment made by a user is to be examined as a document and thus each of these comment be elected by an instance a sample of the classification mission. There are two steps methods explains such gather predictions from the classifier on each comment. Second step takes the augury for each of the comment and integrating them in a greater voting representation to predict a final resolves to separate account [1].

Autonomous Deception Detection is a framework for Computer-Aided Deception Detection building on the Interpersonal Deception Theory (IDT) of human interpersonal communication research and also a text-processing method for smoothening deception analysis of text-oriented data exchange [9]. A transition diagram based scheme is proposed to represents the dynamic expansion of an interpersonal exchange with a sender and receiver situated on the IDT-based operation schema. The software is always been make effective to design a deception detection agent to process textual data. Deception detection also is interpreted as a process of process verification.

III. PROPOSED SYSTEM

The proposed method in the survey is detecting deception by using Nonverbal behavior of each and every user. Here considering an example for open collaborative project such as Wikipedia. It is a collaborative project where large mass of people can efficiently signup, create or edits articles and

also made comments. By transferring limited amount of information for login page and thus every people can easily added fake data to each article, also create malicious articles and provide false information to recipient. The nonverbal behavior explains about set of activities which are carryout by the fake persons. Detecting nonverbal behavior is by using any of machine learning algorithms such as support vector machine algorithm. Wikipedia also contains page revision logs such as activity logs files. Each user has separate activity log files, which contains activities that are carryout by each user such as articles created, articles deleted, time taken to make a process etc.

3.1 Nonverbal Behavior of Users

Non verbal explains about activities done by each user separately.

- Number of articles generates
- Number of searches done for same articles
- Number of bytes added and also removed
- Number of times same spelling mistakes carryout constantly
- Time taken between each revision

To evaluate the performance of this detecting mechanism, detection accuracy is to be calculated. Detection accuracy involves check out detecting rate of every mechanism in nonverbal behavior. Detecting rate can be evaluated by the help of 3 methods.

- Recall
- Precision
- F-measure

IV. CONCLUSION

The social media always keeps an evolving and continues to be enlarged with a various set of tools and also technologies that malicious users can be used. When the original part that divides the deceiver and the user may always see high and thus the damage that can be done is away from insignificant. Individuals, organizations and governments are at risk. Identity deception is always being a serious issue in online and offline world. By analyzing the survey report understand that by using verbal and nonverbal behavior of user can easily detect the sockpuppet with limited amount of time.

REFERENCES

[1] Thamar Solorio, Ragib Hasan and Mainul Mizan, “A Case Study of Sockpuppet Detection inWikipedia”, Proceedings of the Workshop on Language in Social Media (LASM 2013),pp. 59-68, 2013

[2] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, “Automatically detecting criminal identity deception: An adaptive detection algorithm,” IEEE Trans. System., Man, Cybern. A, System. Humans, vol. 36, no. 5, pp. 988–999, Sep. 2006.

[3] T. O. Meservy et al.,“Deception detection through automatic, unobtrusive analysis of nonverbal behavior,” IEEE Intell. Syst., vol. 20, no. 5, pp. 36–43, Sep./Oct. 2005.

[4] Thamar Solorio, Ragib Hasan and Mainul Mizan, “Sockpuppet Detection in Wikipedia: A Corpus of Real-World Deceptive Writing for Linking Identities,” Cryptography and Security (cs.CR); Computers and Society (cs.CY) arXiv preprint arXiv:1310.6772, Oct 2013, pp.1355-1358.

[5] Sadia Afroz, Michael Brennan and Rachel Greenstadt, “Detecting Hoaxes, Frauds, and Deception in Writing Style Online,” IEEE Symposium on Security and Privacy, 2012. pp. 461-475.

[6] M. Tsikerdekis and S. Zeadally, “Online deception in social media,” Commun. ACM, vol. 57, no. 9, Sep. 2014.

[7] Christine Suniti Bhat, “Cyber Bullying: Overview and Strategies for School Counsellors, Guidance Officers, and All School Personnel”, Australian Journal of Guidance & Counselling Volume 18 Number 1, pp. 53–66, 2008

[8] S. Lu, G. Tsechpenakis, D. N. Metaxas, M. L. Jensen, and J. Kruse, “Blob analysis of the head and hands: A method for deception detection,” in Proc. 38th Hawaii Int. Conf. Syst. Sci. (HICSS), 2005, p. 20c.

