DEFENDING MECHANISM FOR SOCIAL NETWORKS FROM CYBERBULLYING AND ONLINE GROOMING ATTACKS

[1]Anuja B. Pokharkar, [2]Shubham D. Shelake , [3]Nalini D. Kate, [4]Arun C. Murbade

[1] *Student, Computer Engineering, SGOICOE Belhe, Maharashtra, India*
[2] *Student, Computer Engineering, SGOICOE Belhe, Maharashtra, India*
[3] *Student, Computer Engineering, SGOICOE Belhe, Maharashtra, India*
[4] *Student, Computer Engineering, SGOICOE Belhe, Maharashtra, India*

ABSTRACT

As per the technology is developed the use of internet increases due to the necessity of world. The common growth of the social networking sites is done belongs to the communication world. With the help of these social Networking sites peoples are indirectly connected to each other in the world in minimal time spam, usually they express their point of view about some things, their feelings, emotions and opinions which may include public or private talks. Popularity of the social sites cause most important rise in aggressive behavior, giving birth to one of the most serious problem called online Grooming and cyber-bullying. There are number of the social networking users would have come through a worst e-day understanding .The victims of cyber-bullying, mostly being the youngsters, go through deep scars which has led to miserable attempts in many cases. Agenda for this Watchdog application chasing the aim to discover and classify the above-mentioned threats to develop the situation. Threat signs are recognized by social media analysis, text mining and image analysis techniques permitted to raise awareness about continuing attacks and to grant assistance for further actions.

Keyword: *Online Grooming attack, Cyberbullying attack, Abusive Text detection, Abusive Image Detection.*

1. INTRODUCTION

Nowadays, as the use of internet has increased, the Social Networking Sites such as Twitters, Facebook and Google+ etc. are main aspects in it. Social media is defined as the interactions among people in which they create, share and exchange information and ideas in networks and virtual communities. One of the popular and most famous social networks is Facebook in which more than billions of active users daily using it. A multiple of examples exist which demonstrate that how Facebook affect our daily life. Users can post information about themselves, tell people what they've been up to, chats, photos and play games using Facebook. There are many applications of Facebook that make users to get in contact with other users. Examples of such applications are 'RelationBook' (which provides information to users which of their friends are currently single or not) or SpeedDate' (which consist of chat functionality and facilitates the meeting of new contacts).

Facebook also touches sensitive areas and most intimate. The App 'Bang With Friends offers the possibility to mark friends in order to show interest in sexual relationships. All these apps need the confirmation of all persons which are contributing but focus that Facebook is most widely used and provides platform to beginning any form of relations. Grownups are able to draw the track and are more attentive of the danger social networks carry long. By distinction, children or teens often have wrong threat perception and are frequently curious to explore the new parameters without the ability to consider potential risks. Traditional threats of cyber or attacks have

communication organization and battered information that mostly result in economic loss. Generally, launching these attacks needs an intellectual skillfulness. The speedy growth of social media is giving rise to new types of threats that spread over from the cyber world into realistic life.

A survey [1] has shown that 78% of German teenagers between 12 and 17 years commonly use Facebook. So, it is no huge issue that social communication for large number of adolescence is being online and thereby strongly effects their enhancement.

1.1 Cyberbullying Attack

Cyberbullying is an attack depends on frightening, intentionally insulting, awkward or annoying people via mobile phones or on the internet over social networking websites, instant messaging and emails application. Studies show that this attack normally experienced by teenagers. It occurs that the victim and culprit know each other in real life in most cases. Cyber bullying is not taken place directly by face to face and even publics don't know the identity of the individual targeting them, but cyber bullying is no different from any other methods of bullying; the impact is no less devastating and the behavior is the similar. As insults, misinformation and rumors can be quickly disseminated to a large number of audience, Cyberbullying is intentionally hurting for victims in social networks. It is more or less impossible to delete it once posted, secretive information is spread. Because of the digital media in ubiquity. Though it is likely to eliminate the given information, it still stay and exist in the thoughts of readers. Cyberbullying attacks can happen at any point in while and usually last for long period of time [2]. Thus, victims cannot even feel secure and protected in their own firm.

The significances of physical or mental manipulation for adolescents are studied and contain despair, social separation and tries to suicide. Cyber bullying can carried out at anywhere, anytime that young people and children have the use of knowledge. Techniques used by committers through beside insulting text messages, comments or posts, photo and video functions in social networks are developed for cyberbullying attacks. Therefore, compromising pictures and videos and with sexual or violent content, like Sexting or Happy Slapping, can be shared.

1.2 Online grooming Attacks

Online grooming attacks is an mature who tactics children online with the goal of acting sexual actions which contains sexual discussion, unclothing in front of a webcam and lastly a physical gathering for sexual irritation and/or abuse. In many conditions, grooming online is faster and unidentified and results in believing by below undeveloped person i.e. children's social media's friend which is online faster than someone they had just met straight 'face to face'. Those determined on sexually frustrating and spoiling children can simply get information about them and they are able to hide their unique identity, age and gender. Groomer might try to achieve belief with the help of their profile pictures which is false, acting to have same interests, proposing gifts and saying pleasant things to the child. This is a method used by people with a sexual curiosity in children to attempt to engage them in the acts of sexual whichever over the online or actually offline. The likenesses between the initial process of building online relationships and online grooming procedure can namely that some harassment is going unnoticed as many victims don't realize they're going to 'groomed' It is simple for 'groomers' to discovery child victims online [3]. They typically use the chat rooms which are focused about young people's welfares. Many give a wrong physical description of themselves which may bear no similarity to their real natural behavior – some individual send photos of other people and pretending that it is them and so on.

By looking from end to end personal websites such as social networking sites, groomers may also search for probable victims. There is problem about the security of children from online sexual predators have been famed in political and arguments of media in recent times. We can use [4][5] paper for sexual solicitation of children with the help of Internet, which is generally known as 'online grooming'. The intention of this issue is to 'procure' a child to involve in sexual activity whichever online or physically offline. The preparation

online communications that are grow to make children further responsive to sexual relation. Groomers may go to a social websites used by young persons and dramatically performance to be one of them. They potentially try to acquire trust with the help of fake ID or display pictures, showing related kind of welfares, proposing gifts and saying fine things to the child.

2. TECHNIQUES

2.1 Text Analysis

The amount of positive and negative reaction combined with sentiment analysis through different text mining modules by using Abusive Text Detection.

Using Preprocessing technique we make input text more consistent using techniques such as stop word removal and stemming. In preprocessing system removing meaningless word. The feature extraction is one of the most important subtasks in abusive text categorization.

Bag of Words (BoW) model is commonly used model in Natural Language Processing. The creation of vocabulary of words which is in our approach indicates the vocabulary or the collection of abusive words is the primary stage of this model. In BoW model, each word is associated with a count of occurrences.

Check the words in the multiple categories, there are multiple dataset categories are provided like history, Education, Entertainment, sports, politics. Finding vulgarability of message using rules of semantic analysis. If vulgarability is find in the message than block the message.

2.2 Image Analysis

Image analysis is the extraction of meaningful data from images or pictures; mostly from digital images by means of digital image processing techniques. Image analysis jobs can be as simple as reading bar coded tags or as refined as detecting a persons. Computers are crucial for the analysis of huge quantities of data, for jobs that need complex computation, or for the extraction of quantitative info. On the other side, the cortex of human visual is an excellent image analysis apparatus, especially for takeout higher-level info, and for numerous applications including medicine, security, and remote sensing — human analysts still cannot be replaced by computers. In this image analysis technique for abusive image detection this system implement the Skin color detection algorithm. Using this algorithm fetch the image in pixel value. After this finding the total number of pixels in the image. Find the value of each pixel using (x , y) coordinator and RGB value. There are all possibility of skin tone value are store in RGB value. There are assign skin colour delta value is 50 & PornDelta value is 5. Using following formula finding the

Delta value of current pixel

Where r_1, g_1, b_1 are the skin tone value ,

r_2, g_2, b_2 are the pixel value

If Delta value of current pixel is less than equal to the skin colour delta value then the increase the skinTonePixel value $= \sqrt{|r_1 - r_2|^2, |g_1 - g_2|^2, |b_1 - b_2|^2}$

Find the threshold value,

Threshold= $\left(\frac{skinTonePixel}{totalpixelvalue} * 100 \right)$

Compare Threshold value with the PronDelta value if there are more skin colour pixel value is available in image then block this image. This is only a one small part which is we implementing in image analysis. Just like that we implement more algorithms for image analysis.

4. SYSTEM ARCHITECTURE

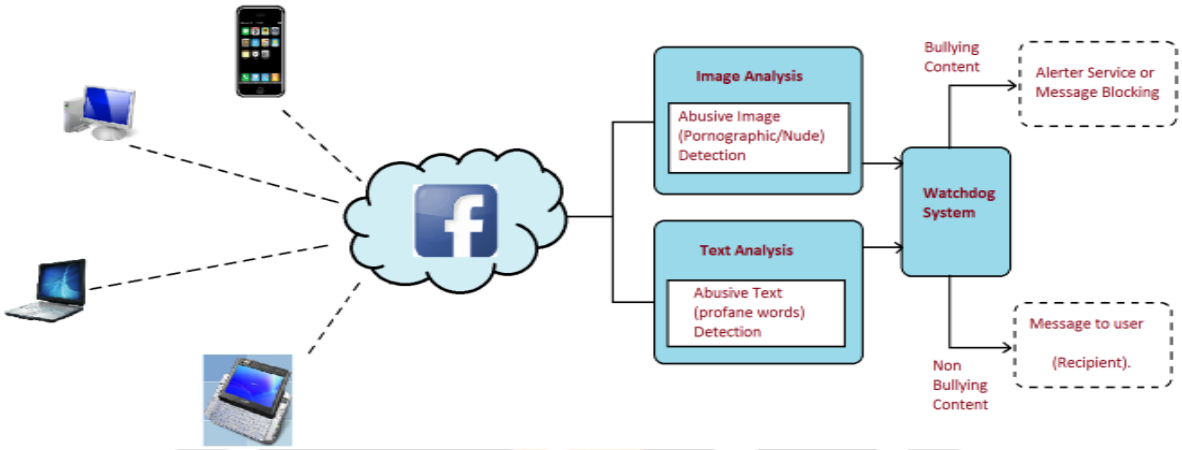

Fig- 4: System Architecture

In the existing system can only detect the attack like Cyberbullying, online grooming etc. but we introduced our system as the Defensive mechanism turns on it, and perform act to avoid system from outdoor attacks. Our system can defend victim from offender and done automatic handling of attack while in the previous system, the manual action should be taken for handling attacks.

4. RESULT

In this system user can post some information in image & text format. In this post if there are some Abusive information is posted than the post is blocked, this post is cannot display to the user, the information about that post is resides in database of the system. The warning alert message is send to the user. If more than four times this user posted abusive message then banned this user's account.

5. CONCLUSION

Up till now, a very minor development has been formed which detect the activities of cyberbullying by analyzing the combination of both image and text data. As a detection mechanism, only the text analysis has gained the majority. We have defined the system which is automated and find out the abusive kinds of text and images content. Our system diagnosis the abusive image using Skin color detection algorithm, whereas text analysis is performed using text mining technique. We are using a Watchdog system to detect the presence of bullying and grooming content information by implementing both text and image analysis results. Our Proposed intension for analysis of incoming messages in the form of text or image on the social networking sites is capable for the cyberbullying and grooming detection.

6. ACKNOWLEDGEMENT

We offer special thanks to Prof. Ingale S.E. who to guide toward development of our system. Also thanks to all who helped in the development of systemand giving their valuable suggestion. So that we are able to improve our system.

7. REFERENCES

[1] Margaret Anne Carter,"Third party observers witnessing cyber bullying on social media sites", Procedia - Social and Behavioral Sciences 84 (2013) 1296 – 1309 www.sciencedirect.com.

[2] Zeynep Tufekci, "Grooming, Gossip, Facebook And Myspace", University of Maryland, Baltimore, MD, USA, Online Publication 01 June Date: 2008.
[3] Christos K. Spyropoulos," Victimization of children by cyber-bullies and online groomers: minor netizens facing the Web's reality".
[4] "Cyber Bullying And Other Internet Dangers", communications@sunderland.gov.uk tel: 0191 520 5555, March 2014.
[5] Kim-Kwang Raymond Choo, "A literature review on the misuse of social networking sites for grooming children for sexual offences", **AIC** Reports Research and Public Policy Series103, www.aic.gov.au
[6] Paridhi Singhal and Ashish Bansal, "Improved Textual Cyberbullying Detection Using Data Mining", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 6 (2013), pp. 569-576,© International Research Publications House, http://www. irphouse.com /ijict.htm 2013.
[7] Charles E. Notar *, Sharon Padgett, Jessica Roden, "Cyberbullying: A Review of the Literature" ,http://www.hrpub.org,Universal Journal of Educational Research 1(1): 1-9, 2013 DOI: 10.13189/ujer.2013.010101.
[8] Aleksandra Kuczerawy and Fanny Coudert, "Privacy Settings in Social Networking Sites: Is It Fair?", Interdisciplinary Centre for Law & ICT (ICRI) – K.U. Leuven – IBBT, Sint-Miechielsstraat 6, 3000 Leuven, Belgium, IFIP International Federation for Information Processing 2011
[9] Dinakar, K., Jones, B., Havasi, C., Lieberman, H., and Picard, R., "Common Sense Reasoning for Detection, Prevention, and Mitigation of Cyberbullying",ACM Trans. Interact. Intell. Syst. 2, 3, Article 18(September 2012), 30 pages.DOI = 10.1145/2362394.2362400, http://doi.acm.org/10.1145/2362394.2362400, 2012.
[10] Vinita Nahar, Xue Li, Chaoyi Pang, "An Effective Approach for Cyberbullying Detection", Communications in Information Science and Management Engineering,School of Information Technology and Electrical Engineering,the University of Queensland, Brisbane, Queensland 4072, Australia 3 ,The Australian E-Health Research Center, CSIRO, Brisbane, Queensland 4029, Australia 1 2013.
[11] NaliniPriya. G and Asswini. M., "A Dynamic Cognitive System For Automatic Detection And Prevention Of Cyber-Bullying Attacks", ARPN Journal of Engineering and Applied Sciences ©2006-2015 Asian Research Publishing Network (ARPN). VOL. 10, NO. 10, JUNE 2015
[12] Zhaoquan Yuan, Jitao Sang, Changsheng Xu, Fellow,(2014), "A Unified Framework of Latent Feature Learning in Social Media",IEEE Transactions On Multimedia, Vol. 16, No. 6, October 2014.
[13] Takako Hashimoto, Supavadee Aramvith and Teeranoot Chauksuvanit, Yukari Shirota ,"Framework for Language Independent Social Media Analysis Platform to detect Reactions on Global Topics", Japan , 2013.
[14] Marco Vanetti, ElisabettaBinaghi, Elena Ferrari, Barbara Carminati, Moreno Carullo, "A system to filter unwanted messages from OSN user walls ", Department of Computer Science and Communication ,University of Insubria 21100 Varese, Italy, 2013,
[15] Rybnicek M, Poisel R, Tjoa S, "Facebook Watchdog: Research Agenda for Detecting Online Grooming and Bullying Activities", Systems, Man, and Cybernetics (SMC), IEEE International Conference, 2013.
[16] Krishna B. Kansara † * and Narendra M. Shekokar†, "A Framework for Cyberbullying Detection in Social Network ", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161 ©2015 INPRESSCO®, All Rights Reserved Available at http://inpressco.com/category/ijcet
[17] Jun Yang, Yu-Gang Jiang, Alexander Hauptmann, Chong-Wah Ngo, "Evaluating Bag-of-Visual-Words Representations in Scene Classification", Proceedings of the international Workshop on Workshop on Multimedia information Retrieval , 197-206, 2007.
[18] Nitin Narayankar, Sanjay Dhaygude, "Texture Extraction for Image Retrieval Using Local Tetra Pattern", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) 2013.
[19] Brian O'Connor and Kaushik Roy, "Facial Recognition using Modified Local Binary Pattern and Random Forest",Department of Computer Science, North Carolina A&T State University,Greensboro, NC 27411 ,International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 4, No. 6, November 2013.
[20] Z. Guo, L. Zhang and D. Zhang, "A Completed Modeling of Local Binary Pattern Operator for Texture Classification," IEEE Trans. on Image Processing, vol. 19, no. 6, pp. 1657-1663, June 2010.
[21] Hinge Smita, Gaikwad Monika, Chincholkar Shraddha, "Retrieval of Images Using Map Reduce", International Journal of Advanced Research in Computer Science and Software Engineering ,Research Paper Available online at: www.ijarcsse.comVolume 4, Issue 12, December 2014 ISSN: 2277 128X.