

A New Approach for Secure Login Method and Forestall Cyber bullying in Social Media

K Vijaya Babu, Mrutyunjaya S Yalawar, Shantala S Yalawar

ABSTRACT---The development in the today's technology plays an important role. There are lot of websites like social networking media is essential for various people where number of sites is dramatically high compare to other websites in the internet. The some of the social networking sites are used for both communication and as well as to promote their business Online. Due to the rapid increase in growth of various social networking websites are affected by various cyber attacks like by sharing data which is leaking due to lack of privacy. Hence the various users who are connected to social network websites with their own systems which can be affected by attacks. The various attacks can be like targeted, hacked by someone, stealed information even though antivirus system which we using are not enough to protect the attacks which can be caused by various sites. We proposed overall security like login methods, for various attacks, even like cyberbullying in various sites using voice recognition.

Keywords—cyber-attacks, Social networking, voice-recognition.

I. INTRODUCTION

In the present world the various increased problems of cyberbullying, ways of protecting your personal profile from the bullies online. Strangers, people you know use your personal information against you for different reasons or purposes. There are no particular techniques or methods that got implemented on various social media/sites to protect people from cyber bullies that we are using in our daily life. So, we introduced the bullying detection method called "cyberbullying detection based on semantic enhanced marginalized autoencoder". Our method can detect bullying words or related words from a sentence and blocks it without getting posted. The cyber attack generally distinguished from various other computer related attacks which can be caused by using the websites. The some of the attacks like Denial of Service (DOS), spam email messages can be caused by various third party like hacker. These can usually attack the server. The cyber bullying where the some of the individuals are harassed by other peoples. These can one of the common attacks which can be happen online.

II. LITERATURE SURVEY

The some of the implemented security methods for the mobile devices not enough to avoid cyber attacks from various networking sites [1]. Modeling the Detection of Textual Cyberbullying: This paper shows that the detection of textual cyberbullying may

be tackled through the use of manner of constructing character trouble consider-touchy regions[4].

The findings embody the importance of addressing peer participants of the own family troubles, specially peer popularity and victimization, within the remedy of tension and the prevention of depression amongst nerve-racking children[3].

Notwithstanding the reality that the net has transformed the manner our worldwide operates, it has additionally served as a venue for cyberbullying, a severe form of misbehavior amongst young people. With lots of these days's young adults experiencing acts of cyberbullying, a developing body of literature has started out to file the prevalence, predictors, and consequences of this conduct, but the literature is notably fragmented and lacks theoretical awareness[2].

Being bullied for the duration of young adults or children is a danger aspect for someone's properly-being and adjustment. furthermore it is identified that bullied college students additionally may be laid low with awful bodily fitness and show a numerous variety of health troubles like backache, belly pain, pores and pores and skin troubles, sleeping issues, bedwetting, or dizziness. regardless of the fact that the ones effects had been confined via the small quantity of research blanketed inside the meta-assessment and the consequences have been additionally restrained with the useful aid of the a longitudinal format[5].

Bullying that includes emotional or physical intimidation is related to a number of mental fitness problems coping with kids. 1,2 approximately 70% of children document having professional bullying in some unspecified time inside the future inside the path of their college careers, 3 and at any 1 time, about 20-25% of children are recognized as being proper now involved in bullying at college. 1,2 the fast increase of conversation generation mainly among young adults, four cyberspace has been implicated as a modern day volatile environment for bullying. five They recognize about wherein and the way younger human beings come across bullying on-line, chance elements related to repeated intimidating on line evaluations, and the possible overlap and connection among bullying encountered in college and on line. 6 Given the revolutionary increase in internet use of 12- to 17-yr-old younger people within the beyond 56 years 4 and the dearth of individual supervision online, there are numerous motives to be worried that cyberspace gives a fertile ground for bullying. Public troubles have focused mainly at the risks related to the generation allowing short

Revised Manuscript Received on May 15, 2019.

K Vijaya Babu, CMR Engineering (CMREC) College, Dept of CSE, Hyderabad., Telangana, India. (Vjb059@gmail.com)

Mrutyunjaya S Yalawar, CMR Engineering (CMREC) College, Dept of CSE, Hyderabad, Telangana, India (mrutyunjaya.cmrec20@cmrec.ac.in)

Shantala S Yalawar, TCS Pvt Ltd, System Engineer, Bangalore, Karnataka, India.

and nameless spreading of messages to probable big audiences. for that reason, cyberbullying is widely described as the use of the net or other digital communicate gadgets to insult or threaten someone[6].

Investigating the interconnections amongst character fitness/nicely being and socio-mobility. The underlying idea is to come to be aware of the composites of extended-term behavioral dispositions (e.g. numerous social hobby) that may be predictive of health related tendencies like highbrow fitness or cooperative thoughts-set. Analyzed the social interaction kinds of a network of customers to check the impact of social behavior on special components in their life. One take a look at has determined correlations maximum of the social behavior of humans measured thru top notch modalities like call, SMS, Bluetooth, and GPS logs and their spending behavior. 2d its positioned community topology, records go along with the drift, and harmony in a network may be used to are looking ahead to the commonplace happiness diploma in the community. paintings in development to make use of those records to generate precise and implicit nudges for customers to undertake considered one of a kind movements in severa properly being settings[7].

scientific research on own family[8] elements associated with the primary cyberbullying roles are no matter the fact that scarce. the existing check analyzed circle of relatives weather and parent adolescent communicate inside the four roles worried in cyberbullying: cybervictims, cyberbullies, cyberbullyvictims, and noninvolved younger humans. The test hadprimary desires: (1) to investigate the versions in own family climate (concord and conflict) and conversation styles with the mother and father (open, avoidance, and offensive) the severa 4 roles, controlling the variables intercourse and academic grade; and (2) to decide the predictive weight of numerous family variables inside the roles involved in cyberbullying. in the long run, the ones own family variables together (war and no open and avoidant conversation) expected the area of cyberbullyvictim[10].

III. EXISTING SYSTEM

Currently there is no existing system to detect bullying words and block it on social media. But, there are some sites which use manual methods to block bad words. Admin does the blocking if in case any complaint is given by the other users. Even the lot of security attacks like DOS, DDOS, and Zero day attack making the information to be unsecured.

IV. PROPOSED SYSTEM

Our proposed system going to provide more authentications for social network user login through the voice recognition. There are total three modules in this system which will be clearly described in system architecture later. First a social platform is created just to experiment our proposed method of detecting bullying words. A list of bullying words will be entered into the database and it is compared with the user's usage of words when they try to post anything on their timeline. Our semantic Enhanced Marginalized Denoising Auto-Encoder helps in detecting bullying words and block them

automatically. Admin has the authority to block the users who use bullying words. Each time any user uses a various bullying kind of word, their login details go to the admin and admin gets the block option, if the users use up all their 3 chances. Features: It is simple and robust which means it is most effective and efficient way of detecting cyberbullying. This method reduces the labor work or manual work which, it will not really possible to detect all the various kind of bullying words used by the users across the social platform.

V. COMPONENTS

Architecture

When users use bullying words in their posts, detector detects those words with the help of bullying words list that's already saved in the database and blocks it. Then, it updates the bullying words users details to the admin where these users get blocked by the admin. The server gets the requests from users and admin and responds accordingly.

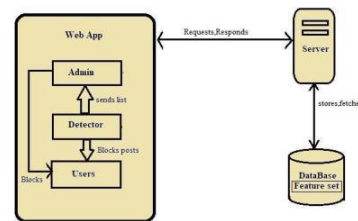


Fig: 5.1. Architecture

Dataflow Diagram

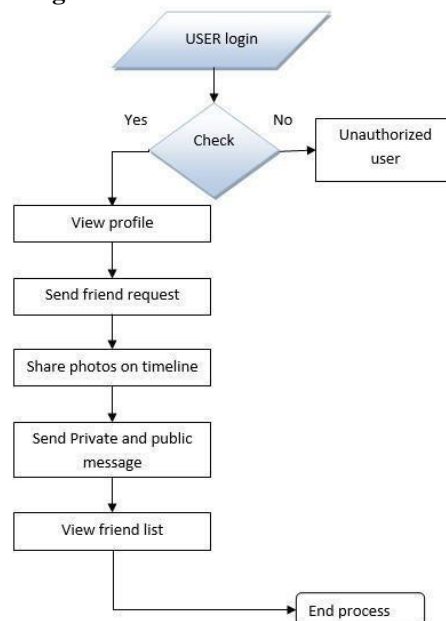


Fig-5.2: User DFD



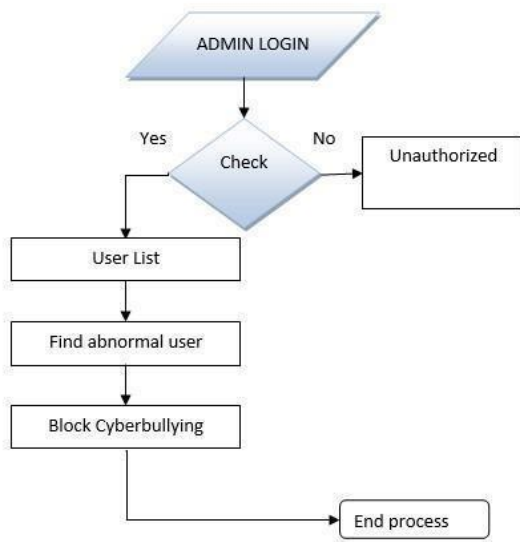


Fig: 5.3- Admin DFD

Voice Recognition:

The Voice recognition is a manner in which the cell or alaptop tool identifies the speech it is given with the useful useful resource of customer to get proper of get right of entry to to the Social networking net sites. It technique that the device can pick out out speech it truly is given thru the customer and it is able to apprehend the voice which can able to access theaccount. The Proposed approach is secured with the voice get right of entry to as Voice is the particular subjects for individual or purchaser. The hacker well-knownshows little difficult or complex to hack the get proper of access to for numerous login methodologies. Voice recognition technique is on foot on a voice platform, net servers, and authentication servers alongside facet voice bio metric matching engines. as speedy because of the truth the individual gives the voice command the tool will mechanically generated to a vocal password. The entered voice is probably check with the stored information inside the database server and if the voice of the customer is legitimate the character can securely login to their debts. Incase if the entered voice is a fraudulent one it's miles going to be recorded thru the server and stored within the database to be aware of the real person of the account. however, in some tries to login the use of with use of vocal password can be failed to triumph over the mission the person is given three attempts to offer the voice to the login attempt to after the attempt the device will matching the voice with the saved voice within the database. furthermore, if the person desires to reset the voice the person can login with the given voice and exchange the vocal password with the useful useful resource of giving the current-day vocal password to the account.

VI. EXECUTION SCREENSHOTS



Fig 7.1: Normal Post

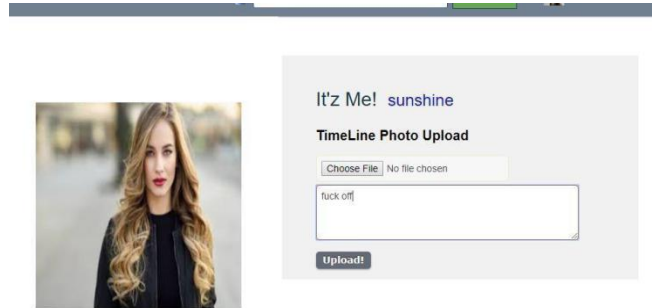


Fig 7.2: Bullying post



Fig 7.3: Popup message



Fig 7.4: Bullying users list





Fig 7.5: Blocked Users list

VII. CONCLUSION

we've evolved more suitable marginalized denoising car encoder procedure for cyberbullying detection. Our mission is meant for detecting cyberbullying text to block the posts and users who're using bullying words. This process might help in reducing the cyberbullying to an volume as the public posts have become blocked and saves the users from feeling embarrassed or threats of spreading their non-public facts on timelines.

VIII. FUTURE ENHANCEMENTS

To control the cyberbullying, images and videos blockage can also be implemented in future with the help of other technologies. The same procedure can be implemented to block posts, messages, images and videos using image detection and machine learning techniques using python along with java.

REFERENCES

1. M Chi, (2011), "Security Policy and Social Media Use" SANS InstituteInfoSec Reading Room, [Online], Available: <https://www.sans.org/readingroom/whitepapers/policyissues/reducing-risks-social-media-organization-33749>
2. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and A. Mopportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.
3. R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and M. R.Lattanner, "Bullying in the digital
4. age: A critical review and metaanalysis of cyberbullying research among youth." 2014.
5. B. K. Biggs, J. M. Nelson, and M. L. Sampilo, "Peer relations in the anxiety–depression link: Test of a mediation model," Anxiety, Stress, & Coping, vol. 23, no. 4, pp. 431–447, 2010.
6. G. Gini and T. Pozzoli, "Association between bullying and psychosomatic problems: A metaanalysis," Pediatrics, vol. 123, no. 3, pp. 1059–1065, 2009.
7. B. L. McLaughlin, A. A. Braga, C. V. Petrie, M. H. Moore et al., Deadly Lessons::Understanding Lethal School Violence. National Academies Press, 2002.
8. J. Juvonen and E. F. Gross, "Extending the school grounds?bullying experiences in cyberspace," Journal of School health, vol. 78, no. 9, pp. 496–505, 2008.
9. Q. Huang, V. K. Singh, and P. K. Atrey, "Cyber bullying detection using social and textual analysis," in Proceedings of the 3rd International Workshop on Socially-Aware Multimedia. ACM, 2014, pp. 3–6.
10. M. Ybarra, "Trends in technology-based sexual and non-sexual aggression over time and linkages to nontechnology aggression," National Summit on Interpersonal Violence and Abuse Across the Lifespan: Forging a Shared Agenda, 2016.

AUTHOR'S BIOGRAPHY:

1) K Vijaya Babu



Mr. K. Vijaya Babu Working as Assistant Professor at CMR Engineering College, Medchal Hyderabad, India and He done M. Tech. (IT) from JNTUK Vizianagaram Campus. He is having 7 years of teaching experience and published 9 papers in various National and International Journals. His areas of interest are Computer Networks, computer forensics, Information Security, Network security and Data Mining.

2) Mrutyunjaya S Yalawar



Mr. Mrutyunjaya S Yalawar working as Assistant Professor at CMR Engineering College, Medchal, Hyderabad, India and having more than 3 years of experience in IT-Industries as Software Developer and more than 2 years of Experience in Teaching Field. He published about more than 8 Papers in various National and International Journals.

3) Shantala Yalawar

Shantala Yalawar has completed M.Tech(CSE) from BEC, Bagalkot, VTU Belgaum, Karnataka. Presently she is working as Systems Engineer at TCS Pvt Ltd, Bangalore, having the more than 6 years of Experience in the software Development.