Secure Social Network

Prof. Minakshee Chandankhede[1], Priya Madke[2], Amrapali Fusate[2], Rizwan Farah[3], Chetna Sonik[2], Anand Gurve[2]

[1]*Assistant Professor, CSE, GHRAET, Nagpur, Maharashtra, India*

[2]*Student, CSE, GHRAET, Nagpur, Maharashtra, India*

[3]*Business Analyst, Axiom Techguru Pvt. Ltd., Nagpur, Maharashtra, India*

***Abstract*- In our paper, we had introduced authentication service by using aadhaar details dataset. Unlike other social networking sites, here only 18+ users are allowed to make account on this site. If details not matched with the admin's dataset then the admin will not verify the account and denied the registration process. Abusive words are not allowed to post by using preprocessing technique. No image of others get posted without permission.**

***Keywords*: Authentication, security, social networking site, abusive words, preprocessing, dataset**

I.INTRODUCTION

Online social networking sites that are available in today's world are growing day by day. Millions of user's are becoming part of the social networking sites. These social networking sites connect people all around the world. Some of the most useful social networking sites are Facebook, twitter, Instagram, etc. In these sites anyone can creates their profile. Even the persons who are under 18 can also are able to create their profiles. There are no restriction barriers that can be used for user's security purpose. Private data of user's which is not necessarily known by other can be grabbed by them easily. Anyone can use abusive words for doing comments on other's post or public post. Also the social networking sites users can post other user's image which is a risk factor of these sites as if the user is not aware of its post image .Security cannot be maintained in these situations.

In the proposed research we are trying to overcome some issues related to social networking sites that should be secure by some features by allowing some restrictions and privacy should be maintained till some considerations.

II. LITERATURE REVIEW

"Security Policy and Social Media Use" settled by Maxwell Chi presented a secure way to make access the social networking sites. The research paper accomplishes series of privacy schemes to access social networking sites such as keeping a tough password, CAPTCHAs, clearing the surfing history and desktop safety. Since the above detail accomplishes that the system they had introduced was not very much safe with the hackers [1].

"Privacy in Online Social Networks" established by Michael Beye et al. The research involves the methods like how to control a social networking site such as messaging, multimedia, tagging and favorites. The procedure of them is a worthy practice to keep the reserved profiles safe and sound but the structure has not covered a method to login to the account securely. The proposed research is boosted with more privacy features while the user sign in [2].

"Photo-Based Authentication Using Social Networking" research is set up on photo based authentication framework called as Lineup. Lineup mostly used "CAPTCHA" technique. Uses of Lineup can help site administrator to check and approve a client connection by user requirements to detect the cluster of photos. This authentication system gives facility to make enter the website without memorizing the password. [3].

"Security and privacy in online social networks" is one of the research done by Levcio Antonin Cutillo based on the relevant topic. Integrated online social networks pretend a risk to their user's security as social network supplier have infinite access to user's information, this idea comprises in the research done by the organization of Royal Institute of technology. [4].

"Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition" is introduced by L.S.Y.Dehigaspege, U.A.A.S. Hamy, H.P. Dangalla is based on voice recognition system. This method works on voice platform, web server, authentication server along with the voice biometric matching engines. Text based captcha is mainly targeted in this research by using captcha's mechanism. It also includes location identification using GPS server [5].

III.METHODOLOGY

The process starts with, if any particular needs to login, it needs to register itself first. The mandatory field while doing registration is filling aadhar number correctly. After that the registered user needs to be verified by admin. If the admin verified the registration, then only the user can login in its account and vice versa.

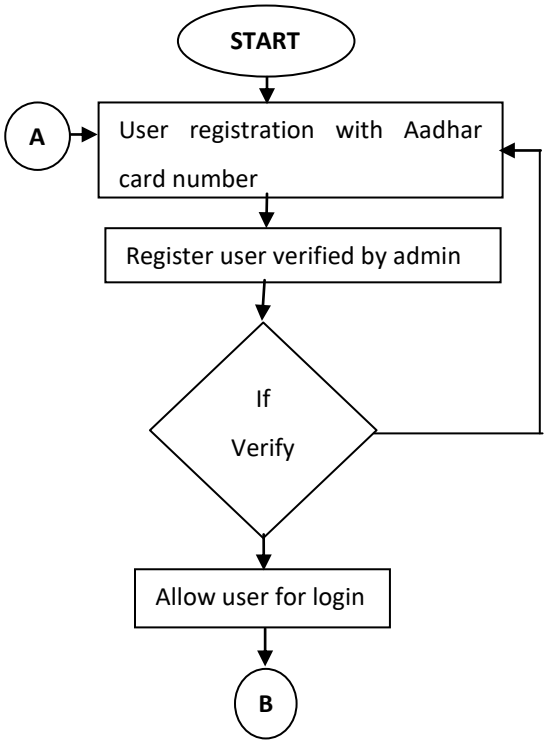

Figure 1: Registration by authentication

Now, we had also provided a module called as guest user just for doing the publicity of site and also for increasing its members. Here the guest user will able to view only registered verified user's profile image and its name. Then, if the guest user needs to login, it needs to registered itself first.

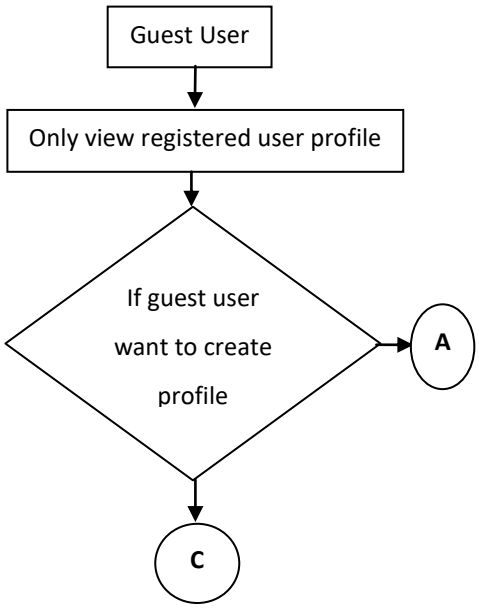

Figure 2: Guest User

As the registered person get verified by the admin, the user can now login in its account, set privileges and update its profile. If the user now post some textual data and if the text contains some abusive words, then the text won't be able to post.

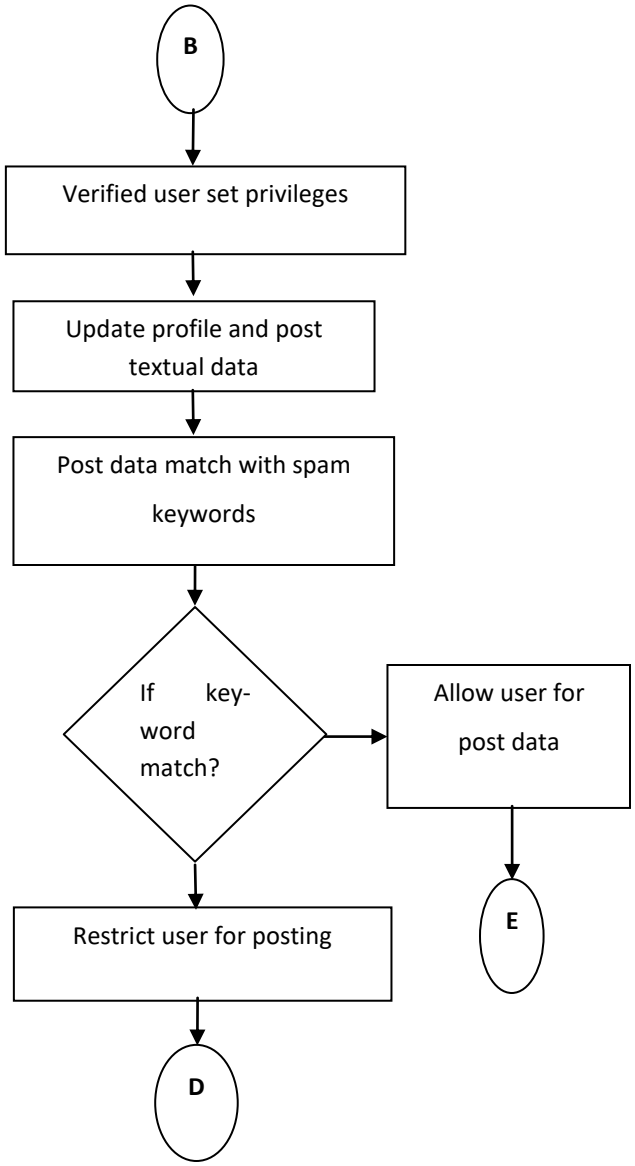

Figure 3: Text Posting

Though we had make restrictions for posting abusive text, we were also concern for image/video security. We had also set restrictions for posting other user's image without seeking their permission. Until the user will not get permission from the user whose image is to be posted, the image will not be able to post.

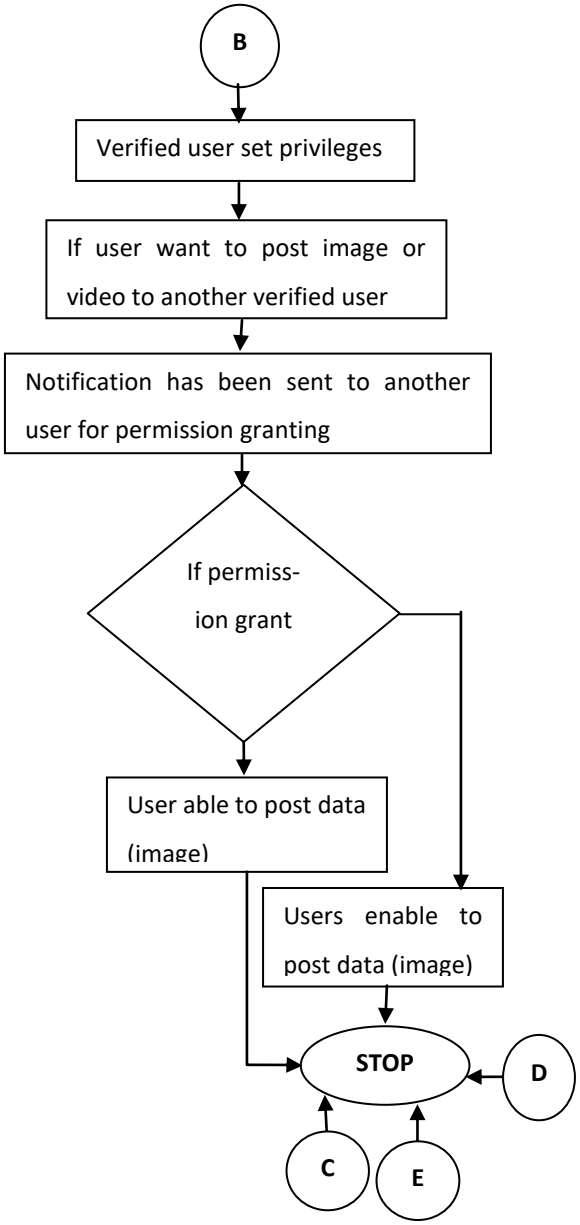

Figure 4: Image Posting

IV. DESIGN AND IMPLEMENTATION

Home Page

Figure 5: Home Page

A. Registration by Authentication

To access any social networking site, that particular needs to register itself first. Here, while doing registrations, it is mandatory for a person to fill its aadhar card number. This field is set because for not providing more than one ID for any person and also for allowing only 18+ age persons to be able to do registrations. In admin's panel, a dummy dataset of Aadhar cards of some 50-100 persons has been maintained. It contains field like name, aadhar card no, date of birth. By using this dummy dataset the admin will be able to verified user as 18+ by matching datasets field's entries with the entries filled by the person while doing registrations. As aadhar card number is unique for every person, the person cannot be able to make its account i.e. fake account.

B. Guest User

In social networking sites which are widely used now a days has many features that are able to increase their members. But for that, they need to make their account first. Then only they can see the sites. But in our case we are providing a facility for people who are willing to survey our site before making their account i.e. Guest User. In guest user module people only have to put their names in the block and then click Ok. Now the person is able to view only profile image and name of the registered verified users. If the person finds their friends, relatives and any known name in the list they would also wish to join this site. For this they need to register themselves now. This is used for publicity of the site.

C. Text Posting

It contains friend suggestions, keyword extractions and matching with data dictionary. The registered users can send friend request as way done in other sites. Users are able to post textual data like comments on their walls as well as on their friend's wall. But here, we are avoiding the posting of abuse words. Because security is one of the important concern in our site to make the user's profile clean. So we are maintaining a dictionary of abusive words. If anybody try to use these words in their post, then this post get discarded by administrator. We are using data mining rules and had apply to the process of posting textual data which is been posted by registered user. Here, we preprocess that posted content and apply rules on that so that it gets classified into abuse and non-abuse data set. Natural Language Preprocessing module include the data set preprocessing and posted contents preprocessing. Here the parsing data i.e. abuse and non-abuse, and at the posting time if any abuse keyword occurs then it get restricted by admin and denied the user for posting.

D. Image Posting

Apart from restricting posting of abusive word, one function is there, which restricts users for posting others image without

seeking their permission. We are providing a notification to user whether they wants to post that image. If that particular persons denies to post that image that post will never be seen by any user on the site.

V. RESULT AND DISCUSSION

While doing registration in site, the persons needs to fill its date of birth. If the persons birth is calculated as below 18 then a pop up is generated showing "the user should be 18+".

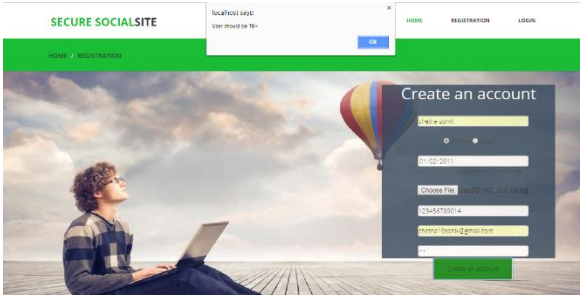

Figure 6: Registration page

Abuse words are enable to post. If the text contains any abusive words, then it won't be post. It shows a pop up i.e. "your post contains abuse words, sorry you are enable to post."

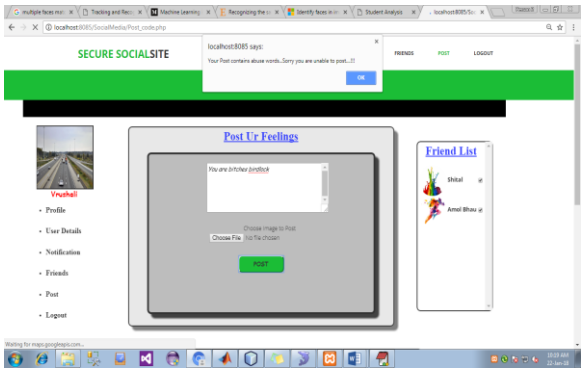

Figure 7: Restrict for Posting Abusive Words or Image

If the text does not contains any abuse words, then users post get easily posted showing the pop up "data posted".

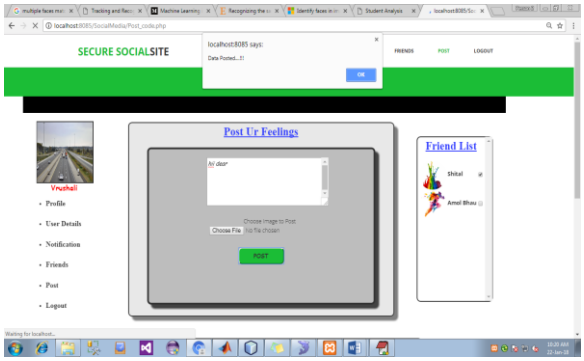

Figure 8: Posting non Abusive Words

VI. CONCLUSION

If the person is under 18, then that particular is not applicable for making account. No abusive words get posted and also no image without seeking permission is going to be post. Guest user is only able to read registered user's profile image and their name and can't write anything on the wall without doing authenticated registration.

Till now, our project is providing one user one account by using aadhar details and also making restrictions from posting abusive words and posting others images without their permission. In future reference, we will work on it to make it more secure and user friendly.Future work contains conducting this survey at a large scale using a large sample of dataset, restrict for posting abusive video, more meticulous security related opinion poll and on other social networking sites also so that more details get covered about the security features of social networking sites. More than this, still there is a lot of research work is required in the field of privacy and security of social networking sites.

REFERENCES

[1]. M Chi, (2011), "Security Policy and Social Media Use" SANS Institute Info Sec Reading Room, [Online], Available: https://www.sans.org/readingroom/whitepapers/pvide vide one user one olicyissues/reducing-risks-social-media- organization-33749 [Accessed: 16 July 2016]

[2]. M Beye, A Jeckmans, Z Erkin, P Hartel, R Lagendijk, Q Tang, (2010) "Literature Overview- Privacy in Online Social Networks", University of Twente, Publication [Online], Available: http://doc.utwente.nl/74094/1/literaturereview.pdf [Accessed: 20 July 2016]

[3]. S Yardi, N Feamster1, A Bruckman, (2008), "Photo-Based Authentication Using Social Networks", ACM Sigcomm Workshop on Online Social Networks [Online], Available: http://yardi.people.si.umich.edu/pubs/Yardi_AuthenticatingSocial Network08.pdf. [Accessed: 17 July 2016]

[4]. Zanero, S, D Keromytis , " Security and privacy measurements in social networks". Available: http://nsl.cs.columbia.edu/papers/2014/lessons.badgers14.pdf [Accessed: 25 July 2016]

[5]. D Gunter , Solomon S, "The Danger of Data Exfiltration over Social Media Sites" , Western International University, Available: https://media.blackhat.com/bh-us-12/Briefings/Gunter/BH_US_12_Gunter_Sonya_SNSCat_WP.pdf [Accessed: 19 July 2016]

[6]. L.S.Y. Dehigaspege, U.A.A.S. Hamy, H.A.H. Shehan, S.A. Dissanayake, H.P. Dangalla, W.H.I. Wijewantha and Dhishan Dhammearatchi "Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition" International Journal of Scientific and Research Publications, Volume 6, Issue 10, October 2016 120 ISSN 2250-3153 www.ijsrp.org