IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Fake Id Prevention In Online Chatting

Ankur Singh Bist
Dept. Of Computer Science, G. b. pant university of agriculture and technology.
ankur1990bist@gmail.com

Abstract
Online chatting has become very popular in current scenario but the challenging factor is the security issue at different levels. Our main focus in this paper is to develop an approach by which we can detect fake id in appropriate manner and for this certain specific process is taken by us that will reduce the various negative vibrations of growing online chatting community.
Keyword: Chatting, FB

Introduction
Chatting websites like facebook is one of the foremost social networking websites, with over 8 million users spanning 2,000 college campuses [1] With this much detailed information arranged uniformly and aggregated into one place, there are bound to be risks to privacy and the presence of fake id increases this problem more drastically . University administrators may search the site for evidence of students breaking their school's regulations . Users may submit their data without being aware that it may be shared with advertisers .Third parties may build a database of chatting websites data to sell. Intruders may steal passwords, or entire databases, from chatting sites . We undertook several steps to investigate these privacy risks. The fake id creates a lot of problem regarding security at personal level ,there is no method to prevent and check if one uses the image of some another person as its identity on chatting websites , for example if I uses the photo of my friend as my id mark and my friend does not know about it then I can make reach to persons known by my friends until they recognize me. In this paper , I will try to resolve this problem by proposing a methodology and if implemented can lead to sort out this problem.

Related Work
Users share a vital information about themselves on their chatting profiles, including photos, contact information, and tastes in movies and books. They list their friends including friends at other schools. This all creates a kind of connecting path so if fake id get survive for long time it may affect a lot to many entities involved in it. Most of the chatting sites includes various privacy setting comprised in it. The problem what we are discussing is still uncovered by any known chatting site , but if we want to secure ourselves at various levels , it is provided in chatting sites like in facebook you can block certain sources and many other privacy measures are there but to fulfill our objective something more is required.
Below pictorial representation explains the problem statement and interpolates the situation how one fake user can creates its id by inserting the photo of someone else and put a mask on its identity and such activities will lead to ambiguity and unsecure activities on social networking sites as well as it creates the problem for other whose identity one is using . Other case of fake id that involve the identity image of someone general icons will be covered under our scheme rather than this it is clear that someone is at once joins the friend circle if one finds the image of its known and second factor are name and other details.
Working of proposed architecture flows as shown in figures ,the photo of user taken at registration time for new users by webcam and at upgrade time by other users determine the inspection considering here that the pattern recognizing ,classification and identification of images techniques are enriched enough to tackle all situations , other biometric components like fingerprint and voice record can be taken for higher authentication these parameter are not used for fake id prevention in our architecture but these parameter should be used in our architecture to prevent the trial by anyone for creating fake account.

The whole activity related to computer vision [4] methodology research , further high level analysis can include the face expression counting sequence and analyzing the facial activity of the user making id it can be done by collecting a set of dataset including the vital measurement of the expression

study while making id and tried to match with the current situation at the time of id creation by user.

With the above feature certain other features and factors are necessary for strong detection and prevention but to implement the whole scenario require to arrange and synchronize the certain schedule of input data as taken by developer side for matching user activity, user current situation, arrangement of modules in proper format and whole expansion of further activity with certain planning so that detachment of user could not produce.

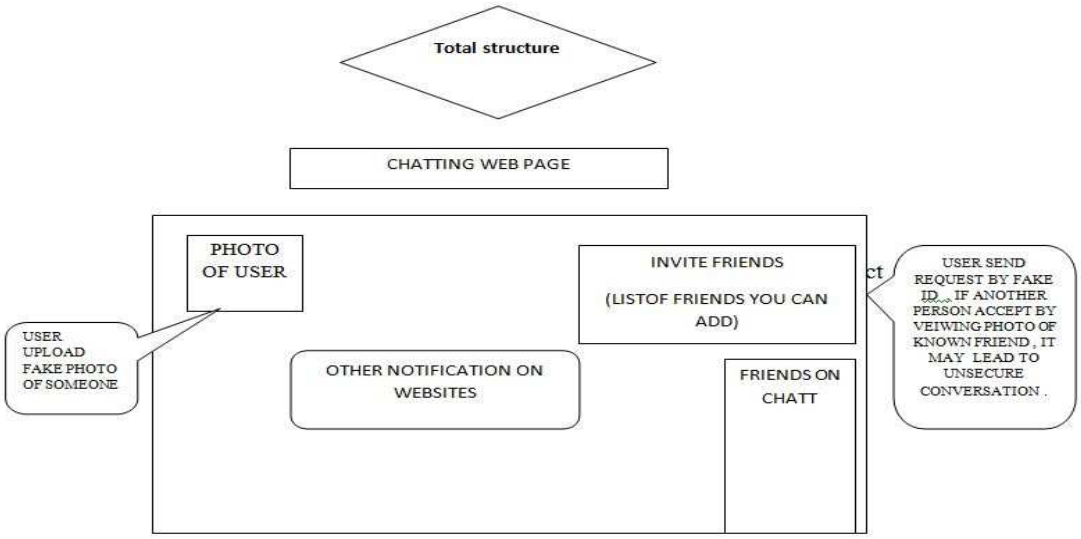

Fig 1. Showing the problem of fake id

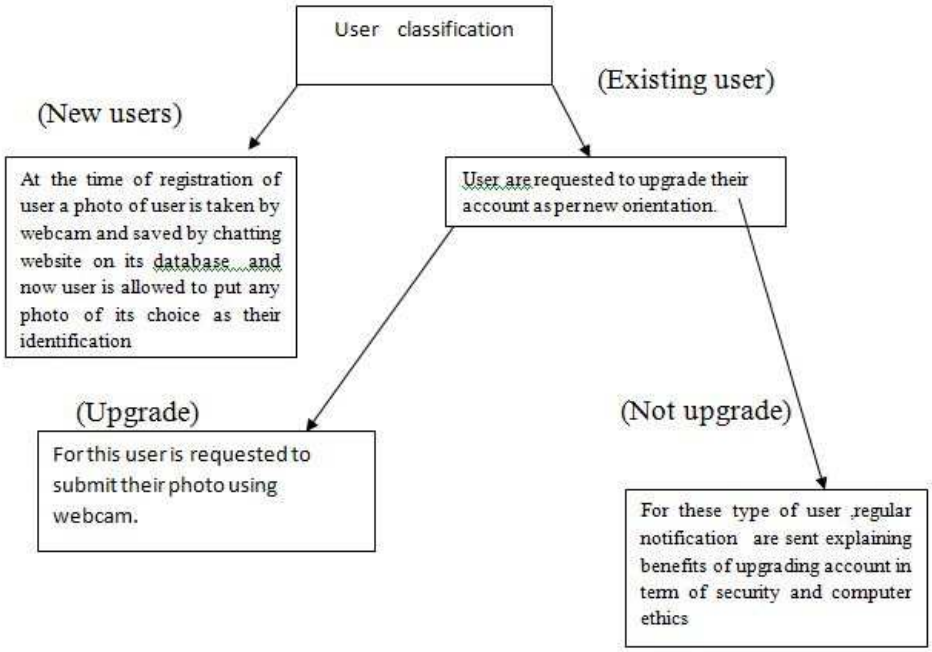

Fig 2. Front end of architecture

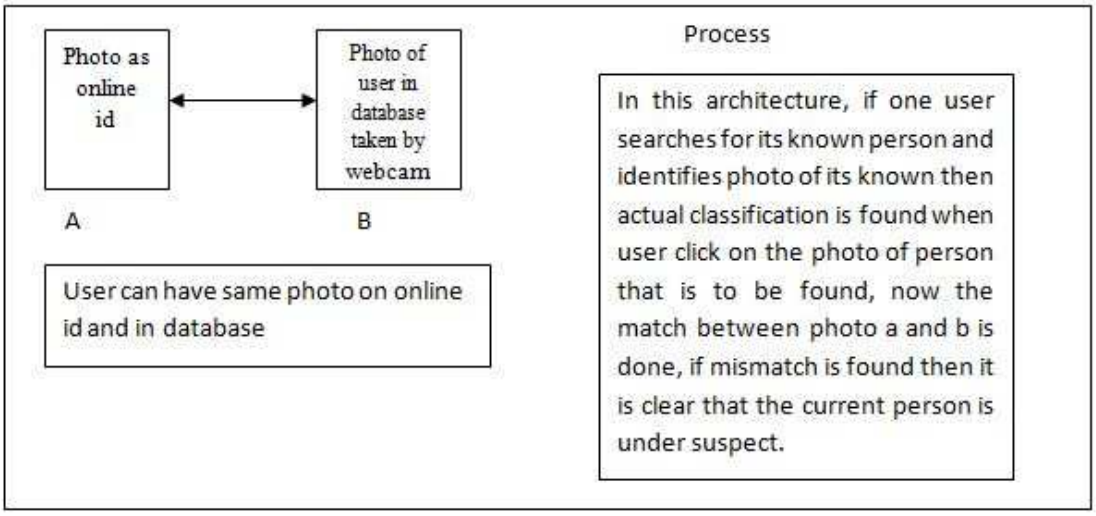

Fig3. Internal working and Fake id detection

Experimental analysis

The experimental setup involve the front end architecture where java get used and at back end oracle 10g is used , it is not much typical to implement it but it is needed to be adopted by all those websites developers where millions of user are concern with the issue of security , the proposed framework or approach will mould and bring a revolutionary change in the world of social networking where we call the social networking place as noble social networking place where every user behaves as in good society and will enjoy the same factors as face now. As In small domain of developed experimental setup , it gives a different secure environment .In countries where people have freedom to talk anything social networking sites may cause big impact ,people do this by using fake id. The real success of this approach will appear when we will see every networking site like facebook and google plus will use this approach actually it need only a start.

Updating criteria maintenance

Users of secure community called community j maintaining same photo in database and online id may fell unease in changing their photo on their pages , there can be two options here either they have to timely update their online photo with database or for maintaining user friendly environment website developer may opt another path which includes a record maintenance for community j users and if for a certain period of time for example 6 month or 1 year activities of user appears authentic like user does not perform any activities like sending

Justification of proposed approach

There are various queries that can be raised on this particular system but I am trying to cover all possible answers in this particular session. Firstly our proposed architecture is made keeping in mind about user flexibility so user is allowed to have any photo that is differ from database image of user , secondly upgrade is not made compulsory it is done because it gives user time to observe the benefits of new scheme and sudden implementation may effect website business so it helps both.

Community approach

This whole process will evolve two community under one roof named as community j(joined upgrade) and nj(not joined upgrade).Everyone wants to maintain better look on social sites so our proposed will attract that want security and finally everyone will come under this for various reasons like one reason might be that one would want to be a part of good and secure community .This will regulate the computer ethics [2][3] framework get modeled with this existing system.

unusual friend requests and many other criteria taken under this . If user satisfies noble case under time limit then user allow to have freedom of putting any image mark as its identification under security label .

Workload to developers

The storage and various arrangement in term of pattern matching and other related activities will cause extra burden for developers and one another issue of sustaining user information in this means will rise another issue but the major concern is associated with user security and reliability with

certain system of frame. Finally it can be maintained and arranged by creating suitable policy.

Conclusion and Future Work

The reach and use of social networking websites are increasing day by day but their effect to society in term of various security issues need to be studied seriously.

So that sustainable adjustment can take place. In our proposed plan we try to cover one major aspect that is creating ease in term of fake id handling among users ,further in coming time all negative factors will require to be modeled in control and efficient manner to cover all associated issues .Future work includes the strong pattern recognizing techniques, better use of biometric features of user, better and secure arrangement of user information and govern all possible changes after getting user feedback about newly proposed techniques as given here. We can make hope that according to our model all user after a time span will lie in community j and community nj will be totally eliminated.

Acknowledgement

I would like to thanks my parents mr . khem singh and kamla devi who encouraged and assist me for this work and always keep concern about various security issues of computer world .

References

[1] Terremark's Worldwide, Inc. \Facebook Expands Operations at Terremark's NAP West Facility" Tuesday November 1, 8:30 am ET.

[2] Manner, w. (1980). Starter kit in computer ethics .Helvetia press.

[3] Johnson , D. G. Computer Ethics. Prentice Hall.

[4] Keith Price's Annotated Computer Vision