ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Captcha Authenticated Unwanted Message Filtering Technique for Social Networking Services

Fathimath Shahistha M., Prabhakara B. K.

4th Sem M.Tech, Dept. of CSE., SCEM, Visvesvaraya Technological University, Adyar, Mangaluru, India

Associate Professor, Dept. of CSE., SCEM, Visvesvaraya Technological University, Adyar, Mangaluru, India

ABSTRACT: The authentication and security mechanism for any application is important. The major function of any security system is to protect the data from unauthorized access. The existing password mechanism based on textual passwords provides low level of security against the unwanted access. One of the alternatives to improve the security and authentication is a graphical based password. One of fundamental issue in day today's life is Social Networking Services (SNS) to give users the ability to control the messages posted on their own private wall. SNS provide little support to this requirement. In this paper a system with hybrid graphical password system based on captcha technology. Captcha is a standard Internet security technique to protect online emails and other services. Captcha as graphical password known as Carp. Carp is a click-based graphical password. In which a sequence of clicks on an image is used to derive the password. It includes rule-based system, which allows users to customize the filtering criteria and a Machine Learning-based soft classifier automatically labelling messages with content-based filtering.

KEYWORDS: Social Network Services, Short Text Classification, Policy-based Personalization, Information Filtering, Graphical password, Filtering Rule.

I. INTRODUCTION

The password is used for the authentication purpose. The major function of any security system is to protect the data from unauthorized access. Passwords are the secrets that are provided for the user. Conventional password scheme uses textual passwords or alphanumeric characters and this password scheme is easy but the problem is that if user give small password then the user can easily guess the password and these small passwords are hacked by different attackers. When the text password length is bigger, then it is hard to remember and if the passwords are not frequently used then the passwords are easily forgotten. Graphical passwords are alternative to the textual passwords where graphical passwords use pictures as passwords instead of textual passwords. Graphical based password system is the combination of recognition and recall based techniques where in the recognition method user need to identify the images or objects which are displayed to him/her and in the recall based method the user need to recall the images or redraw the images which he has already selected. The main advantage of using graphical password is that it can be easily remembered. Existing system consist only images for password or draw a secret pattern for password, but there was a problem of shoulder surfing. One person can easily steal the password by seeing and access his secret information. The hybrid graphical password system based on captcha is the security system based on hard Artificial Intelligence (AI) problems where the captcha presents the user with a challenge or a puzzle. This proposed system is based on the click method (portions of the image where the users are likely to select the click-points), captcha is a standard Internet security technique to protect online emails and other services. Carp is a click-based graphical password with a sequence of clicks on an image is used to derive the password. Carp scheme is classified into two categories first is the recognition and the second is the recall based methods. The images used in the Carp are captcha challenges. For every login attempt a new Carp image is generated. Carp resolves the number of security issues such as dictionary attacks on passwords, online guessing attacks etc. Carp requires a captcha challenge for every login. The problem with this password system is that the login process is slow. Carp is robust to shoulder surfing- attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Social Networking Services (SNS) is mainly used to share contents like text, image, audio, and video data a considerable amount of human life information. SNS is a platform to build social networks (or) social relations among people for sharing interest, picture, text and real time connections. A social network service consists of each user having his own profile, social links, blogs and additional services. Web based service allows individuals to create a public profile to create a list of users with whom to share connection and to view the connection within the system. Some of the social networks which are mainly used to connect with friends, example applications like: Face book, Google+, YouTube, Twitter etc. Web content Mining is used to discover useful and relevant information from a large amount of Data. In SNS, information filtering can be used with a different purpose. In SNS there is the possibility of posting (or) commenting other posts on particular public (or) private areas called Walls. Information filtering is mainly used to give user the ability to control the message written on their own walls by filtering out unwanted messages. The aim of the present work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW) which is able to filter unwanted messages from SNS user walls. We introduce a Machine Learning text categorization technique to automatically assign with each short text message a set of categories based on its contentment. Efforts in creating a short text classifier are concentrated in the extraction and selection of a set of characterizing and discriminates features. Data mining (sometimes called data or knowledge discovery) is the process of analysing data from different perspectives and summarizing it into useful information. Data recovery software is one of a number of analytical tools for examine data. It allows users to study data from various different views and methods. Data extraction is the method of finding correlations or patterns among dozens of fields in large relational databases.

II. RELATED WORK

Mohammed Y Aasalem, Wazir zara khan and Yang Xiang proposed a password security method called Graphical password scheme [1] which is an alternative to the textual password where the pictures are used as the password instead of textual passwords. The graphical password scheme is classified into four categories: Recognition, Pure recall, Cued recall and Hybrid systems. The recognition based systems involves identifying whether the user has seen the image before and the needs to identify the previously seen images. Example for recognition-based scheme is Passfaces [2], where the user is provided with the portfolio of faces from the database. In the pure recall based system the user has to recall the images or objects which he has selected before that is during the registration phase. In the cued recall based system the user is provided with the hint so that the user can recall his password which he selected before. The hybrid system is the combination of one or more schemes such as recognition and pure recall based or text and graphical password systems. One of the important graphical password schemes is Passpoint [3], a password is derived from the sequence of five click points on a given image and the user may select any pixel in the image as click points for their passwords.

M. Chau and H. Chen proposed the Web surfing, it has become increasingly difficult to search for relevant information using search engines [5]. Topic-specific is an alternative way search engines that support efficient information retrieval on the Web by providing more precise and customized searching in various domains. Developers of topic-specific search engines need to address two issues: how to locate relevant documents (URLs) on the Web and how to filter out irrelevant documents from a set of documents collected from the Web. Machine-learning-based approach is proposed which combines Web content analysis and Web structure analysis. Each Web page is represented by a set of content-based and link-based features which can be used for machine learning algorithms as the input. Implementation can be used as both a feed forward/back propagation neural network and a support vector machine. The experiments are designed and conducted to compare the proposed Web-feature approach with two existing Web page filtering methods - a keyword-based approach and lexicon-based approach. It has performed better than the benchmark approaches, when the number of training documents was small. This can be approached in Web applications such as Web content management and topic specific search engine.

Macro Vanetti, Elena Ferrari, and Moreno Carullo proposed a system that provides the user to have a straight rule over their own private wall to avoid the unwanted messages [6]. Here we provide users to have a straight control over messages posted on their own private space. Automated system called Filtered wall (FW) is used, which can filter unwanted messages .The system can blocks only the unwanted messages send by the user. Drawback of the system is that the user will not be blocked; only the content posted by the user will block .The system supports content based message filtering and short text classification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Mohamed Sylla proposed Combination Drag Pattern Graphical Password [7]. Here in the System one graphical keyboard is provided to user for selection of a password. During password selection the user has to choose set of characters from the graphical keyboard. The characters will be shown in textbox. User have to follow the sequence for creation of password. Then system checks password if it is not strong then system suggests different character between passwords. And to create a password user draws a pattern.

III. PROPOSED SYSTEM

Our system is based on Recognition Technique in which three group of image is used. Each group contains 25 images. User has to select at least one image from each group during registration phase. During login time user has to click on that images which is selected during registration phase. This system provide protection against shoulder surfing attack, dictionary attack, brute force attack using text password as well as graphical password. And also introduces the admin who controls all the filtering analysis done when ever any user sends or chats with the other. The information are in the database. The admin accesses this database and apply filtering techniques on each message content. We proposed a system allowing SNS users to have a direct control on the messages posted on their walls. This is achieved through a flexible rule-based system that allows users to customize the filtering criteria to be applied to their walls, in support of content-based filtering. If any user's message content is filtered immediately a pop up window will be displayed to that user saying that your message is filtered do you want to post the message .we have a filtering graph which represents how many bad words are used how many times by each user. The filtering technique we are using here is content based filtering which performs on the basis of content such as text. In existing system there is no content based filtering in our system we are implementing content based filtering. Once you login to admin we can know how many users are there, he can add filter words like vulgar, violence, Sexual, Offensive, Hate type of messages and filter these messages. The system architecture is as given below:

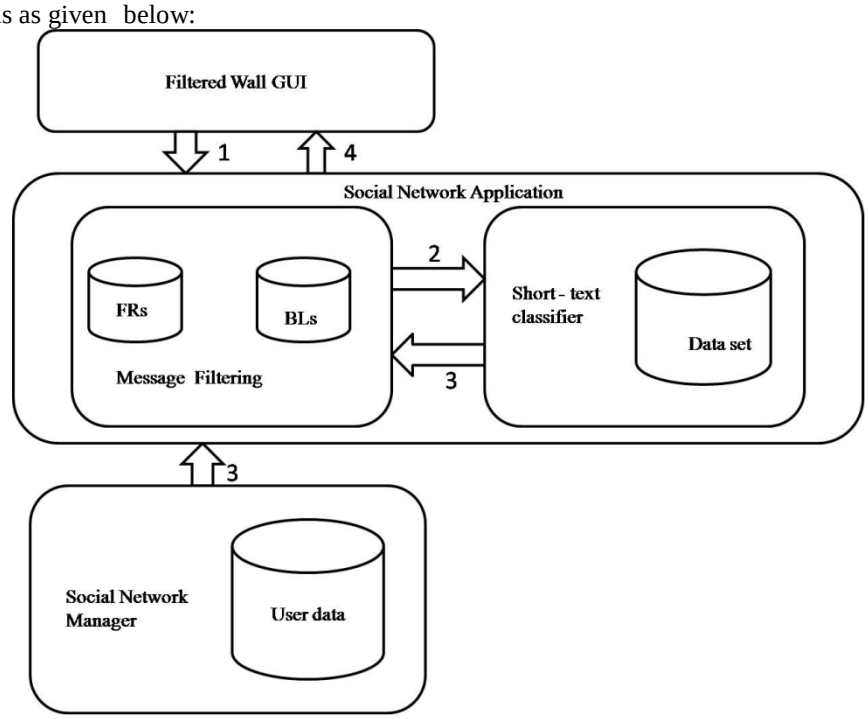


Fig 1: System Architecture

The SNS is a three-tier structure. The first layer called Social Network Manager (SNM) which aims to provide the basic SNS functionalities like profile. The second layer provides the support for external Social Network Applications (SNAs). The supported SNAs require an additional layer in turns for their Graphical User Interfaces (GUI). According to this architecture, the proposed system is placed in the second and third layers. The users interact with the system by means of a GUI to set up and manage their FRs and the GUI provides users with a FW. The core components of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

proposed system are the Content-Based Messages Filtering (CBMF) and the Short Text Classifier (STC) modules. The first component exploits the message categorization provided by the STC module to enforce the FRs specified by the user. Given below is the Data flow representation.

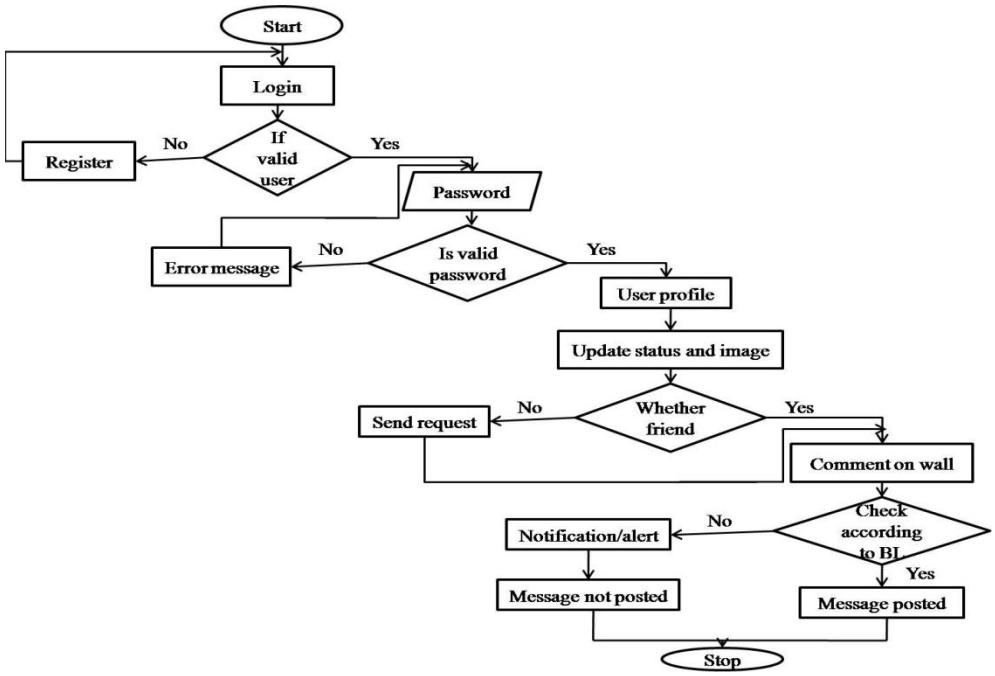


Fig 2: Data flow diagram

Designing and implementing a filtering System to provide users with classification mechanism to avoid they are overpowered by useless data. The path followed by a message, from its writing to the possible final publication can be summarized as follows:

1) User gets registered to the system.
2) User logs into the system.
3) User adds the other users available in the network as friends according to user's wish.
4) User may make use of the options available for filtering and also blacklisting option.
5) When he/she tries to comment on other's wall then, the sender will be the current user, and the receiver is the destination user to whom this message has to be posted.
6) In this checking the sender is checked with the list of users blacklisted in the receiver's blacklist. If match is found then message is discarded and cannot be posted, as the sender is blacklisted by the receiver.
7) If the sender is not blacklisted by the receiver, then the other check has to be made, this time it is for the message/ content of the comment to be posted to the receiver. This check is made with the filter of the receiver, if the message contains any of the words blocked by the receiver. If match is found then the message will be discarded due to the content not acceptable by the receiver.
8) Finally after the verification and testing is done, the message is either posted on the receiver's wall or discarded at the sender's end itself. Next the User may choose to continue some transactions or logout of the session.

IV. RESULTS

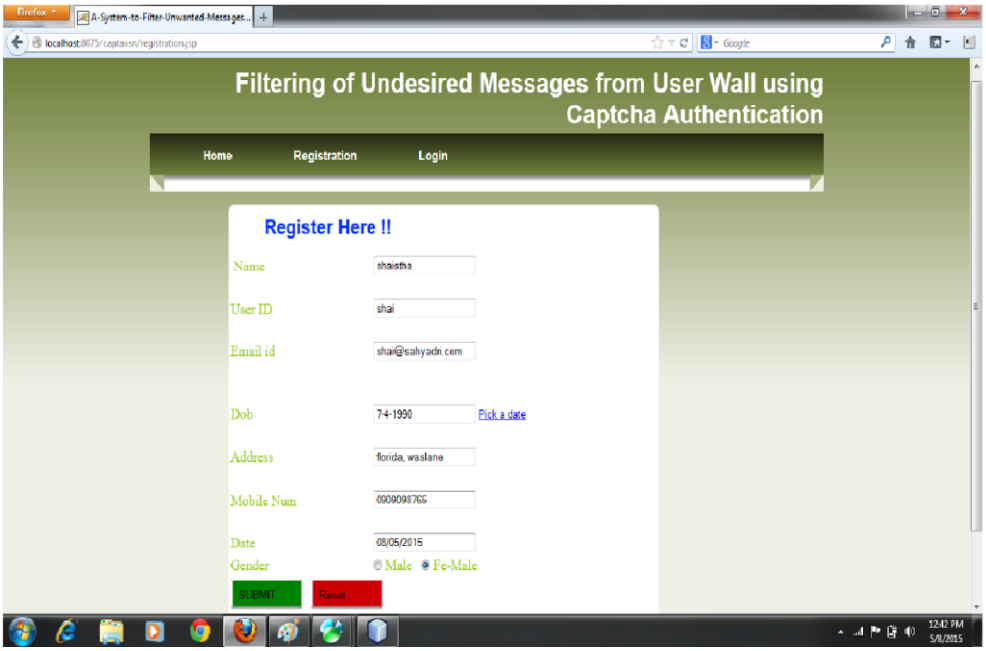
The snapshots given below gives a glance on the working of the proposed system. Snapshot1 provides new user to register into the system. User provides his/her details for registration. This page allows user to register to the system providing his name, user-id, email, date of birth, address, gender .It is mandatory for user to provide his mobile number and email id during registration. Validation is done for unique 10 digit mobile number and email id. The user can select his gender by selecting the appropriate radio button. The provided data are stored into the database of the system. Once all the fields in the registration form are filled, the user needs to click on submit button for successful registration.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

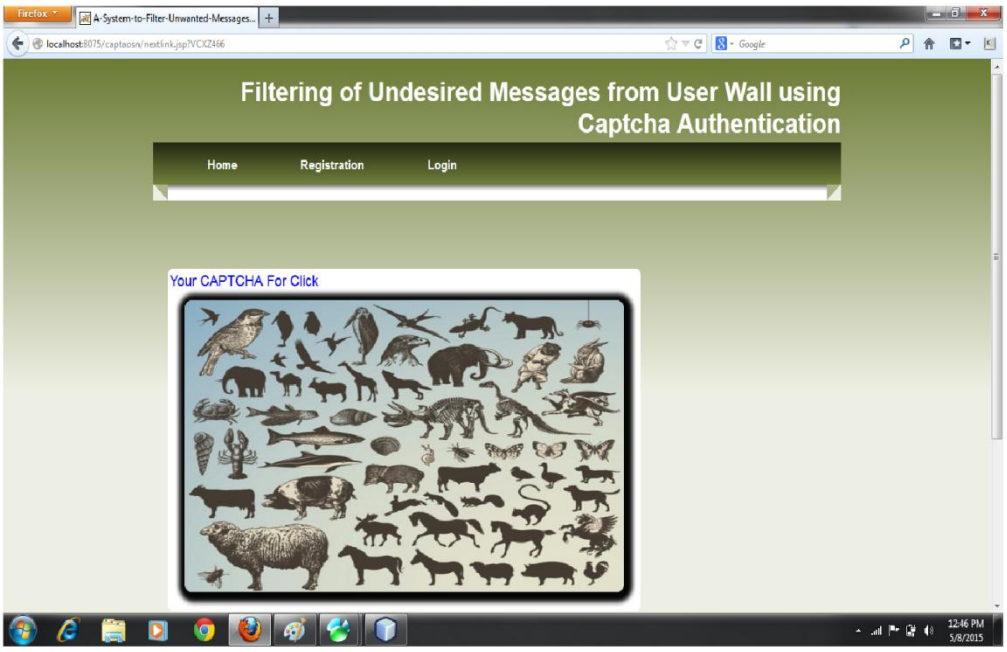
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015



Snapshot1: Login Page

Snapshot 2 The registered user can now log into the system. This is done by user, first selecting his stored profile image. This is followed by selecting a sequence of three images from the given image set. The sequence of images should be the same as selected during registration .this is the secret password of the user.



Snapshot 2: Authentication

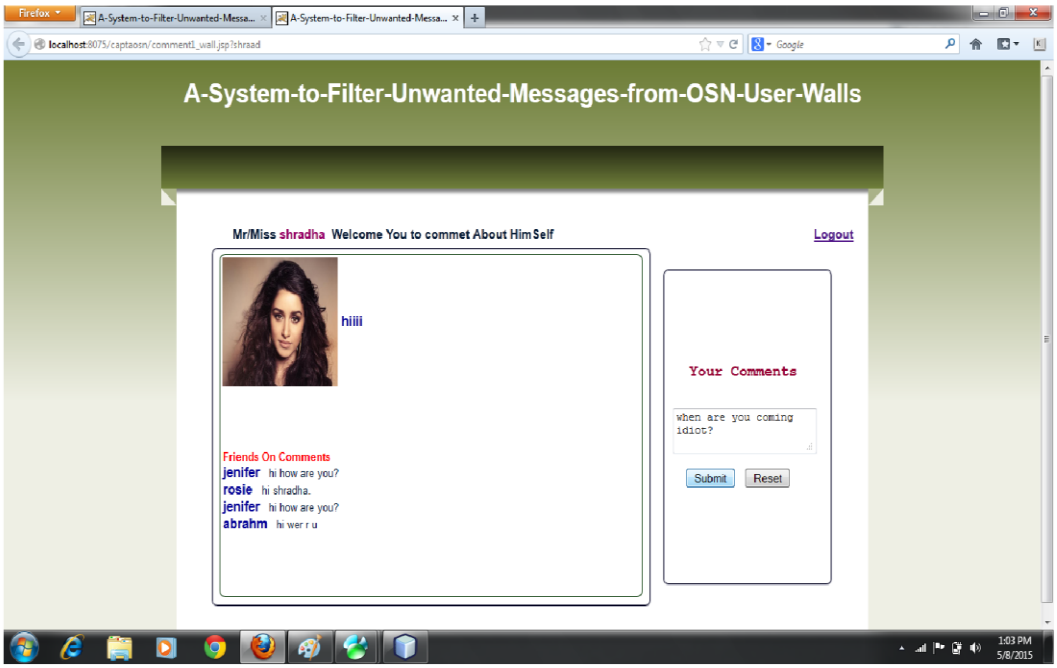
Snapshot 3 This page enables the valid user to view his/her profile. It enables the user to update status and profile image. New friends can be added by the user through this page. It allows to view all the comments posted by user on his/her walls. The user can also reply to the comments posted by their friends.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

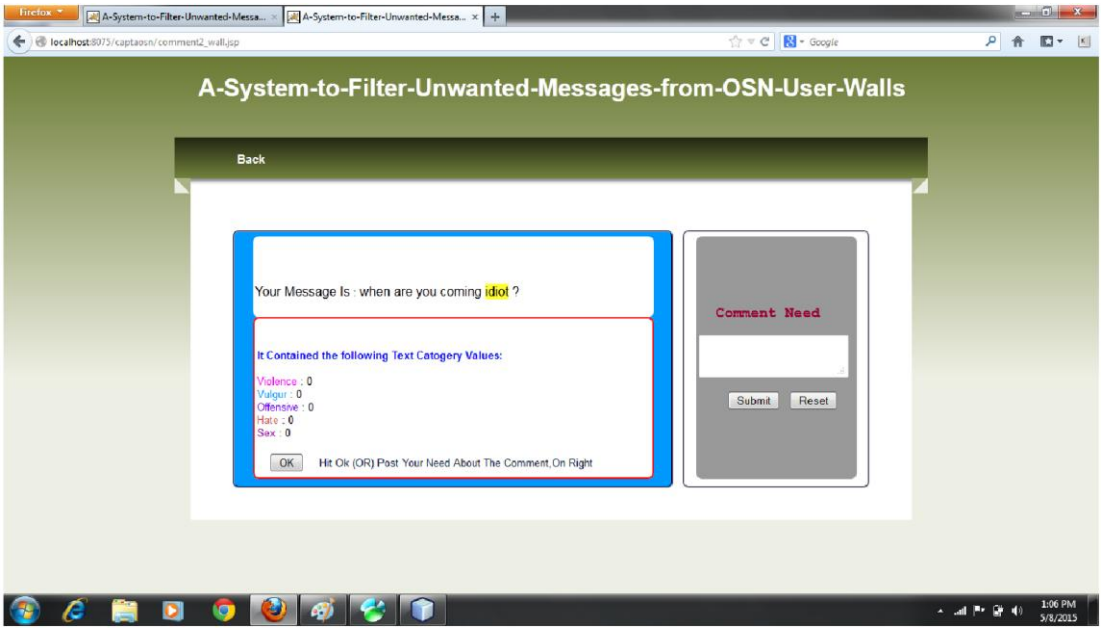
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015



Snapshot 3: User Wall

Snapshot 4 depicts the alert page. It displays an alert message on encountering any bad words by filtering it.



Snapshot 4: Notification/ Alert

V. CONCLUSION

Our graphical password system provides more security to data and protection against different attack. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide text password which

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

provide more security to data. A password of Carp can be found only by automatic online guessing attacks including brute-force attacks. A desired security property that other graphical password schemes lack. Hotspots in Carp images can no longer be exploited to count automatic online guessing attacks in many graphical password systems. And also we have presented a system to filter undesired content from user posting messages. Here the proposed system is limited to only certain extent. This is because our developed application is applicable or implemented in only one system. For example, two people can chat at a time using two different systems or through one system but ours is applicable to only one system. Even though this may be a difficulty problem in our proposed work our intention was providing privacy rather than simply implementing the existing features of social networking sites. We mainly focused on Privacy of users. The entire work is specifying filter rules/filter words is going to be done by the administrator. The proposed procedure can be applied to any other social networking sites like twitter, Gmail etc. The better privacy protection can be provided to users by using emerging data mining techniques.

.

ACKNOWLEDGMENT

I express my sincere gratitude to my guide, to the staff and management of my college, for their support and guidance to carry out the research.

REFERENCES

1. L. Von ahn, M. Blum, N. J. Hopper, and J. Landford, "Captcha: Using hard AI problem for security", in Proc.Eurocrypt, 2003, pp.294-311.
2. Ragavi V, Dr. G. Geetha "Captcha celebrating its Quattuordecennial – A Complete Reference", Department of Computer Applications, Sathyabama University, Chennai, India.
3. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks", in Proc. ACM CCS, 2002, pp.161-170.
4. R. Lin, S. Y. Huang, G. B. Bell, and Y. K. Lee, "A new CAPTCHA interface design for mobile devices", in Proc. 12th Austral. User Inter. Conf., pp. 3-8.
5. M. Chau and H. Chen, "A Machine Learning Approach to Web Page Filtering Using Content and Structure Analysis", Decision Support System, vol.44, no.2, pp.482-492, 2008.
6. Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, an Moreno Carullo, "A system to Filter Unwanted Messages from OSN User Walls", 2013.
7. Mohammed Sylla, Muhammad, Kaleem Habib and Jamaludin, Ibrahim, "Combinatoric Drag-Pattern Graphical Password", Journal of Emerging Trends in Computing Information Sciences, Vol.4, NO.12, Dec 2013.

BIOGRAPHY

Fathimath Shahistha M. is a 4th Semester M.Tech student, in the Computer Science and Engineering Department, Sahyadri College of Engineering and Management, Visveswaraya Technological University, India. Her research interests are Programming, Web Designing, Data mining etc.

Prabhaka B. K. is Associate Professor, in the Computer Science and Engineering Department, Sahyadri College of Engineering and Management, Visveswaraya Technological University, Mangaluru, India.