A SYSTEM TO FILTER UNWANTED MESSAGES FROM OSN

Mrs. KavithaBai A.S [1], Shabnam[2], SaiRevathi M[3]
[1.]Assistant Professor, Department of CSE, Vemana Institute of Technology, Bangalore.
[2, 3]UG student, Department of CSE, Vemana Institute of Technology, Bangalore.
kavithabai.pawar@gmail.com , [2.]shabnam.hannan786@gmail.com, [3.]revathi.malikireddy@gmail.com.

Manuscript History
Number: IRJCS/RS/Vol.06/Issue06/JNCS10103
Received: 29, May 2019
Final Correction: 30, May 2019
Final Accepted: 02, June 2019
Published: June 2019
doi://10.26562/IRJCS.2019.JNCS10103
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

ABSTRACT - One crucial issue in the present Online Social Networks (OSNs) is to enable clients to control the messages that are posted individually private space to evade that undesirable substance is shown. Up to now, OSNs give little help to this necessity. To fill the hole, in this paper, we propose a framework that permit OSN clients to have an immediate control on the messages that are posted on their dividers. This is accomplished through an adaptable standard based framework, which enables clients to change the separating criteria that is connected to their dividers, and a Machine Learning-based soft classifier consequently naming messages in help of content based filtering.

KEYWORDS – Online Social Network, Message Filter, Soft Classifier, Content-based filtering.

I. INTRODUCTION

ONLINE Social Networks (OSNs) are today a standout amongst the most mainstream intuitive medium to convey, share, and spread a lot of human life data. Every day and constant correspondences shows the trading of a few kinds of content, including free content, picture, sound, and video information. The enormous and dynamic character of these information makes the announcement for the work of web substance mining systems that have an expect to consequently find helpful data inside the information. The point of most of these proposition is chiefly to give clients a characterization component to evade they are overpowered by useless information. In OSNs, data separating can likewise be utilized for an alternate, progressively delicate, reason. This is a direct result of the way that in OSNs there is the likelihood to post or remark different posts on specific open/private zones, brought all in all dividers. Data sifting can along these lines be utilized to enable clients to naturally control the messages that are composed individually dividers, by separating the undesirable messages[1]. Content-based inclinations are not supported and subsequently it is beyond the realm of imagination to expect to forestall messages that are not needed, for example, political or obscene ones, regardless of the client who posts them. Giving this administration isn't just a matter of utilizing recently characterized web substance digging procedures for an alternate application, rather it is important to structure specially appointed characterization systems.

In OSNs, information filtering can also be used for a different, more sensitive, purpose. This is because of the fact that in OSNs there is it is possible to post or comment other posts on particular public/private areas, called in general walls. Information filtering can be used to give users the ability to automatically control the messages that are written on their own walls, by filtering unwanted messages. We believe that this is a key OSN service that has not been provided so far. Today OSNs provide very little support to prevent unwanted messages on user walls. For example, Facebook allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends).

However, content-based preferences are not at all supported and therefore it is not possible to prevent messages that are not wanted, such as political or vulgar ones, no matter of the user who posts them. Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it required that we need to design ad hoc classification strategies. This is because wall messages are constituted by short text for which traditional classification methods have some serious limitations since small texts does not provide sufficient word occurrences. The aim of the present work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW), that is helpful to filter unwanted messages from OSN user walls[4]. We make use of Machine Learning (ML) text categorization techniques to automatically assign with each small text message a set of categories based on the content of it. The major efforts in building a robust short text classifier (STC) are concentrated in the removal and selection of a set of characterizing and discriminant features.The solutions that are researched in this paper are an addition of those that are adopted in a previous work by us from which we derive the learning model and the procedure to generate pre-classified data. The original set of features, derived from external properties of short texts, is enlarged here including exogenous knowledge related to the context from which the messages are created. As far as the learning model is concerned, from the current paper we confirm that the use of neural learning which is today identified as one of the most efficient solutions in text classification. In particular, we base the overall short text classification strategy on Radial Basis Function Networks (RBFN) for their capabilities that are proven in acting as soft classifiers, that manage noisy data[9]. Moreover, the speed in performing the learning phase creates the statement for a satisfactory use in OSN domains, as well as facilitates the experimental evaluation tasks. However, the design of these audit-based tools is complicated by some issues, like the conclusions an audit system might have on users privacy and/or the limitations on what it is possible to audit in current OSNs. A work that is prepared in this direction is done in the context of trust values that are used for OSN access control purposes. However; we would like to remark that the system proposed in this paper represents just the core set of functionalities that are needed to provide a sophisticated tool for OSN message filtering. Even if we have complemented our system with an online assistant to set FR thresholds, the development of a complete system easily usable by average OSN users is a wide topic which is out of the scope of the current paper [6].

The proposed system may suffer of problems which are similar to the one that is encountered in the specification of OSN privacy settings. In this context, many studies have shown that average OSN users have difficulties in understanding the very simple privacy settings which are provided by today OSNs. To overcome this problem, a promising trend is to reduce the data mining techniques to reduce the best privacy preferences to suggest to OSN users, on the basis of the available social network data. Filtering is very much similar to access control. Actually, content filtering can be considered as an extension of access control, just because it can be used to protect objects from unauthorized subjects, as well as subjects from objects that are not suitable. In the field of OSNs, the majority of access control models proposed so far causes topology-based access control, according to which access control requirements are shown in terms of relationships that the one who request should have with the resource owner.

II. METHODOLOGY

Design is a strategic approach for someone to achieve an expectation that is somewhat different. It defines specifications, plans, parameters, costs, activities, processes [11]. A design approach is a general philosophy for specific approach to guide the overall goal of the design. Design is rarely perfect and sometimes repetitive. In this project the server sends the packets through multicast stream via the router where digitally signing takes place with the help of private key. The router forwards the packets to the clients and verification takes place using the public key at the client side. Architecture is both the process and product of planning, designing and construction. Fig 1 depicts the system architecture. In the material form of buildings, the architectural works are often regarded as cultural symbols and as works of art. Historical civilizations are often identified with their surviving architectural achievements. Architecture is a medium of cultural expression displayed using a specific set of principles. These principals try to explain the meaning so that the culture of a period or a nation can be fully expressed and understood. Architectural design is the starting of design process of identifying sub-systems and to provide a support for sub-system control and communication. Using large-grain components improves performance, and using fine-grain components improves maintainability, so if both of these are important system requirements developers should find some compromise solution. There is an overlap between the process of requirements engineering and architectural design.

Sub-system design is a splitting of a system into large components, each of which may be an essential system in its own right[3]. Block diagrams are used to describe sub-system designs in which each box that is shown in the diagram represents sub-system. Sub-systems can have their own sub-systems, in that case boxes are placed into boxes. Arrows means that data and or control signals are moved from sub-system to sub-system in the direction of the arrows. Architectural design is a creative process so many decisions are made based on the requirements, specific rules for particular project and the experience of the architect.

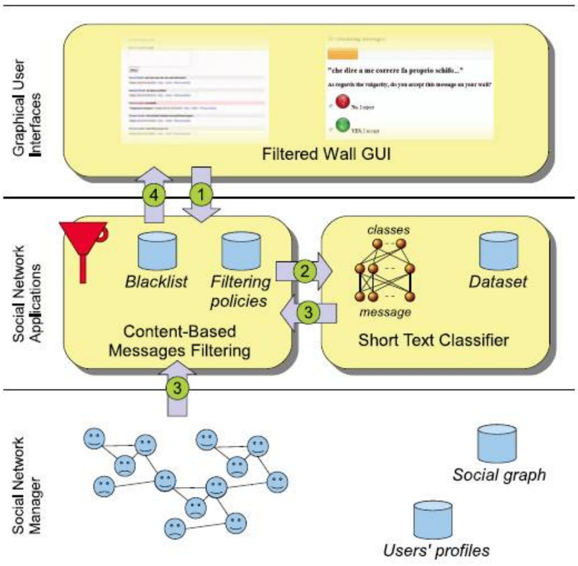
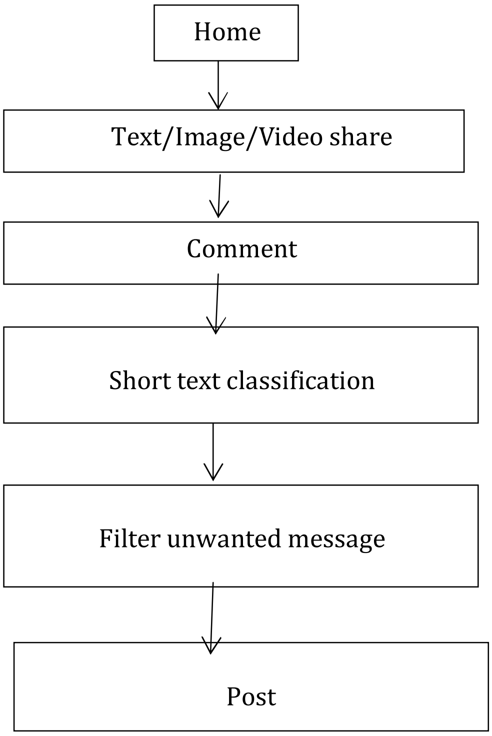


Fig.1 System Architecture

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling the process of architecture as shown in Fig 2. They are a prepared step that is used to create an overview of the system that can be developed later. DFDs can also be used for the visualization of data processing (structured design).



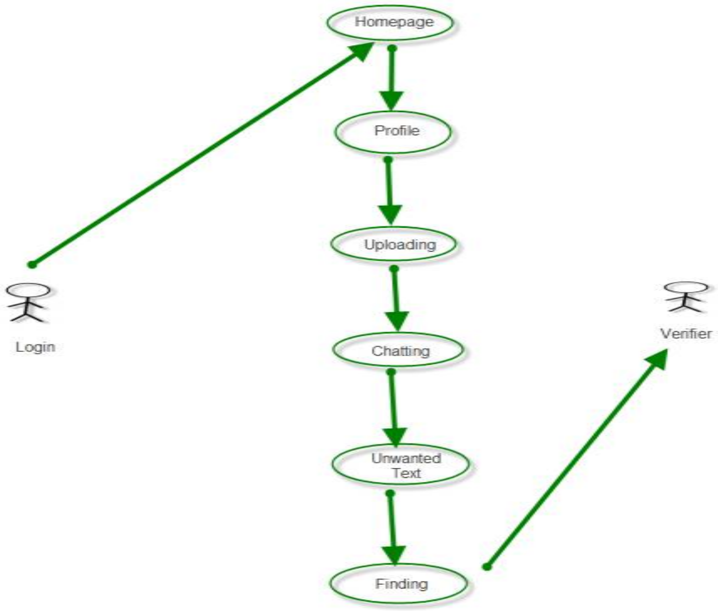


Fig. 3 Use Case Diagram

As shown in Fig 3, here the user will create a account and login. His/her profile will be created were he/she can upload a picture, make friends, send messages, and avoid unwanted messages being uploaded.

III. IMPLEMENTATION

Implementation is the stage of the project when the design that is detailed is resulted into a working system. Therefore it said to be the most critical stage to achieve a successful new system and giving the user more confidence that the new system will work properly in an effective way. The implementation stage include planning very carefully, researching about the existing system and the limitations on implementation, designing of methods to bring a complete change and evaluation of the methods that are changed[7]. It consists of five modules, they are: Online Social Networks, Filtering of the Information, Classification of the Short Text, Policy Based Personalization, Blacklist.

A. Online Social Networks

The only social networking service in which we have some knowledge to provide filtering abilities to its users is My WOT, this is a social networking service which gives its subscribers the ability to rate resources with respect to the four criteria[10]. Those four criteria are: trustworthiness, vendor reliability, privacy, and child safety specify preferences which determine whether the browser should be blocked or not. Frameworks are very powerful and general enough to be modified and/or made larger for different application scenarios they have not been specifically created to address information filtering in OSNs and therefore to consider the user social graph in the policy specification process. So, it is better to prefer to define our own abstract and more compact policy language, instead of extending one of the above-mentioned ones.

B. Information Filtering

Filtering is very similar to access control. Actually, content filtering can be considered as an extension of access control, because it can be used to protect objects from unauthorized subjects, and also to subjects from objects which are not suitable. Filtering policy language extends the languages proposed for access control policy specification in OSNs to deal successfully with the extended requirements of the filtering domain. We are dealing with filtering of unwanted contents instead of dealing with the access control, one of the key ingredients of our system is the availability of a description for the message contents that are to be used by the filtering mechanism.

C. Short Text Classification

Exploiting classification mechanisms for personalizing access in OSNs. For instance, in, a classification method is proposed to categorize short text messages because to avoid overwhelming users of micro blogging services by raw data[2]. The system is described in focuses on and associated with a set of categories with the each and every tweet describing the content of it. Filtering criteria which is very less flexible than the Filtered Wall because they are based only on the four criteria that are mentioned above.

D. Policy-Based Personalization

In probabilistic text classifiers which are very hard classifiers in nature and they do not easily combine soft, multimember ship paradigms. In our scenario, we consider gradual membership to classes a key feature to define the policy-based personalization strategies that are flexible[8]. The application of content-based filtering on messages that are posted on the OSN user walls poses additional challenges that are given the small length of these messages other than the wide range of topics that can be discussed. Short text classification has received a little bit of attention in the scientific community.

E. Blacklists

Another component of our system is a Batch Learning (BL) mechanism to avoid messages from some unwanted creators, which are independent from their contents. BLs are managed by the system directly, which should be able to determine who are the users that are to be inserted in the BL and decide when the users have some control in the BL is finished. To improve the flexibility, such type of information is given to the system through a set of rules that are called as the BL rules. This type of rules is not defined by the SNMP; so, they are not meant as general high-level directives that are to be applied to the whole community. Instead of that, we decide to let the users themselves, i.e., the wall's owners to specify BL rules regulating who has to be banned from their walls and for how much long time they must be banned.

Therefore, at the same time, the user might be banned from all, and able to post in other walls. Similar to FRs, our BL rules make the wall owner able to identify users that are to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means a BL rule, wall owners are, for example, able to ban from their walls users they do not directly know (i.e., with which they have only indirect relationships), or users that are friend of a given person because they may have a little bad opinion of his person. This banning can be adopted for a time period that is not determined or for a specific time window. Moreover, banning criteria may also take into account users' behavior in the OSN[5]. Among possible information watching the bad behavior of the user we have focused on two main measures. The first measure is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for some more time, because his/her behavior is not improved. This principle works for those users that have been already inserted in the considered BL at least one time. To catch new bad behavior we use the Relative Frequency (RF) that let the system be able to detect those users whose messages continue to fail the FRs. The two measures can be calculated either locally, that is, by considering only the messages and/or the BL of the user specifying the BL rule or globally, that is, by considering all OSN users walls and/or BLs.

I. PSEUDO CODE

$$tf - idf(t_k, d_j) = \#(t_k, d_j) \cdot \log \frac{|\mathcal{T}_r|}{\#\mathcal{T}_r(t_k)},$$

$$\phi(m_a, m_b) = \frac{1}{2} + \begin{cases} m_b/10 & \text{if } m_a = Filter \\ -m_b/10 & \text{if } m_a = Pass. \end{cases}$$

II. EVALUATION

This section, we illustrate the performance evaluation study we have carried out the classification and filtering modules. Here we start by describing the data set. The analysis of related work has made a special attention on the lack of publicly available benchmark for comparing different type of approaches to content-based classification of OSN short texts. To deal with this lack, we have built and made a data set D of messages available and taken from the Face book. One thousand two hundred and sixty-six messages from publicly accessible Italian groups have been selected and calculated by means of an automated procedure that removes undesired spam messages and, for each message, stores the body of the message and the name of the group from which it originates. The messages come from the group's webpage section, where any registered user can post a new message or reply to messages that are already posted by other users. The role of the group's name within the text representation features was explained already. The set of classes considered in our experiments is ¼ of Neutral, Violence, Vulgar, Offensive, Hate, where these words are the second-level classes. The percentage of elements in D that belongs to the Neutral class is 31 percent. In order to deal with intrinsic ambiguity in assigning messages to classes, we conclude that a given message belongs to more than one class. Each message here is labeled by a group of five experts and the class membership values for a given message were computed by a majority voting procedure. After the ground-truth collection phase, the messages are selected to balance as much as possible second-level class occurrences. The group of experts has been chosen in an attempt to ensure high heterogeneity concerning sex, age, employment, education, and religion. In order to create a consensus concerning the meaning of the Neutral class and general criteria in assigning multiclass membership we invited experts to participate to a dedicated tuning session. Issues that are based on the behavior between the opinions of experts and the impact of the data set size in ML classification tasks will be discussed and evaluated. We are aware of the fact that the extreme diversity of OSNs content and the continuing evolution of communication styles create the need of using several data sets as an reference benchmark. We hope that our data set will also cover the way for a quantitative and more precise analysis of OSN short text classification methods.

iii Short Text Classifier Evaluation

We hope that our data set will also cover the way for a quantitative and more precise analysis of OSN short text classification methods. Two different types of measures are present and these measures will be used to form an idea of the effectiveness of first-level and second-level classifications. In the first level, the short text classification procedure is evaluated on the basis of the contingency table approach. In particular, the derived well-known Overall Accuracy (OA) index capturing the simple percent agreement between truth and classification results, is complemented with the Cohen's KAPPA (K) coefficient thought to be a more robust measure taking into account the agreement occurring by chance.

The lack of benchmarks for OSN short text classification makes the development very problematic of a reliable comparative analysis. A comparison of our method can be done indirectly with work that shows the similarities with our solution. A study that responds to these characteristics is proposed where a classification of incoming tweets into five categories is described. Similarly to our approach, messages are very short and represented in the learning framework with both internal, content-based and contextual properties contextual features are found to be very discriminative and BoW considered alone does not reach a satisfactory performance. Best numerical results that are obtained in our work are comparable with those obtained in. Limiting to accuracy index, which is the only metric used in, our results are slightly inferior, but this result must be explained by considering the following aspects. First we use a much smaller set of reclassified data (1,266 versus5,407), and this is an advantage over the tweets classification considering the efforts in manually reclassifying messages with an a level of consistency that is must be accepted. Second, the classes we considered have a more degree of vagueness, since their semantics is closely linked to subjective interpretation. A second work provides each one a comparative evaluation. The authors deal with the short text classification using a statistical model that are named Prediction by Partial Matching (PPM), without feature engineering. However, their study is described to text that contains complex terminology and prove that the classifier on medical texts from Newsgroups, clinical texts, and Reuters-21,578.7 These differences may lower the level of reliability in comparison. In addition, we observe that the performance reported in is strongly affected by the data set used in the evaluation. If we consider results in obtained on clinical texts our classifier with the best results of Prec. 0.76, Recall 0.59, is considerably higher than PPM classifier (Prec. 0.3 Home6, Recall 0.42). It has a comparable behavior, if we consider the averaged performance on three Reuters subsets (Prec. 0.74, Recall 0.63) and slightly inferio when considering the newsgroups data set (Prec. 0.96, Recall 0.84).

In order to provide an overall assessment of how effectively the system applies a FR, we look again at Table 2. This table allows us to have an estimation of the Precision and Recall of our FRs, since values reported in Table 2 have been computed for FRs with content specification component set to ðC; 0:5Þ, where C 2. If suppose the system applies a given rule on a particular message. As such, Precision reported the level of possibility that the decision taken on the considered message (that is, blocking it or not) is actually the correct one. In contrast, Recall has to be interpreted as the probability that, given a rule that must be applied over a certain message, the rule is really enforced. Let us now discuss, with some examples, the results presented in, which reports Precision and Recall values. K value obtained training the model with different fractions of the original training set. Results that are achieved by the content-based specification component, on the first-level classification can be considered as good enough and reasonably aligned with those obtained by well-known information filtering techniques. Results obtained for the content-based specification component on the second level are slightly less brilliant than those obtained for the first, but we should interpret this in view of the intrinsic difficulties in assigning to a messages a semantically most specific category. However, the analysis of the features reported shows that the introduction of contextual information (CF) significantly improves the ability of the classifier to correctly distinguish between non-neutral classes. This result makes more reliable all policies exploiting non-neutral classes, which are the majority in real-world scenarios.

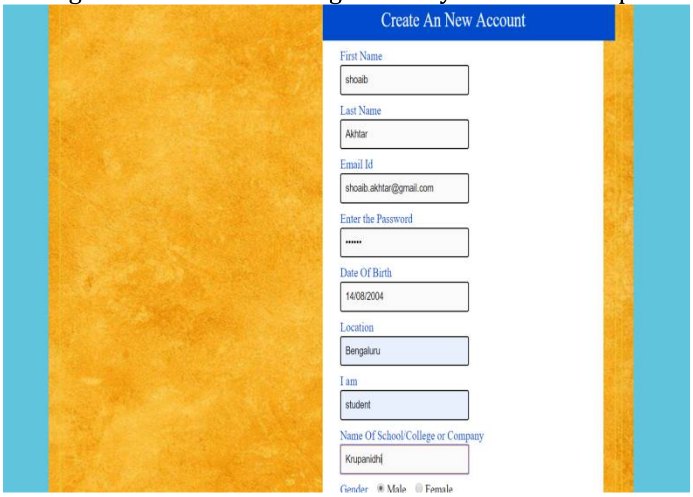
DicomFW is a model Facebook application that mirrors an individual wall where the client can apply a straightforward blend of the proposed FRs. All through the advancement of the model, we have concentrated all the more just on the FRs by leaving the BL usage as a future improvement. Notwithstanding, the executed usefulness is basic since it allows the STC and CBMF segments to collaborate. What's more, since this application is considered as a wall and not as a group, the logical data (from which CF are removed) are connected to the name of the gathering that are not accessible straightforwardly. Logical data that is as of now utilized in the model is in respect to the gathering name where the client that composes the message is generally dynamic.

As a future extension, we want to integrate contextual information that is related to the name of all the groups in which the user participates, appropriately weighted by the participation level. It is important to stress that this type of contextual information is related to the environment preferred by the user who wants to post the message; thus, the experience that you can try using DicomFW is consistent with what described and evaluated. To summarize, our application permits to

1. View the list of users' FWs;
2. View the messages and post a new one on a FW;
3. Define the FRs using the OSA tool.

IV. RESULTS

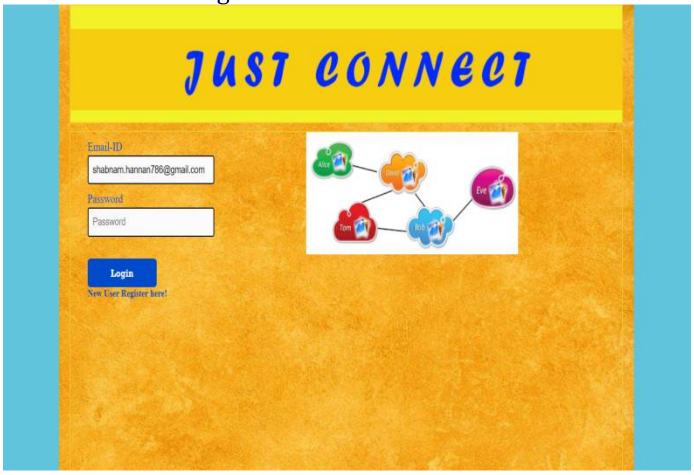
This is starting phase of our project where we implement our conceptual and design view to our desired project. Here we used java functions to give an organized and structured view to propose an overall architecture of our project. As shown in Fig 4,User creates his/her account by providing his/her credentials. Fig 5 illustrates that User ID and Password will be created using which the user can login. Finally the user can upload image as shown in Fig 6.



Create An New Account

First Name: shoaib
Last Name: Akhtar
Email Id: shoaib.akhtar@gmail.com
Enter the Password: ••••••
Date Of Birth: 14/08/2004
Location: Bengaluru
I am: student
Name Of School/College or Company: Krupanidhi
Gender ● Male ○ Female

Fig. 4 Create New Account



JUST CONNECT

Email-ID: shabnam.hannan786@gmail.com
Password: Password

Fig.5 Login Page

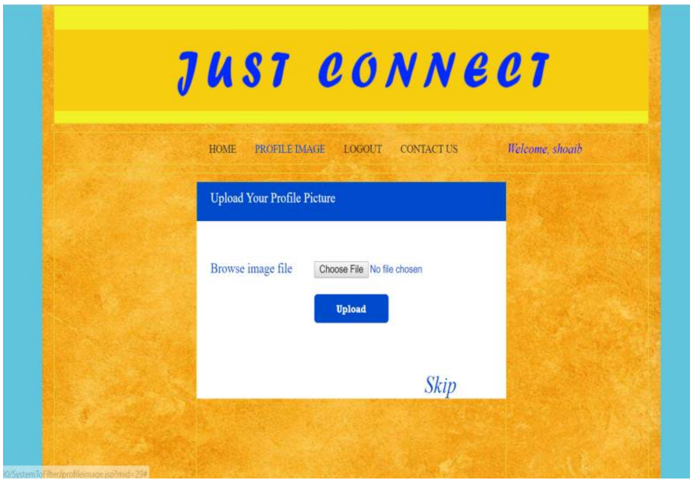
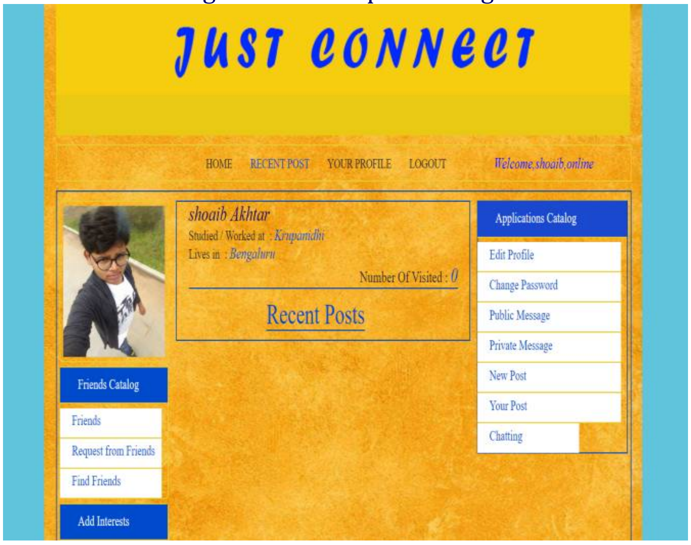


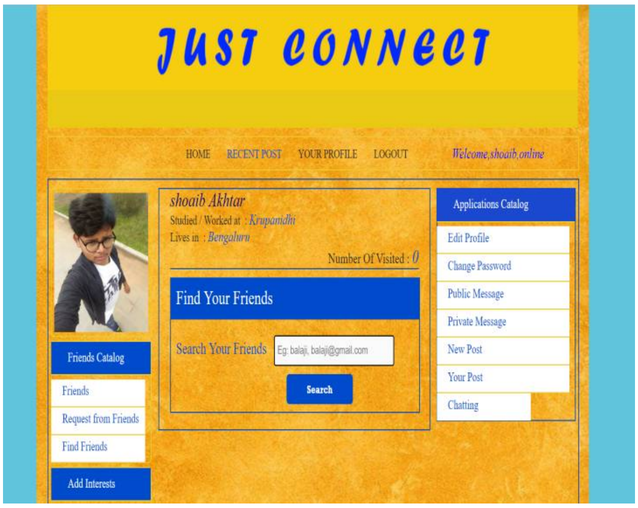
Fig. 6 User can upload Image



shoaib Akhtar
Studied / Worked at : Krupanidhi
Lives in : Bengaluru
Number Of Visited : 0

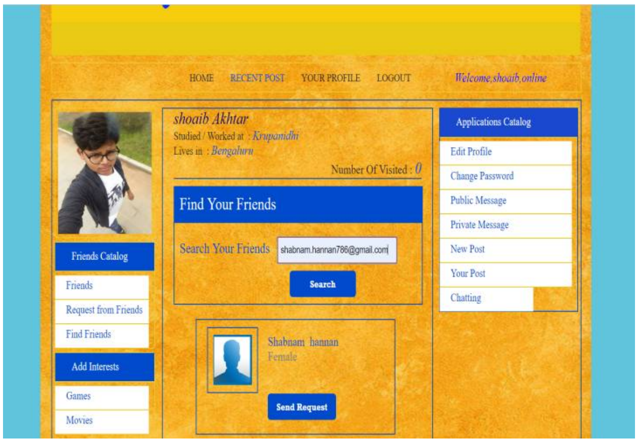
Fig.7 Profile View

The following Fig 8, 9, 10, 11illustrates the option to search a friend, view their profile, send a request and view the requests sent by the other friends.



shoaib Akhtar
Studied / Worked at : Krupanidhi
Lives in : Bengaluru
Number Of Visited : 0

Fig.8 Option for Search



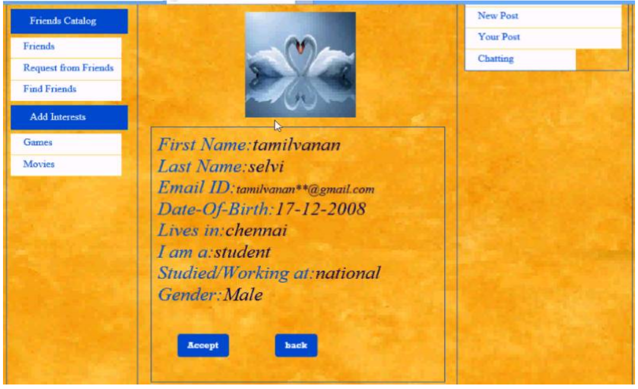
shoaib Akhtar
Studied / Worked at : Krupanidhi
Lives in : Bengaluru
Number Of Visited : 0

Find Your Friends

Search Your Friends shabnam.hannan786@gmail.com

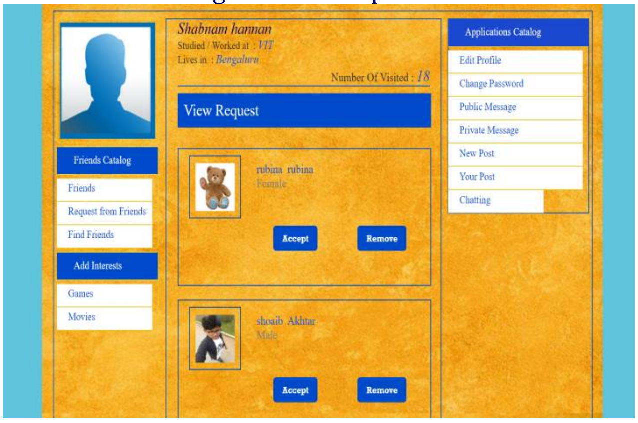
Shabnam hannan
Female

Fig. 9 Search Found



First Name:tamilvanan
Last Name:selvi
Email ID:tamilvanan**@gmail.com
Date-Of-Birth:17-12-2008
Lives in:chennai
I am a:student
Studied/Working at:national
Gender:Male

Fig. 10 Friend's profile



Shabnam hannan
Studied / Worked at : VIT
Lives in : Bengaluru
Number Of Visited : 18

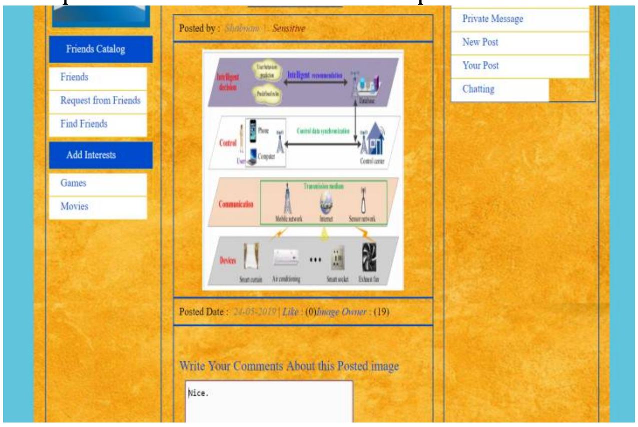
View Request

rubina rubina
Female

shoaib Akhtar
Male

Fig. 11View Request

The following Fig 12 illustrates the option to comment on a friend's photo.



Posted by : Shabnam | Sensitive

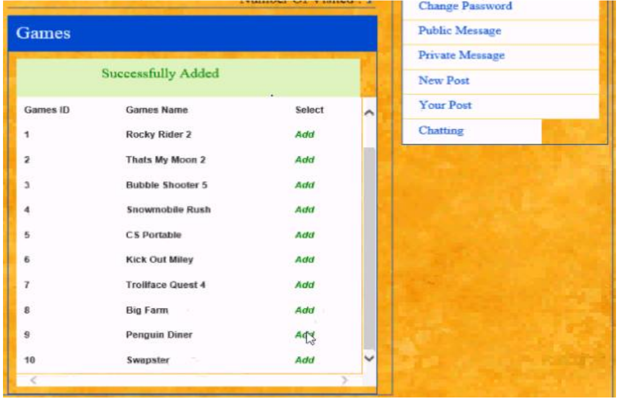
Posted Date : 24-05-2019 | Like : (0)Image Owner : (19)

Write Your Comments About this Posted image

Nice.

Fig. 12 User can Comment

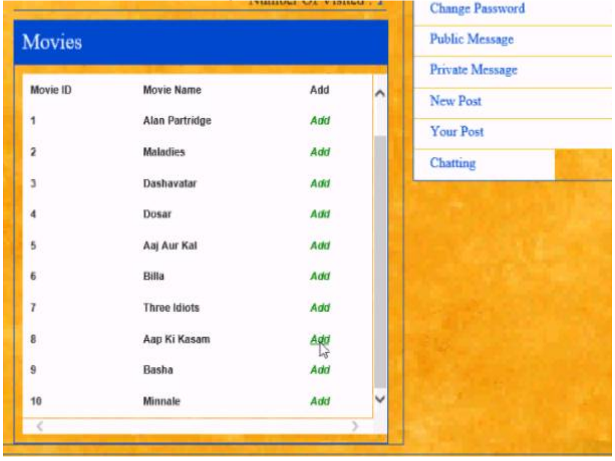
The following Fig 13and Fig 14shows the page where favorite movies and games can be added to the profile.



Successfully Added

Games ID	Games Name	Select
1	Rocky Rider 2	Add
2	Thats My Moon 2	Add
3	Bubble Shooter 5	Add
4	Snowmobile Rush	Add
5	CS Portable	Add
6	Kick Out Miley	Add
7	Trollface Quest 4	Add
8	Big Farm	Add
9	Penguin Diner	Add
10	Swapster	Add

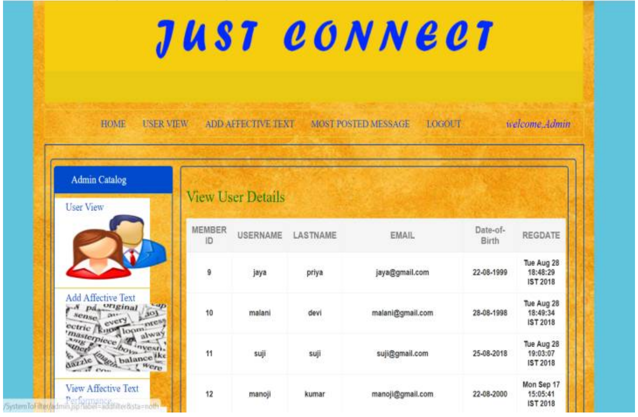
Fig. 13 Add Games



Movie ID	Movie Name	Add
1	Alan Partridge	Add
2	Maladies	Add
3	Dashavatar	Add
4	Dosar	Add
5	Aaj Aur Kal	Add
6	Billa	Add
7	Three Idiots	Add
8	Aap Ki Kasam	Add
9	Basha	Add
10	Minnale	Add

Fig. 14 Add Movies

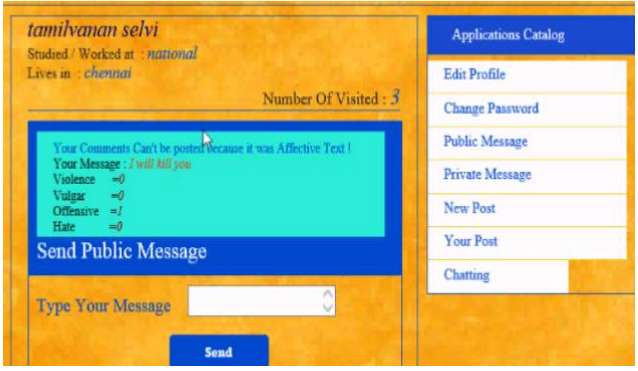
The below Fig 15 illustrates the admin login catalogue and user details, a filtering message page with categorization.



View User Details

MEMBER ID	USERNAME	LASTNAME	EMAIL	Date-of-Birth	REGDATE
9	jaya	priya	jaya@gmail.com	22-08-1999	Tue Aug 28 18:48:29 IST 2018
10	malani	devi	malani@gmail.com	28-08-1998	Tue Aug 28 18:49:34 IST 2018
11	suji	suji	suji@gmail.com	25-08-2018	Tue Aug 28 19:03:07 IST 2018
12	manoji	kumar	manoji@gmail.com	22-08-2000	Mon Sep 17 15:05:41 IST 2018

Fig. 15 Admin Login



tamilvanan selvi
Studied / Worked at : national
Lives in : chennai

Number Of Visited : 3

Your Comments Can't be posted because it was Affective Text !
Your Message : I will kill you
Violence =0
Vulgar =0
Offensive =1
Hate =0

Fig. 16 Filters Unwanted Messages

V. CONCLUSION

Here we have displayed a framework to channel messages that are undesirable from OSN walls. The framework utilize a ML soft classifier that causes adaptable content subordinate FRs. Also, the adaptability of the framework regarding separating alternatives is upgraded through the administration of BLs. This work is the initial step of a more extensive venture. The early reassuring outcomes we have on the classification procedure brief us to proceed with other work that will plan to the better nature of classification. Specifically, the tentative arrangements consider a more profound examination on two interdependent tasks. The primary task is identified with the removal and/or selection of contextual highlights that have been appeared to have a high discriminative power. The secondary task incorporates the learning stage. Since the hidden area is changing, the gathering of pre classified data probably won't be agent in the more drawn out term. The present clump learning technique, that depends on the preliminary collection of the whole set of labelled data from specialists, permitted an exact trial assessment however should be created to include new operational requirements.

REFERENCES

1. A. Adomavicius and G. Tuzhilin, "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions," IEEE Trans. Knowledge and Data Eng., vol. 17, no. 6, pp. 734-749, June 2005.
2. M. Chau and H. Chen, "A Machine Learning Approach to Web Page Filtering Using Content and Structure Analysis," Decision Support Systems, vol. 44, no. 2, pp. 482-494, 2008.
3. R.J. Mooney and L. Roy, "Content-Based Book Recommending Using Learning for Text Categorization," Proc. Fifth ACM Conf. Digital Libraries, pp. 195-204, 2000.
4. F. Sebastiani, "Machine Learning in Automated Text Categorization," ACM Computing Surveys, vol. 34, no. 1, pp. 1-47, 2002.
5. M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari, "Content-Based Filtering in On-Line Social Networks," Proc. ECML/PKDD Workshop Privacy and Security Issues in Data Mining and Machine Learning (PSDML '10), 2010.
6. N.J. Belkin and W.B. Croft, "Information Filtering and Information Retrieval: Two Sides of the Same Coin?" Comm. ACM, vol. 35, no. 12, pp. 29-38, 1992.
7. P.J. Denning, "Electronic Junk," Comm. ACM, vol. 25, no. 3, pp. 163-165, 1982.
8. P.W. Foltz and S.T. Dumais, "Personalized Information Delivery: An Analysis of Information Filtering Methods," Comm. ACM, vol. 35, no. 12, pp. 51-60, 1992.
9. P.S. Jacobs and L.F. Rau, "Scisor: Extracting Information from On- Line News," Comm. ACM, vol. 33, no. 11, pp. 88-97, 1990.
10. S. Pollock, "A Rule-Based Message Filtering System," ACM Trans. Office Information Systems, vol. 6, no. 3, pp. 232-254, 1988.
11. P.E. Baclace, "Competitive Agents for Information Filtering," Comm. ACM, vol. 35, no. 12, p. 50, 1992.
12. P.J. Hayes, P.M. Andersen, I.B. Nirenburg, and L.M. Schmandt, "Tcs: A Shell for Content-Based Text Categorization," Proc. Sixth IEEE Conf. Artificial Intelligence Applications (CAIA '90), pp. 320- 326, 1990.