ISSN: 0974-5823 Vol. 7 No. 5 May, 2022

International Journal of Mechanical Engineering

FILTERING OF UNWANTED MULTIMEDIA MESSAGES FROM ONLINE SOCIAL NETWORK USER WALLS

Martand Ratnam[1]

M Tech Scholar, Department of Computer Science, BBDIT Ghaziabad, AKTU Lucknow Uttar Pradesh , INDIA

Prof.(Dr.) Shwetav Sharad[2]

Department of Computer Science, BBDIT Ghaziabad, AKTU Lucknow Uttar Pradesh , INDIA Corresponding

Prof.(Dr.) Santosh Kumar Shukla[3]

Department of Computer Science, BBDEC Lucknow, AKTU Lucknow Uttar Pradesh , INDIA

ABSTRACT

Many sorts of information can be shared, communicated, and exchanged via online social networks (OSNs) in today's world: text, images, audio and video. All of this openly shared material seen by others who are linked to the blog or network, and this is having a huge social impact on the human mind. If you use the wall, you run the risk of posting or commenting on things like spam or confidential information that should be kept private. Because it may be used to remove unused terms from public communications, information filtering can help social media sites like Facebook and Twitter function better. Using information filtering, we've created a system that allows OSN users to post and remark on their walls directly. To prevent spam, the wall uses Filtering and Black List Rules to sort messages posted by users. Users' walls will display messages that do not breach filtering or blacklist criteria.

Keywords: Demographic Filtering ,Collaborative Filtering, Content Based Message Filtering, On-line Social Networks

1. INTRODUCTION

It is possible to connect people based on shared interests, hobbies, and a significant quantity of personal data using a social networking service, for example : “All of these sorts of content must be exchanged on a daily basis in order to maintain a constant flow of communication.” People of all ages and backgrounds are increasingly spending time on social networking sites to communicate, share data, and seek common interests as a result of social media's rapid rise in recent years. OSNs don't offer much assistance in the fight against spam on user walls. Text messages, such as those posted by OSN members on specific public or private sections known as walls, make up a significant portion of the content on social networking sites. Users who follow each other are inundated with their posts because there are no methods for sorting or filtering. A never-ending bombardment of notifications is regularly thrown at users. The security of various communication systems, particularly social networks, is urgently needed. Online social networks (OSN) are currently tasked with the critical task of information screening. Information filtering has been thoroughly examined when it comes to literary materials and web content. Message filtering can in handy for a variety of tasks, one of which is automatically removing spam from a user's wall. According to a recent suggestion, OSN users may soon be able to limit the messages that display on their walls by using a "filtered wall." As a feature of the separating system,users can determine the data they would rather not see on their dividers,and machine learning (ML) is utilized to arrange messages on the sifted divider.Boycott Rule can likewise be utilized to hinder a user from getting to the divider all of a sudden.Greater security provided by the proposed approach will be beneficial to social media websites.

1.1 OVERVIEW

To communicate in today's world, one must use technological media. Online social networks (OSN) and e-mail is commonly used for official communication, but they are rarely used for personal communication. Internet consumers are currently dealing with the most important problem: spam. One definition of spam is "the practise of sending unsolicited electronic messages to other people with the intent of advertising, distributing malware, conducting phishing schemes, or causing irritation." The propagation of spam can be facilitated by the fact that people are more likely to believe and share the information to others. When consumers are bombarded with spam, it not only wastes their time but can also cost them money. Many methodologies exist for managing spam ,which is troublesome issue for web clients to adapt to.

Cyworld, Bebo, Myspace and Facebook have attracted millions of users, and many of them use them on a regular basis. Many social networking sites (SNSs) exist today, each with a unique set of features and capabilities that cater to a wide range of interests and behaviours. Despite their technological similarities, social networking sites (SNSs) have a diverse spectrum of cultures. These destinations assist users with keeping up with their current interpersonal organizations, while others assist outsiders with associating with another in light of shared interests, political perspectives or different exercises and interests. There are sites that appeal to a wide range of people, while others focus on a narrower group of people who share linguistic or cultural qualities, such as ethnicity, sexual orientation, religion, or nationality. These new information and communication elements are available on a number of websites, such as blogging, photo/video sharing, and mobile phone connectivity.

Researchers from a variety of fields have studied social networking sites (SNSs) in an endeavor to better understand their behaviours, repercussions, culture, and significance. Social networking sites are examined in a wide-ranging array of methods, theoretical traditions, and analytical approaches in this special issue of the Journal of Computer-Mediated Communication. The objective of this issue is to put together these papers in order to highlight some of the multidisciplinary study on these sites.

This introduction's goal is to set the articles in this anthology philosophical, historical, and scholarly context. One perspective on the history of social networking sites (SNSs) is presented, relying from personal interviews as well as public reports about the evolution of SNSs. In the next section, we analyse a recent scholarship on SNSs in an effort to contextualise and highlight important studies. As a final note, we'll go over the papers that made up this particular section and make a few suggestions for future study.

Social Network Sites: A Definition

Websites that enables people to create public or semipublic profiles within a circumscribed system, list other users with whom they have connections, and browse and navigate their own and others' lists of connections are what we mean when we say "social networking sites." Depending on the location, these links may have a different character and terminology.

In public discourse, the terms "social networking sites" and "social media" are sometimes used interchangeably to describe this problem. Both emphasis and scope are two reasons to steer clear of the term "networking" when describing this process. It's all about building relationships with individuals you don't know when it comes to "networking." Although networking is permitted on many sites, it is neither the predominant practise or what sets them apart from other types of computer-mediated communication (CMC).

2. LITERATURE REVIEW

2.1 Content and Identity Based Filtering

Spam filtering strategies have split into two main groups by some studies in the spam detection field, namely content and identity based filtering. In the spam category, e-mails are analysed and rated based on the typical spam keywords and patterns. Filtering on the basis of content is extremely vulnerable to attack. Poison attacks are less likely to detect spam because spam e-mails contain many legitimate words. An email address can be whitelisted or blacklisted using identity-based filtering. It is more inclined to pantomise assaults since it depends on the shippers' email IDs, making it more defenseless against those endeavoring to take common users characters.Spam channels should have the option to endure both of these kinds of assaults to work.

Social network data were also incorporated into the e-mail system for improving the efficiency of spam filtering. Spam may be filtered using many variables such as trust, interest, and closeness amongst social network users, according to some research studies. It's not enough to look at social network profiles to identify and classify spam e-mails. No variables explicitly from the email wew processed to group the messages. Lizhou et al. (2016) proposed an active learning based spam message classification to reduce the classification time without reducing the accuracy. Classification of e-mails with images is not considered in their work.

Yuanchun et al. (2011) proposed a content-based e-mail spam message classification through local concentration based method. Content and identity-based filtering are discussed in Lourdes et al. (2010). A content based fusion algorithm for the spam e-mails identification is proposed by Congfu et al. (2014). Different classifiers are used and based on the voting strategies their output is considered for classification of e-mails. A fuzzy based method was proposed by Salehi et al. (2017) for e-mail spam classification. To lessen the noise point problem, the structural patterns of spam messages are examined, and a fuzzy-based technique is used. The Optimization of parameters and feature selection approach is proposed for spam message identification in e-mails by Sang et al. (2011). The identification of spam messages by examining the departing messages was discussed by Zhenhai et al. (2012).

Gopi et al. (2018) talked about the component choice for a spam message separating in messages is based on the term frequency and category ratio to select the features of the number of samples in each class. Fida et al. (2016) described how to increase the accuracy of spam detectors in e-mails using an economic metric method. A helping strategy is talked about by Amany et al. (2018) for the discovery of email spam.

No false positives occur if the innocent email's content matches that of unrelated spam. The nodes must forward all communications exchanged in the system without revealing their identities in order to protect the users' privacy. When the information is to be forwarded across the people in a community, all the details concerning the earlier visited nodes must have to be removed before it is being sent to the next node. System communications are kept in the peer to peer level. The Reduction in bandwidth cost in parallel with the increment in spam detection rate is introduced in their approach. The distinguishing proof of destructive connections in messages was portrayed by Yehonatan et al. (2018).

Another spam recognition model was proposed by Ismaila andassociated in 2015 with better multitude streamlining. Negative Selection Algorithm detector creation benefits from stochastic data modelling in Particle Swarm Optimization (PSO) (NSA). Particle swarm enhancement and negative selection were coupled. The performance and accuracy to detect the e-mail spam effectively when compared to the NSA and PSO model individually.

2.2 INFERENCES FROM LITERATURE

Haiying et al. (2014) advocated using social network data to screen spam emails. Additionally, it utilized a content based and identity based spam filtering method. Spam e-mails are analysed and graded using spam-specific keywords and patterns. A content-based category is what it's called. Ordinary users' identities can be impersonated in content-based assaults by fabricating their IDs or exploiting their machines. A whitelist and a blacklist of email addresses are kept up with users in identity based filtering systems. These systems are particularly vulnerable to a poisoning assault because they rely only on the senders' email addresses. It is more difficult to identify spam emails that contain a big number of valid words. However, only certain social networks factors such as closeness, interest, trust were computed from the social networking sites were used in an e-mail systems to find ham e-mails and spam ones. Bayesian spam filters were used for better accuracy, protection against attacks and finding spam efficiently. Further, trust, interest factors were not computed from email networks.

Machine learning (ML) techniques were introduced by Chao et al. (2013) to identify Twitter spammers. The empirical investigation was carried out using a big dataset of millions of tweets. Twitter spammers were identified using a neighborhood-based detection feature. Both profile-based feature evasion and evasion tactics were used to identify Twitter spammers. It was possible to identify spam accounts on Twitter by looking at their follower counts, tweet volume, and other metrics. Investigations into the spammers' methods of evasion, including the 24 detection features they employ, have been conducted. A drawback to this approach is that only

accounts that did not post malicious URLs were included in the dataset crawled from Twitter and classified as benign.

3. EFFECTIVE FILTERING OF UNSOLICITED MESSAGES FROM ONLINE SOCIAL NETWORKS (OSN)

3.1 INTRODUCTİON

In today's world, OSN has become a need. Anyone of any age can have a good time on social media sites. The existence of spam is one of the drawbacks of OSNs, in addition to their many advantages. Unsolicited messages sent by e-mail, microblogging sites, instant messengers, and other forms of electronic communication are referred to as spam. It's inconvenient and time-consuming for users, too. At the moment, it's difficult to tell if an email is spam just by looking at it. Despite the fact that machine learning (ML) techniques are utilized to help detect spam, the unit of measurement for each type of spam is different and has varying consequences on internet users.

The SF and BF have gained popularity due to their benefits over other approaches. In comparison to other classification models, the BF, a basic classifierin view of likelihood values, unites all more quickly. Furthermore, it simply requires a little amount of preparing information and is very simple to carry out. The purpose of the SF is to increase the distance between the student and either of the two classes. If a disruption occurs in the SF,a component vector situated close to the isolating plane will experience the least. In other words, increasing the distance from the margin means that even if there is a disturbance, the feature vector will not be altered. The SF is a suitable choice for high-dimensional data because of its high classification rate and large range of kernel functions.Every one is customized to a specific kind of information. Kernel functions are used to split data that cannot be split linearly. Soft margins are used to prevent overfitting. Soft margins are given slack values, and error rates are calculated using the slack values. Error rates can be diminished by utilizing delicate edges and satisfactory leeway values. Although the two classifiers listed above do a good job of identifying text, they fall short when it comes to classifying messages from OSN.

3.2 IDENTIFICATION AND FILTERING OF ONLINE SOCIAL NETWORK (OSN) SPAM

Spammers utilize a variety of techniques to spread their messages, including text URL spam, review spam, text spam and spam in comments. through the internet.Thus unique spam recognition strategies were proposed by many specialists. The mapping of URLs to destination URLs, outlined in De Wang et al., can be used to detect URL spam (2015). The examination of URLs was completed after the invalid or inactive URLs were removed. URLs were grouped based on the values of a number of trends that include the statuses having unique URLs.The Markov chain model was employed which is then converted to a classifier to detect URL spam. When comparing the two, spam URLs tend to be more valuable. It is possible to identify and eliminate spam URLs using these data. Spam URLs can be distributed via tweeted or instant message. URL spam can be shifted through by matching indicated URL spam designs. A classifier is first trained on a collection of features taken from tweets. When a given period of time has passed, the tweets that have been collected are also forwarded to the classification model. Chao et al. examine the effectiveness of various machine learning(ML) methods for identifying spam tweets (2015).

The spammers can spread spam by posting or commenting on irrelevant texts in social networks. Mansour et al. (2015) discussed different machine learning approaches to fighting against spam comments. This feature was used to detect spam by extracting some of the features such as post-comment similarity and inter-comment similarity, the comment length, phone information, e-mail information as well as amount of words within the comment and the gap between the post and the comment. The spammers find different techniques to spread spam and exploit OSN to spread spam. Customers' reviews are essential for product sale with the proliferation of online shopping, but there is no control in writing the reviews. These review spam might affect the sales of a particular product. Siddu et al. (2015) discussed a review of spam detection techniques. Sentiment analysis was done to find review spam by finding the rating computed based on the content of the review. The values were assigned to the reviews based on the content of the reviews if the value higher than a threshold value, then it was stated as spam.

3.3. SPAM DETECTION TECHNIQUES

The data mining methods plays a vital role in spam detection. A review of different data mining techniques for social media was presented in Mohammad Noor et al. (2016). Quality assessment rules were employed to perform a quality valuation of data. A quality score was maintained as a cutoff value and if the quality score is higher than a particular value, that data is trustable. The data extraction strategy was employed to find answers for some questions. Also, the reciprocal translation method was employed. The anomalies were also detected using data mining techniques.

For anomaly detection, a variety of strategies were utilized:conduct based procedures,underlying strategies utilizing diagrams,and ghostly baed techniques (2016).The inside happy of communicating and getting messages was dissected to find surprising action utilizing the way of behaving based methods's substance based sifting. There wew particular chart measurements for various hubs in structure based procedures,which implied that the hubs had differed values when contrasted and the abnormal clients.

In spectral-based technique, a segment was performed by disposing of connections between the hubs;a work on a calculation alluded to as SPCTRA was utilized.Subgraphs with thick subgraphs were worked for assaiants and strange clients .Tingmin et al. complete the word-to-vector ID of spam messsages in twitter (2017b).

The conventional approaches are used to detect spam in OSNs. The Current emergence in the spam detection techniques in the social network was surveyed in Manajit et al. (2016). Co-classification framework, least-square SVM (both non-linear classifiers and linear classifier), and social tagging systems are some of the examples. Time-sensitive features such as the similarity of a review on a product, the similarity of a product review, the reviewer's review frequency and the product's repeatability measure are used to determine whether a review is spam.

Ruxi et al. discussed how classifiers were created to identify comment spam on social networks (2015). Sample selection, extraction of words from a sample and generation of the results are the four stages of classifier building. A web search tool ,an internet search engine, or "web crawler," is utilized to assemble data about a web page's content and afterward remove words that are superfluous. Finally, the classifier was built and tested.

The word segmentation and manual annotation of comments were done to get accuracy for the calculation of comments according to manual tags. The content based filtering performed in a semi supervised way was discussed by Surendra et al. (2018).

3.4. PROBLEM STATEMENT AND SOLUTION APPROACH

Electronic communication is a need in today's environment. For personal communication, OSNs (online social networks) are preferred, whereas email is used for official communication. Spam is the most pressing issue that internet users face nowadays. Unsolicited or unrequested electronic messages that are used for promoting, distributing malicious malware or phishing or simply aggravating the recipients are known as spam messages. As a result, spam communications have the potential to proliferate rapidly, thanks to the human instinct to trust and repost content that has already been circulated. Spam can cause financial harm as well as time waste for its recipients. Internet users have to deal with spam on a daily basis, but there are a number of techniques to counteract it.

4. PROPOSED WORK

The figure 4.1 shows modified filtered wall architecture used in the current system.

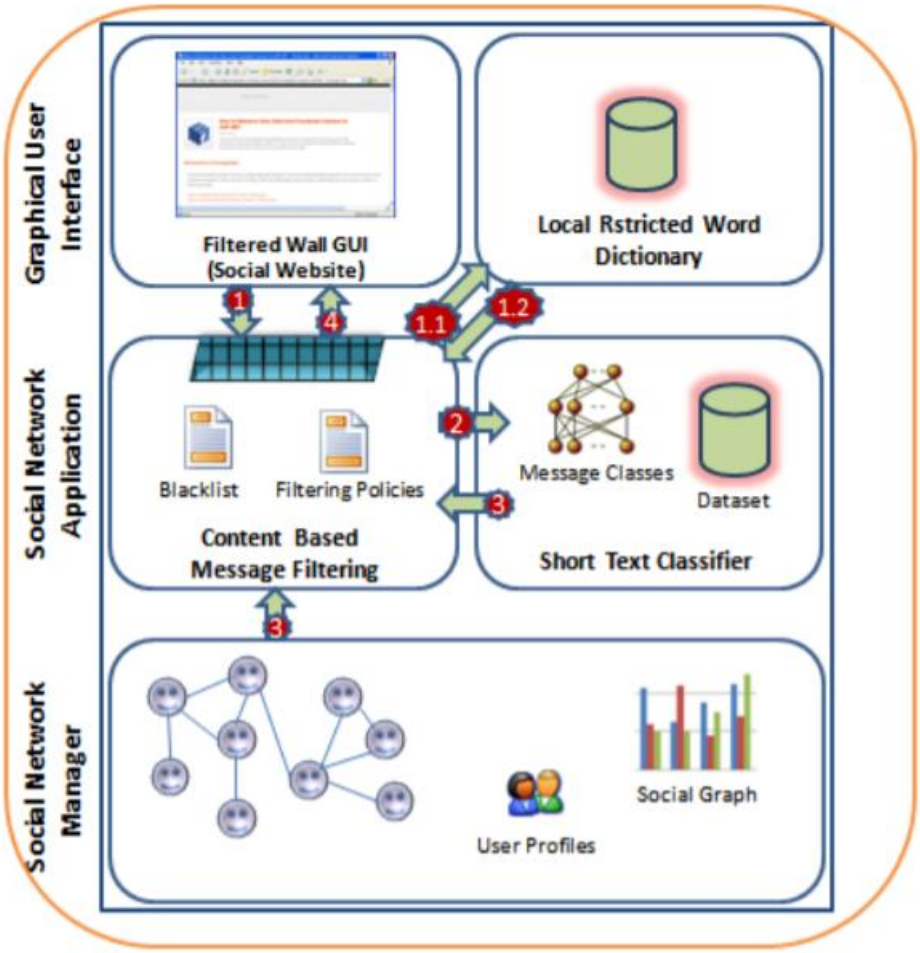


Fig 4.1 Filtered Wall Architecture.A. Social Network Manager (SNM)

The initial level of Social Network Manager provides the essential OSN features (i.e., relationship and profile). It also keeps track of information about the people with whom you've interacted. Filtering rules and black lists will be applied to all user data sent to the second layer (BL).

B. Social Network Application (SNA)

Content Based Message Filtering (CMBF) and Short Text Classifier (STC) is composed in the second layer. This level plays main role in message categorization. Also Black list (BL) is maintained for bad words and the user who frequently sends bad words.

C. Graphical User Interface (GUI)

The Third layer is a Graphical User Interface (GUI) application for the user who wants to post his messages as an input. Another main function of this layer is to filter unwanted messages using Filtering Rules (FR) and user who posts the unwanted messages will be kept in Black List (BL) until user removes the blacklisted user. The GUI likewise comprises of a filtered wall (FW) where the user can post and see his desirable messages. [1].

Fig. 6.1 points can be summarized as follows:

1. The FW captures a message that the user and his/her friends try to post.

2. A Machine Learning (ML) based text classification technique tracks metadata from the content of the posted message.

3. This metadata is combined with data from the social graph, LRWD, and user profiles in order to execute the filtering Rules and Black List at the FW level of the application.

4. FW [1] will display or suppress the message based on the outcomes of steps 1 through 3.

4.1 Methodology

When posting to a user's wall, posts on their Blacklist will not be seen by other users. BL rule is utilised in this work, which is a continuation of the prior paper, which includes all categorization and filtering rules as well. Users can be blocked by wall owners based on their relationships and the walls they possess. It is possible that this ban will be in place for an indeterminate amount of time. In the next paragraphs, we'll go over the methods employed in the preceding paper:

A .The Short text classifiers

B. Filteration

C. User Black Listing

A. Short Text Classification:

It is possible and simple to classify texts using a vast amount of data. However, when there is a shortage of documents, this poses an issue. Short text classification is utilised because of this issue. We want to identify and differentiate legitimate posts from spam in a step-by-step process rather than a single one. Step I: Normal and undesired types of mail are separated in the first level of classification. As a sort of unwelcome post categorization, the second level chooses which class a given post falls within. This class data will be used in the filtering process. Machine learning (ML) is used to classify short text.

B. Filtration

A message can have a variety of meanings and significance depending on who is writing it, just like in real life. As a result, FRs should allow message creators to specify limitations. Creators on which a FR applies can be baes on a few unique measures: one of the most applicable is by forcing conditions on their profile's credits. In this way, for example, it is feasible to set regulations that only apply to young creators or those with a certain political/religious viewpoint. In a world of social networks, it's possible to learn more about the authors themselves by looking at their social graph. In order to implement provided rules, it is necessary to specify the types, depths, and levels of trust associated with the relationships in which the creators are involved. This diagram depicts the filtering process.

C. User Blacklisting Process

The system also has a Blacklist (BL) mechanism to keep out messages from people you don't want to hear from. Black List (BL) is directly managed by the system, which should be able to determine who are the users to be inserted in the BL and for how much time and decide when user's should be removed from Black List (BL) is finished. A collection of rules, known as BL rules, are used to provide the system with the knowledge it needs to be flexible. To put it another way, these rules aren't specified by the Social Network Management, hence they aren't designed to be applied to the entire community. It was decided that the wall owners, rather than the proposed system, would be in charge of determining who was and wasn't allowed on their walls. This means that a user can be blocked from a wall but still be able to post to it.

In the proposed system, a user can register himself as a New User and creates a profile. The user can login in order to start begin his work on OSN. The user can create and manage their own groups. The additional features are like user can find his friends based on preferences set in profile. User can send request to his friend or accepts a request send by other. User can Post or receive messages.

Steps in Preparing Local Restricted Word Dictionary (LRWD):

1. OSN user decides restricted words (RW) by categories.

2. Search synonyms of restricted words (RW) and store them to LRWD.

3. Search opposite of restricted words (RW) and store them to LRWD.

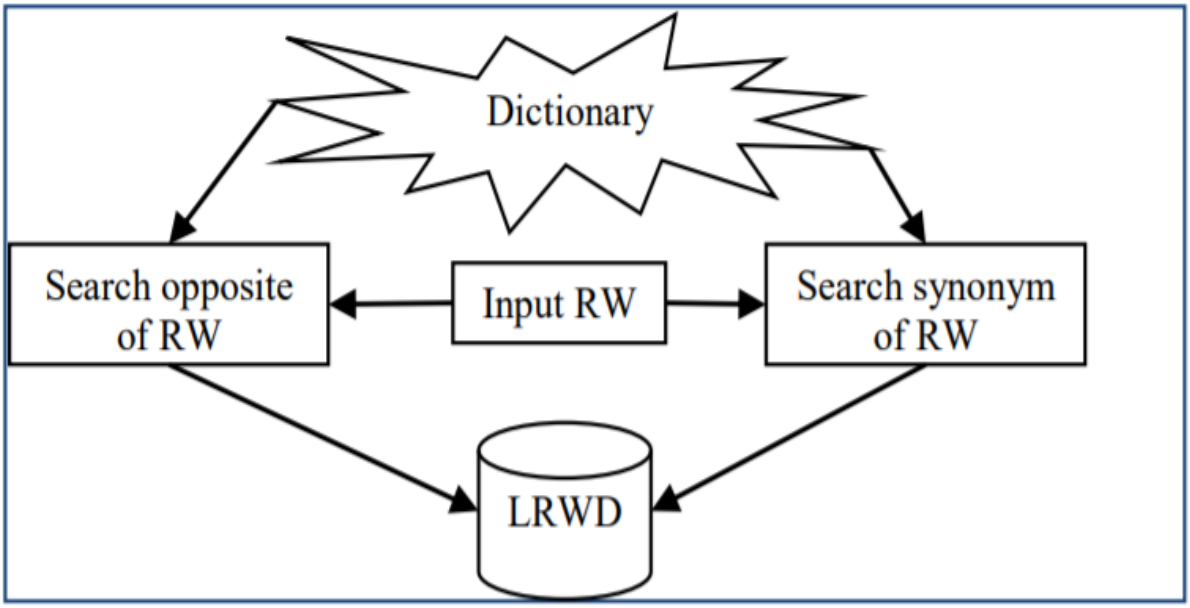
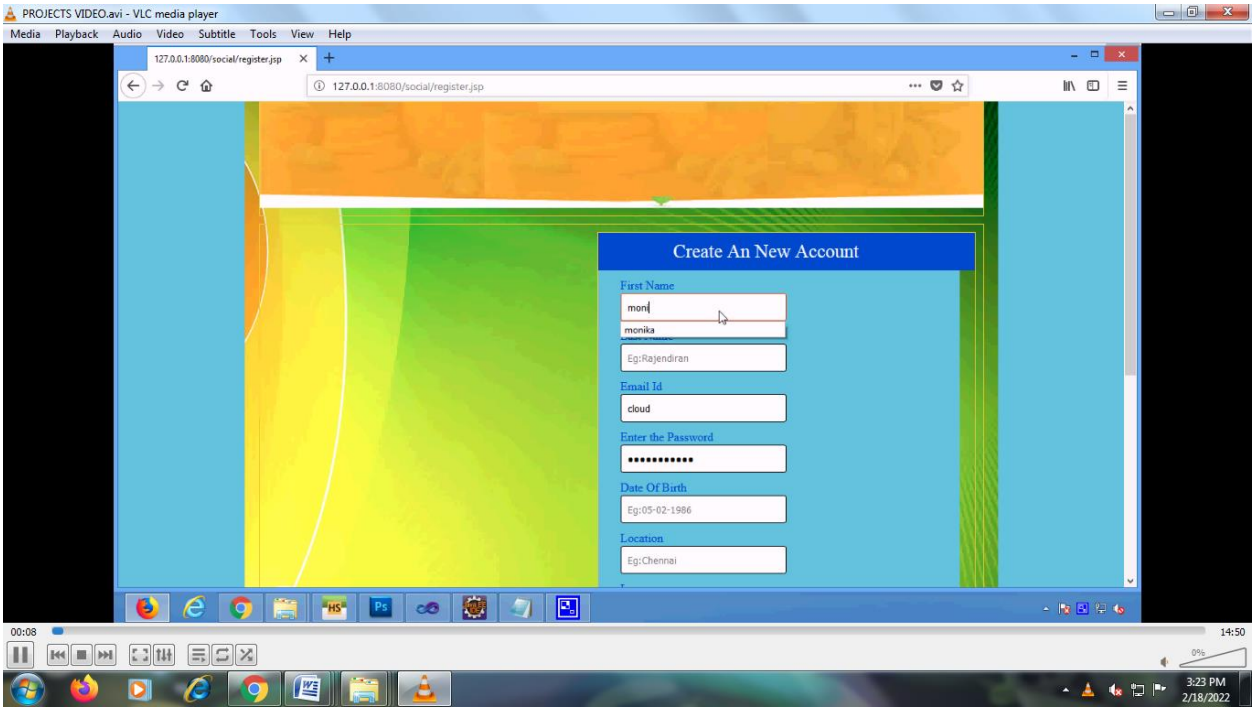
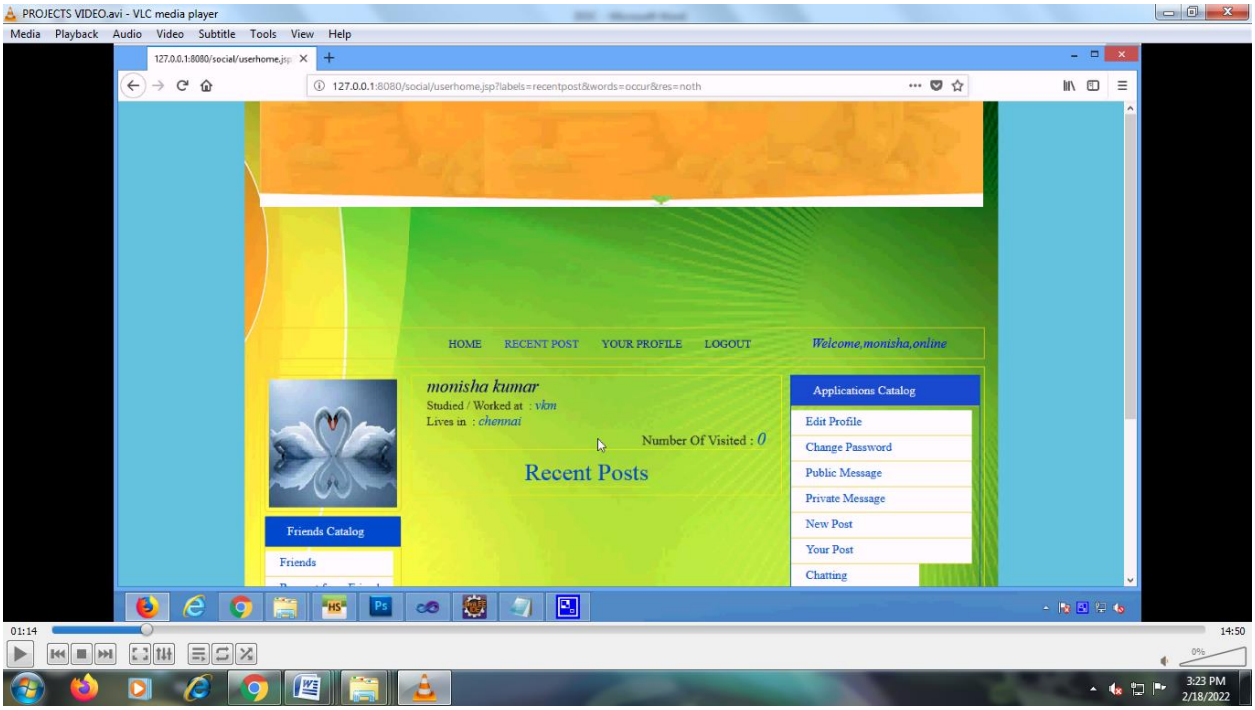
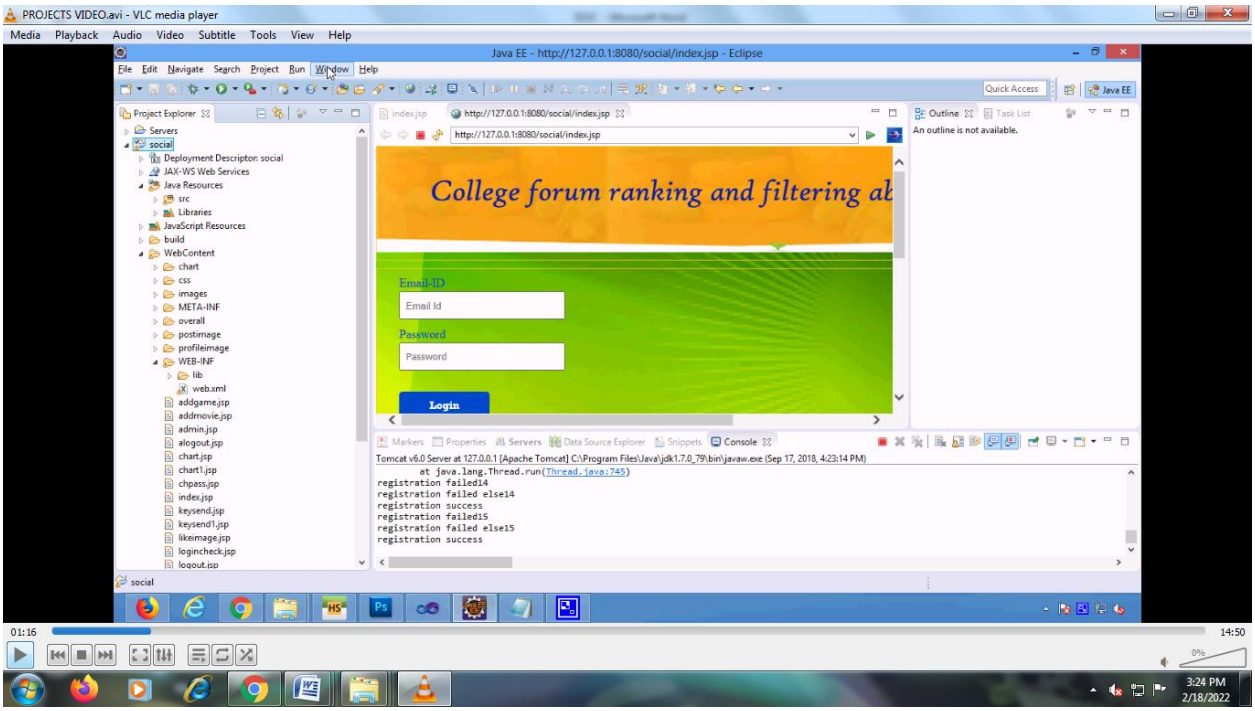


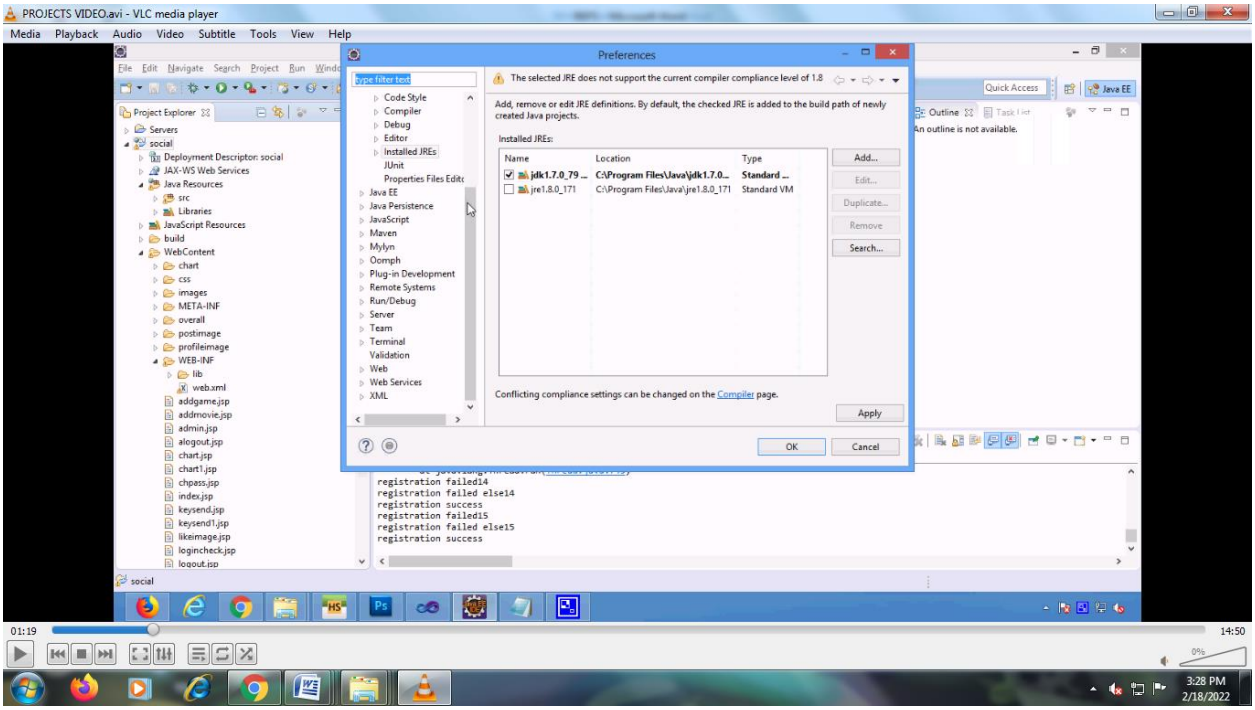
Fig. 4.2: Generating LRWD

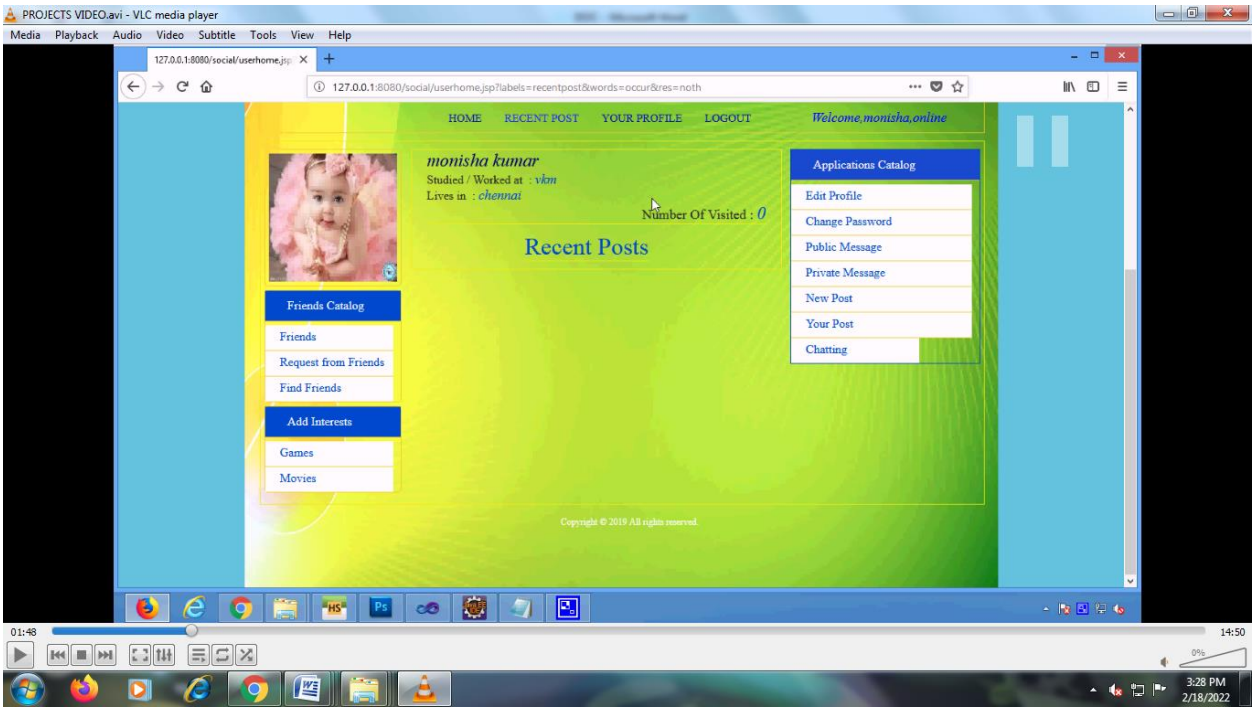
5. RESULTS AND DISCUSSION

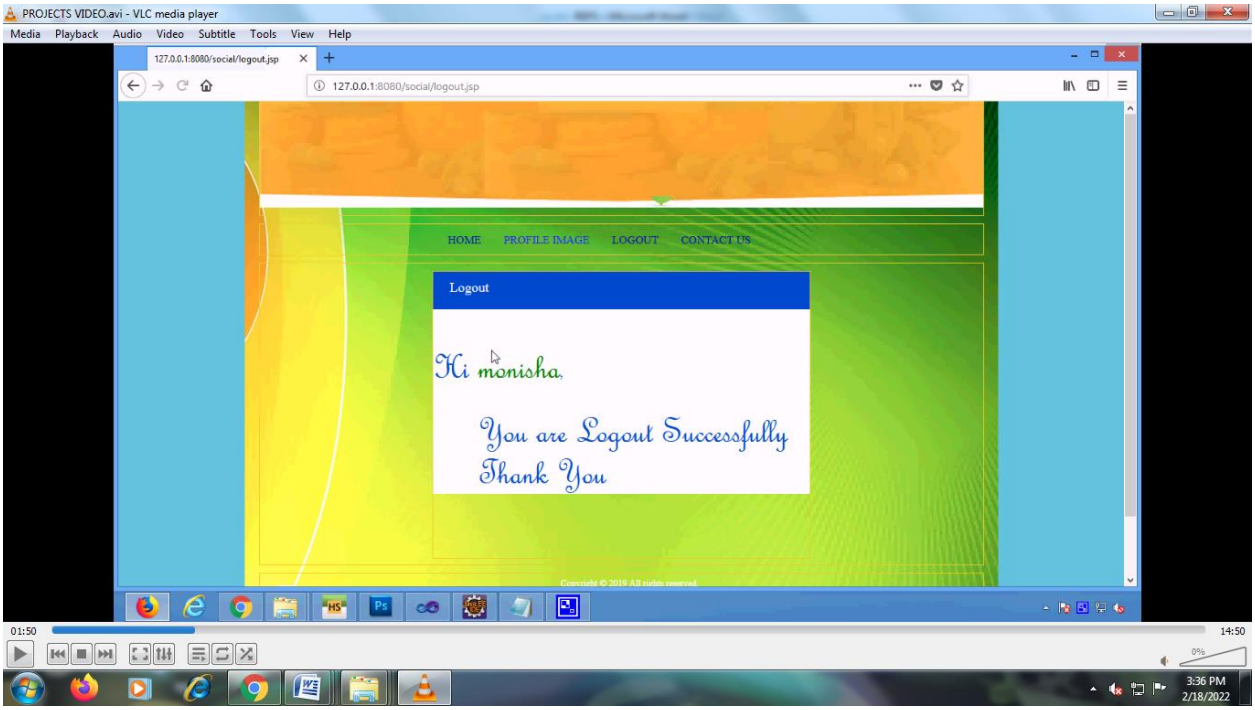



PROJECTS VIDEO.avi - VLC media player
Media Playback Audio Video Subtitle Tools View Help
127.0.0.1:8080/social/userhome.jsp?labels=recentpost&words=occur&res=noth
HOME RECENT POST YOUR PROFILE LOGOUT Welcome,monisha,online
monisha kumar
Studied / Worked at : vkm
Lives in : chennai
Number Of Visited : 0
Recent Posts
Applications Catalog
Edit Profile
Change Password
Public Message
Private Message
New Post
Your Post
Chatting
Friends Catalog
Friends
01:14
14:50
3:23 PM
2/18/2022


PROJECTS VIDEO.avi - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Java EE - http://127.0.0.1:8080/social/index.jsp - Eclipse
File Edit Navigate Search Project Run Window Help
College forum ranking and filtering al
Email-ID
Email Id
Password
Password
Login
Tomcat v6.0 Server at 127.0.0.1 [Apache Tomcat] C:\Program Files\Java\jdk1.7.0_79\bin\javaw.exe (Sep 17, 2018, 4:23:14 PM)
registration failed14
registration failed else14
registration success
registration failed15
registration failed else15
registration success
01:16
14:50
3:24 PM
2/18/2022


PROJECTS VIDEO.avi - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Preferences
Type filter text
Code Style
Compiler
Debug
Editor
Installed JREs
JUnit
Java EE
Java Persistence
JavaScript
Maven
Mylyn
Oomph
Plug-in Development
Remote Systems
Run/Debug
Server
Team
Terminal
Validation
Web
Web Services
XML
The selected JRE does not support the current compiler compliance level of 1.8
Add, remove or edit JRE definitions. By default, the checked JRE is added to the build path of newly created Java projects.
Installed JREs:
Name
Location
Type
jdk1.7.0_79 ...
C:\Program Files\Java\jdk1.7.0...
Standard ...
jre1.8.0_171
C:\Program Files\Java\jre1.8.0_171
Standard VM
Add...
Edit...
Duplicate...
Remove
Search...
Conflicting compliance settings can be changed on the Compiler page.
Apply
OK
Cancel
registration failed14
registration failed else14
registration success
registration failed15
registration failed else15
registration success
01:19
14:50
3:28 PM
2/18/2022


PROJECTS VIDEO.avi - VLC media player
Media Playback Audio Video Subtitle Tools View Help
127.0.0.1:8080/social/userhome.jsp?labels=recentpost&words=occur&res=noth
HOME
RECENT POST
YOUR PROFILE
LOGOUT
Welcome,monisha,online
monisha kumar
Studied / Worked at : vkm
Lives in : chennai
Number Of Visited : 0
Recent Posts
Applications Catalog
Edit Profile
Change Password
Public Message
Private Message
New Post
Your Post
Chatting
Friends Catalog
Friends
Request from Friends
Find Friends
Add Interests
Games
Movies
Copyright © 2019 All rights reserved
01:48
14:50
3:28 PM
2/18/2022



CONCLUSION

Even though so many spam message separating strategies are available continuously, the existence of spam messages in E-mails and OSN is a current issue for users. In addition to irritating the users, spam communications can cause a loss of confidence amongst the users and caus monetary losses. It is therefore necessary to devise a mechanism that can successfully recognise and filter spam communications without causing issues for end users or service providers. Unsolicited email and OSN messages are the focus of the proposed approach, which aims to identify and remove them. To increase the efficacy of the filtering mechanism and spam e-mail detection factors from social media and e-mail datasets are taken into consideration. Users' trust, reputation, and personal interests are all taken into account, as are aspects of the social network, like the strength and level of association between them. Logistic regression is utilized to combine the independent factors. In order to effectively classify spam, the OCR approach is used to find text in images present in incoming electronic mail (e-mail).

REFERENCES

1. Aboli, SV & Rupa, AF 2016, 'Automated content based short text classification for filtering undesired posts on facebook', Proceedings of the IEEE World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, pp. 1-5.
2. Adarsh, MJ & Ravikumar, P 2018, 'An effective method of predicting the polarity of airline tweets using sentimental analysis', Proceedings of the IEEE 4th International Conference on Electrical Energy Systems (ICEES), pp. 676-679.
3. Adel, HM & Raed, AZ 2011, 'Application of genetic optimized artificial immune system and neural networks in spam detection', Elsevier Journal of Applied Soft Computing, vol. 11, no. 4, pp. 3827-3845.
4. Ali, AA & El-Sayed, ME 2015, 'Dendritic cell algorithm for mobile phone spam filtering', Elsevier Journal of Procedia Computer Science, vol. 52, pp. 244-251.
5. Aliaksandr, B & Petr, H 2018, 'Spam filtering using integrated distribution- based balancing approach and regularized deep neural networks', Springer Journal of Applied Intelligence, vol. 48, no. 10, pp. 3538-3556.

6. Amany, AN, Neveen, IG & Afaf, AS 2018, 'Antlion optimization and boosting classifier for spam email detection', Elsevier Journal of Future Computing and Informatics, vol.3, no. 2, pp. 436-442.
7. Ashraf, A, Zanaty, EA & Ghoniemy, S 2013, 'Improving the Classification Accuracy using SVM (SVMs) with New Kernel', Journal of Global Research in Computer Science, vol. 4, pp. 1-7.
8. Bing, X, Mengjie, Z, Will, NB & Xin, Y 2016, 'A survey on evolutionary computation approaches to feature selection', IEEE Transactions on Evolutionary Computation, vol. 20, no. 4, pp. 606-626.
9. Brian, W & Tong, L 2009, 'Channel e-mail: a sociotechnical response to spam', IEEE Transactions on Computer, vol. 42, no. 7, pp. 63-72.
10. Chao, C, Jun, Z, Yi, X, Yang, X, Wanlei, Z, Mohammad, MH, Abdulhameed A & Majed, A 2015, 'A performance evaluation of machine learning based streaming spam tweets detection', IEEE Transactions on Computational Social Systems, vol. 2, no. 3, pp. 65-76. paper thesis