Rumor Spreading and Source Identification In Social Network Using TOI

B.Yamini[1],V.Krithika[2],V.Manisha[3]
[1]Assistant Professor, Dept of CSE
[2, 3]Dept of CSE
[1, 2, 3] S.R.R Engineering College.

Abstract- *The main aim of this project is to identify the real rumor person and eliminate fake post and rumor person in the social Network. The rumor sources in the network plays a major role in the social network like facebook, whatsapp, twitter. Here the static networks are changed to dynamic networks. Here instead of suspecting every user in the network the paper focusses on reverse dissemination strategy to find the rumor source. With the development of social network, the various issues regarding the spreading of fake messages is also developed. Both positive and negative information are spreading in a rapid manner in the social network. In this paper, the spreading of online fake rumors is focused. Various types of rumors can be spread over the network, this increases to various issues, hence the user spreading rumor is entirely blocked and further those rumor messages is deleted from the network. This is to avoid further spreading of fake messages in the network.*

Here the goal is to minimize the influence of the rumor (i.e., the number of users that have accepted and sent the rumor) by blocking the user spreading rumor in the network

Keywords- Social network, rumor blocking, static network, reverse dissemination

I. INTRODUCTION

Social media has been increasing steadily ever since its origin. The data present in the social media is very important. Data is the most precious factor in every social media like facebook, twitter, whatsapp and many more social applications[14]. Hence it is necessary to protect and preserve each user's data in the social network. The another most important is to avoid spreading rumors in social network[16]. This can be achieved through network security. Rumors spreading in social networks have long been a critical threat to our society. A recent incident of rumors "Obama was injured in two explosions of White House" led to 10 billion USD losses in a few hours[8]. This demonstrates that a single rumor can cause great damage to business and life. Nowadays, with the development of mobile devices and wireless techniques, the temporal nature of social networks (time-varying social networks) has a deep influence on dynamical information spreading processes occurring on top of them[15].The ubiquity and easy access of social networks not only promote the efficiency of information sharing but also dramatically accelerate the speed of rumor spreading. For either forensic or defensive purposes, it has always been a significant work to identify the source of rumors in time-varying social networks[12].Here reverse dissemination strategy is used to suspect the real rumor spreading source. The experiment results show significant advantages for this method in the identification and spreading of rumor sources based on the threshold value the suspect is blocked from the network and the fake post are deleted from the network. In this paper the flash news from TOI API is considered and only the current news updates is considered for identifying the rumor source. The flash news is not categorized into any fields. The flash news will be updated continuously so the posted rumor by one user cannot be compared by the another user after some time since the flash news will be updated.

II. STATE OF ART

Biao Wang et.al[3] In this paper, it is necessary to detect the rumor source and delete related messages, which may be enough to prevent the rumor from further spreading. In terrorist attack and various social attack this can be used for avoiding the critical issues. It is necessary to block the real suspect from the social network and save the victims without spreading further. It is difficult to identify and block the real source from the dynamic network.

D.Kempe et.al[6] In this paper identification of malicious information sources in a network, be it in the case of an online spam spreading in the Internet or a misinformation or rumor propagating in an online social network, allows timely quarantine of the epidemic-like spreading to limit the damage caused. This can lead to a fundamental understanding of the role of network in aiding or constraining epidemic-like spreading. Here the issue of reliably detecting a single rumor source with multiple observations from a statistical point of view of a spreading.

Our goal is to find the rumor source in order to control and prevent network risks based on limited information about the network structure and multiple snapshot observations.

Jiaojiao Jiang et.al[9]In this paper,rumor spreading in social networks have long been a critical threat to our society. Rumors combine the characteristics of spreading scheme with the dynamic connections between individuals in time-varying social networks. For either forensic or defensive purposes, it has always been a significant work to identify the source of rumors in time-varying social networks. However, this techniques generally require firm connections between individuals (i.e., static networks) so that administrators can trace back along the determined connections to reach the spreading sources. It is tedious to identify the real victim in the time varying social network.

Karim El Defrawy et.al[10]In this paper identifying the servers in the network that are first infected also allows us to detect the latent points of weaknesses in the computer network so that preventive measures can be taken to enhance the protection at these points. The source identification problem also arises in the study of rumor spreading in a social network. A rumor started by a few individuals can spread quickly through the underlying social network. In many cases, it is difficult to find the sources of the rumor.

III. EXISTING SYSTEM

The ubiquity and easy access of social networks not only promote the efficiency of information sharing but also dramatically accelerate the speed of rumor spreading[6]. Existing method will not eliminate fake messages. Rumors combine the characteristics of the "word-of-mouth" spreading scheme with the dynamic connections between individuals in time-varying social networks. The existing works efficiently in static network. The existing system allows the user to share and post message and the user can identify the fake message but they could not eliminate the fake messages[3]. It is entirely based on the intimation of other users about the fake message .It doesn't compare with any news article to identify the fake message. The elimination of fake messages and identification of fake messages and posts will be under the control of admin of the social application.

3.1 LIMITATIONS

The existing system contains only the identification of fake messages. The user can share and post any number of fake messages without any control of admin. Here the elimination of fake messages and blocking the rumor spreading user are the problems in existing system[11].The individual who has the maximum centrality value is considered as the rumor source. All of these centrality measures are based on static networks[13]. Time-varying social networks, where users and interactions evolve over time, have led to great challenges to the traditional rumor source identification techniques.

IV. PROPOSED SYSTEM

The proposed system going to restrict the rumor message from friend list if we find any rumor messages post in social network and this kind of post will not be forwarded anymore. There is a rumor option in the social network. If user find friends post contains any rumor messages they can intimate to the authority person, the authority will verify whether the messages is rumor message or not by using news articles. After verification if the message is rumor then the user account will be monitored and maintained threshold for their account. If the threshold reaches then the admin provides warning to them but if they post rumor messages again then their account is blocked by the admin[10].Then the rumor post will be deleted from all the user account so that the posts will not be shared by any person. Thus the rumor post is identified and eliminated from everyone's timeline.

ARCHITECTURE DIAGRAM:

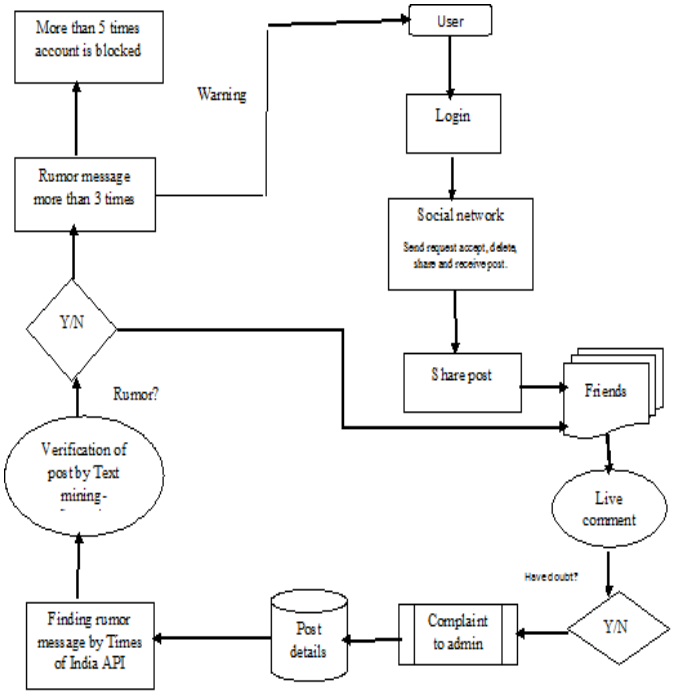

Fig1. Architecture diagram for rumor spreading and source identification in social network using TOI.

V. MODULES

Here we use the modules such as creating the application followed by the module where the user can share post and receive messages. The next module is finding the rumor message using reverse dissemination process and verifying the post using text mining. The next module is admin process where the admin blocks the suspect user spreading rumor.

5.1 APPLICATION CREATION

The first module is creation of social network like facebook. Here any number of user can create their profiles. The user can sign in and register with their basic details like first name, last name, email id to link their account and set profile picture for their account. The user can send friend request and accept friend request. The user can also delete the friend request. These details are maintained in a database for each user.

Algorithm:

Input: Send friend request to 1 or n nodes $n=\{n_1,n_2,\ldots,n_n\}$, no of users $t=\{t_1,t_2,...,t_n\}$.

Method:

Create a new account and send request to other users. The user can either accept or reject the request.

Output: Accept or reject the friend request from 1 or n nodes $n=\{n_1,n_2,\ldots,n_n\}$, no of users $t=\{t_1,t_2,...,t_n\}$.

Initialize: A set of suspects U = ∅
for(t starts from 1 to n)**do**
for(u: sends the request to t_i)**do**
if(t accepts the request) **then** added in the friend list and t_i can view and comment on the post.
end
else(t rejects the request) **then** t_i cannot view or comment on the post.
end
end for
end for
stop

5.2 SHARING POST AND RECEIVE MESSAGES

In this module, the user can share the post to their friends and also receive post from their friends.When the user receive post from their friend in the timeline then the user can share and comment on their friend's post and the information regarding the post such as date and time, detail of the particular user will be stored in the database[4].Live news article will be displayed in each user's timeline to verify whether it is a fake message or not.

Algorithm:

Input: Posting the news by 1 or n nodes $n=\{n_1,n_2,\ldots,n_n\}$, no of users $t=\{t_1,t_2,...,t_n\}$.

Method:

The user post the news. When the user receive the post, the user can share and comment on the post.

Output: Sharing, receiving and commenting on the post by no of users $t=\{t_1,t_2,...,t_n\}$.

Initialize: A set of suspects U = ∅
for(t starts from 1 to n)**do**
for(u: post the news to t_i)**do**
if(t receives the post) **then** t_i can share and comment on the post.
end
else(t din't receive the post) **then** t_i cannot share or comment on the post.
end
end for
end for
stop

5.3 RUMOR MESSAGE FINDING PROCESS

This module contains reverse dissemination process in which it contains all the various rumor spreading path. The node from which the path is suspected to have the maximum threshold value is identified to be the suspect to spread rumors. This method is inspired from Jordan Method[7].If any user find out the shared post contains fake message there is option available called rumor, then it will be updated to the admin if it reaches the threshold value.

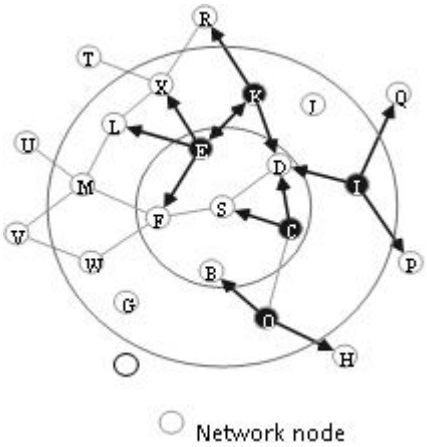

Fig2A. Network connected with n no. of users.

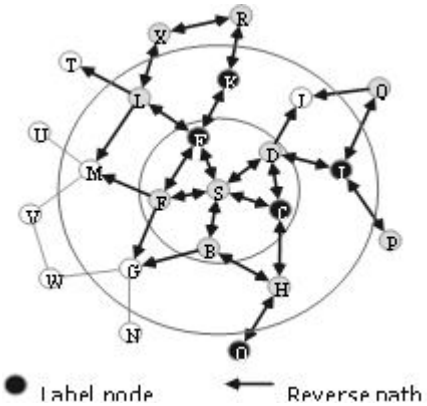

Fig2B. The reverse path to identify the rumor source.

5.3.1 Reverse dissemination Method

The reverse dissemination process is used to identify the suspect from a list of nodes in the network. This process gives the accurate result by identifying the suspect node in the network. From this the suspect can be warned and blocked by the admin of the network.

5.3.1.1 Rationale

The rationale of the reverse dissemination method is to send copies of rumors along the reversed dynamic connections from observed nodes to exhaust all possible spreading paths leading to the observation[1]. The node from which all the paths, covering all the observed nodes' states, originated is more likely to be a suspect. The reverse dissemination method is inspired from the Jordan method. The reverse dissemination method is different from the Jordan method, because this is based on time-varying social networks (involving the physical mobility and online/offline status of users) rather than static networks. All wavefront nodes O_I = {*E,C,I,K,O*} observed in time window $t + 1$ are labeled as black in Fig. 2A. The whole process is composed of two rounds of reverse dissemination[1]. In round 1 (Fig.2A), all observed nodes broadcast labeled copies reversely to their neighbors in time window *t*. For example, nodes *S* and *O* received copies of node *C* (*S,O*← *C*), and node *D* received copies of three observed nodes *C,I* and *K* (*D* ← *C,I,K*). In round 2 (Fig. 2B), the neighbors who have received labeled copies will relay them to other neighbors in time window $t - 1$. In each round, the labels will be recorded in each relay node. We can see from Fig. 2B that node *S* has received all copies from all the observed nodes (*S* ← *C,E,K,I,O*). Then, node *S* is chosen to be a suspect.[1]. Here the starting time for each observed node starting their reverse dissemination processes varies in different types of observations. For a wavefront, since all the observed nodes are supposed to be contagious in the latest time window, all the observed nodes need to simultaneously start their reverse dissemination processes. For a snapshot, the observed nodes stay in their states in the latest time window[1]. Therefore, the reverse dissemination processes will also simultaneously starts from all the observed nodes. However, for a sensor observation, because the infected sensors record their infection time, the starting time of reverse dissemination for each sensor will be determined by t_i. More specifically, the latest infected sensors first start their reverse dissemination processes, and then the sensors infected in the previous time window, until the very first infected sensors.

Algorithm : Reverse dissemination

Input: A set of observed nodes O = $\{o_1,o_2,...,o_n\}$, a set of infection times of the observed nodes $\{t_1,t_2,...,t_n\}$, a threshold α, and a threshold t_{max}.

Initialize: A set of suspects U = ∅, and $t_1 = ... = t_n = T$ if O is a snapshot/wavefront, otherwise $T = \max\{t_1,t_2,...,t_n\}$.

for*(*t starts from 1 to a given maximum value t_{max}) **do for** (o_i: i starts from 1 to n) **do**
if(o_i has not started to disseminate the rumor) **then** Start to propagate the rumor from user o_i separately and independently at time $t + T - t_i$. **end**
for(u: any node in the whole network) **do**
if(user u received n separate rumors from O) **then** Compute the maximum likelihood L(u,t) for
user u;
Add user u into the set U. **end**
if($|U| \geq \alpha N$) **then**
Keep the first αN suspects with large maximum likelihoods in U, and delete all the other suspects.
end

Output: A set of suspects U.

5.4 BLOCKING THE RUMOR SPREADING SOURCE

The rumor message verification process will be happening in the admin process[3]. The admin provides the warning to the user account whenever the admin gets the notification as rumor and the admin verifies using the live news updates from TIMES OF INDIA and also other articles. If the admin finds it to be rumor then he sends warning after three times and if the user continues to spread message then the admin blocks the user for the fifth time . The post shared by the user will be removed from every user's timeline in the network through Jordan Method. The admin verify the shared post consisting various messages and news from the API using text mining. The text mining is also known as data mining known as text analytics. It is the process of deriving high quality information from text. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, text mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Text analysis involves information retrieval, lexical analysis to study word frequency distribution, pattern recognition, tagging/annotation, information extraction, data mining techniques including link and association analysis, visualization, and predictive analytics. For text mining swoogle is used.

5.4.1 DYNAMIC BLOCKNG ALGORITHM

Different from the greedy blocking algorithm, which is a type of static blocking algorithm, we propose a dynamic rumor blocking algorithm aiming to incrementally block the selected nodes instead of blocking them at once. In that case, the blocking strategy is split into several rounds and each round can be regarded as a t. Thus, how to choose the number of rounds is also very important for the algorithm[3]. From the probabilistic perspective, to seek and formulate the likelihood of inactive nodes becoming activated in every round of rumor blocking.

Different from the case of greedy algorithm, the objective function of the dynamic blocking algorithm is implemented in several rounds. It is noticeable that the proposed greedy algorithm is a special case of the dynamic blocking algorithm with n. Accordingly, the dynamic blocking algorithm can be presented as following:

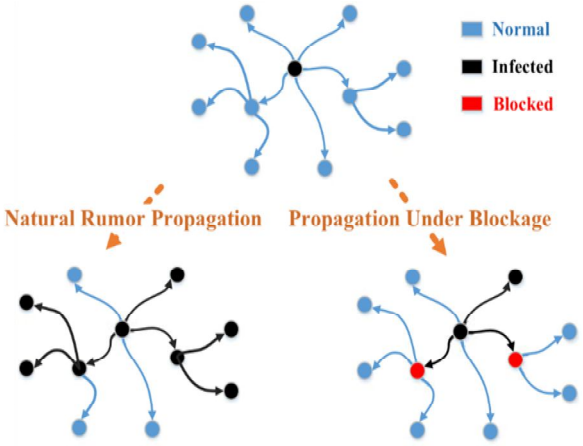

Fig3. Normal, Infected and Blocked nodes are identified using dynamic blocking algorithm.

Algorithm: Dynamic Blocking Algorithm

Input: Set of suspects V(t).

Method: Set of suspects is identified and blocked from the social network and removes the post from entirely from the timeline.

Output: $V(t_j)$

Initialization: $V(t)= \theta$

for(j= 1 to n) **do**
  for(i = 1 to k_j) **do**
    $\Delta f=f(t_j|s(t_j-1);A_i-1)-f(t_j|s(t_j-1);$
    u=arg max v belongs to $\theta(\Delta f)$;
    $A_i=A_i-1\backslash u;$
    $V(t_j)=V(t_j) \cup \{u\};$
  end for
end for
stop

5.4.2 TEXT MINING-SWOOGLE

The swoogle is a web search engine used for semantic web ontologies and documents. The swoogle is mainly used to extract and mine the data. It performs word to word comparison comparing the relevant meanings for a single word. Here wordnet and NLP is used for the comparison of the data. WordNet is a lexical database which groups the words in the sentences eliminating spaces and special characters and compares with its database. Here if any user identifies the rumor post then the user intimates to the admin. The admin compares the rumor post and the flash news using swoogle which gives a value. If the count value is less than 0.5 then the rumor posted is irrelevant to the news and the

admin can notify as rumor. If the count value is greater than 0.5 then the rumor posted is relevant or same to the flash news and thus the admin notifies the user that the status posted is not a fake message. The swoogle compares the status posted by the user with the all current flash news comparing each and every word in the sentence. It compares with all relevant meanings for a single word and finally displays a value for a sentence. The swoogle eliminates blank space and special characters. While analyzing the admin compares by giving the posted rumors without any special characters. The swoogle analyses and sends the result to the admin and the admin intimates to the user. If the admin finds to be a rumor then a warning message is sent to the user. If the user continues spreading rumor and if another user in the social network intimates the admin for the fifth time then the user is permanently blocked from the social network. The admin deletes the rumor post permanently from everyone's timeline so that it cannot be shared by any other user in the social network.

VI. METRIC CLASSIFICATION

Here in metric classification FN is True Negative representing the true news as fake news, TP is True Positive representing the true news as true news, FP is False Positive representing the fake news as true news and TN is False Negative representing the fake news as fake news. Here the values of precision and recall are inversely proportional to each other. The value of precision decreases and recall increases based on the number of news feed given by the users in the network.

Table1. Representing the metric classifiers.

CASE	NEWS	CLASSIFIER OUTPUT	METRIC TABLE
1	True news	True news	TP
2	True news	Fake news	FN
3	Fake news	True news	FP
4	Fake news	Fake news	TN

The value of precision and recall can be calculated by
Precision**(P)** =TP/(TP+FP)
Recall**(N)** =TP/(TP+FN)

Table2. Representing the values of precision and recall calculated from TP,FP,FN.

No of news feed	TP	FP	FN	Precision	Recall
100	88	2	10	0.977	0.897
200	180	5	15	0.972	0.923
300	270	8	22	0.971	0.924

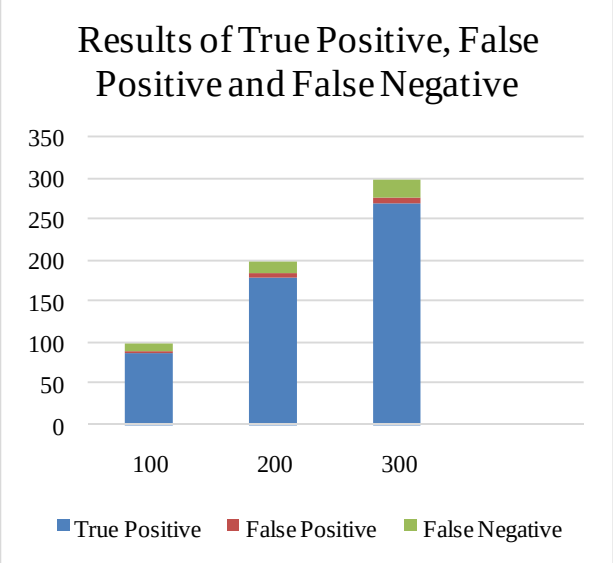

Fig4. The experimental results of true positive, false positive and false negative values in the Socialbook.

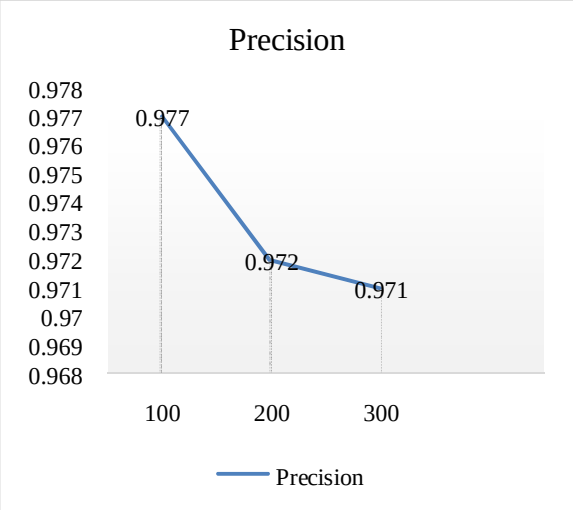

Fig5. The graph representing the experimental result of precision in the Socialbook.

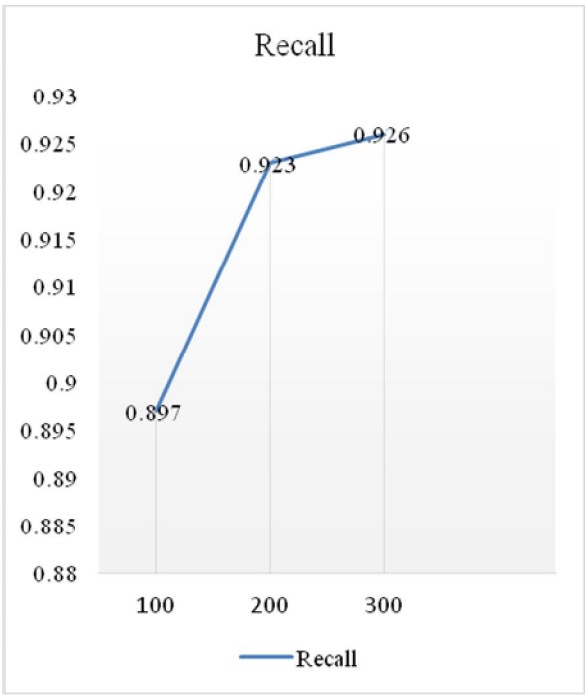

Fig6. The graph representing the experimental result of recall in the Socialbook.

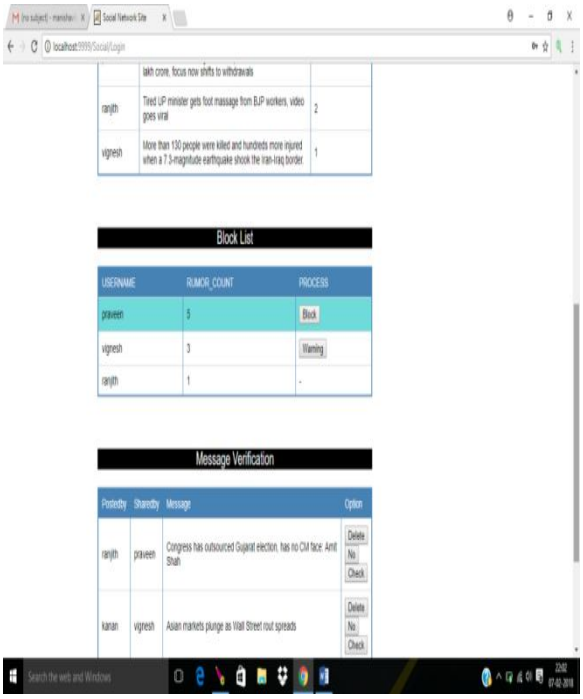

Fig8.Admin process of checking the news, deleting the news and gives warning to the user or blocks the user.

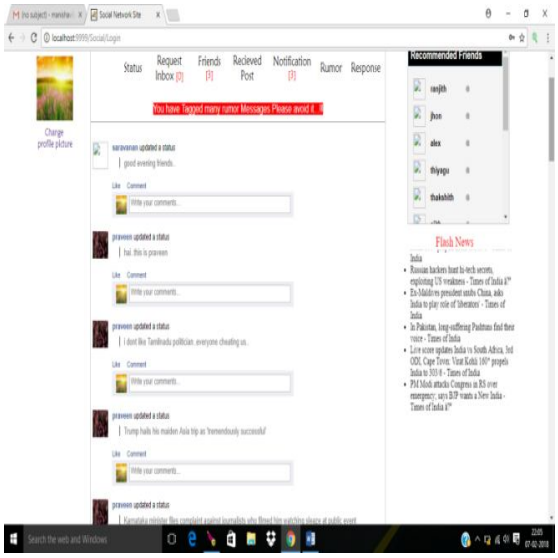

Fig7. Posting news among friends.

Fig9. Admin gives warning to the user by verifying the post with the TOI API.

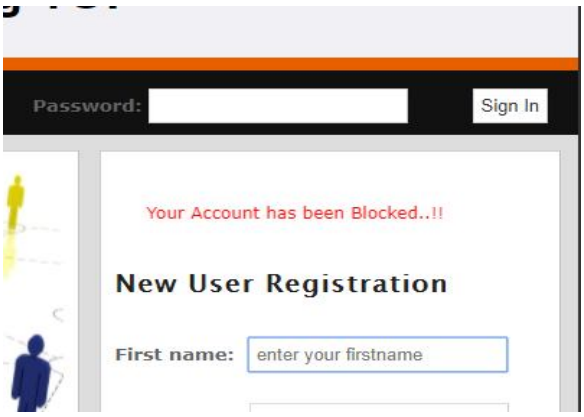

Fig10. Admin blocks the user if the user is identified as suspect spreading rumor.

VII. EXPERIMENTAL RESULTS

The experimental analysis gives the efficiency of the project. Here the Table 1 represents the metric classifiers used to calculate the precision and recall. Here Precision(P) =TP/(TP+FP) is calculated by the values of TP, FP and Recall(N) =TP/(TP+FN) is calculated from the values of TP and FN. The Table 2 represents the values of precision and recall. By giving various number of news feed the rumor posts are identified that is the values of TP, FP and FN are calculated. The fig.4 represents the true positive, false positive and false negative news from100, 200 and 300 news feed posted by various users. The fig.5 represents the graph defining the precision value for the various number of news feed and the fig.6 represents the graph showing the recall value for 100, 200 and 300 number of news feed. Here the graphs represent that the values of precision decreases and recall increases thereby representing that they are inversely proportional to each other. The fig.7 represents the user posting news among the friends. The fig8 represents the admin process of checking, deleting and gives either warning to the user or blocking the user entirely from the social network. The fig.9 represents the admin giving warning to the user posting rumor message and fig10 represents the admin blocking the rumor spreading source.

The experimental result shows that the rumor spreading source is identified through reverse dissemination process and the fake news are compared with the news updates of TOI API and swoogle to identify the rumor source. Thus the admin blocks the user if the user reaches the threshold value of posting the rumor message. Thus the proposed system works efficiently to identify and block the rumor source from the social network.

VIII. ADVANTAGES

Here the reverse dissemination and dynamic blocking algorithm is used to identify the rumor source. The TOI gives the current updates of news which can be used by other users to identify the fake news. The admin can verify the rumor post by using swoogle which gives the accurate result. A dynamic rumor diffusion model incorporating both global rumor popularity and individual tendency is presented. Then the concept of user experience utility and propose a modified version of utility function to measure the relationship between the utility and blocking time is introduced. It won't block the user because of only one rumor message from the user, first it gives warning message to the user and if the user repeats the same it blocks the user**.** Experiments implemented on real world social networks show the efficiency of our method.

IX. APPLICATIONS

This can be implemented in many social networks like facebook, twitter . It can also be used in cloud based applications and in many websites to avoid fake ads leading to another fake webpages containing virus and unnecessary data. It can also be used in google playstore to eliminate fake apps.

X. CONCLUSION AND FUTURE WORK

Thus using TOI API the rumor post can be eliminated from the social network and the user spreading rumor is entirely blocked from the social network to avoid spreading the rumor further in the network. Using swoogle the rumor post is identified and it is intimated to the admin. The swoogle which evaluates the rumor posted by the user gives the count value and based on count value the admin assures that the post as rumor and eliminates the rumor post from the network. The future enhancement can be done using the database to store the news history, the locality news and all the flash news regarding each and every domain can be included such as combining all the news across the world to verify the rumor message posted in the network.

REFERENCES

[1] A. Bessi, et al., "Viral misinformation: The role of homophily and polarization," in Proc. 24th Int. Conf. World Wide Web, 2015, pp. 355–356.

[2] A.Vineela and K.Venkateswara Rao, "Secure Geographic Routing Protocol in MANETs", Proceedings of International Conference on Emerging Trends in Electrical and Computer Technology(ICETECT),pp.1-7, 2015.

[3] Biao Wang, Ge Chen, Luoyi Fu, Li Song, and Xinbing Wang, "DRIMUX:Dynamic Rumor Influence Minimization with User Experience in Social Networks" IEEE Transactions on Knowledge and Data Engineering, Vol.29 No.10,2017

[4] B.Ribeiro,N. Perra and A. Baronchelli, "Quantifying the effect of temporal resolution on time-varying networks," Sci- entific reports, vol. 3, 2013.

[5] C. Budak, D. Agrawal, and A. E. Abbadi, "Limiting the spread of misinformation in social networks," in Proc. 20th Int. Conf. World Wide Web, 2011, pp. 665–674.

[6] D. Kempe, J. Kleinberg, and E. Tardos, "Maximizing the spread of influence through a social network," in Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2003, pp. 1175–1180.

[7] E. Serrano, C. A. Iglesias, and M. Garijo, "A novel agent-based rumor spreading model in twitter," in Proc. 24th Int. Conf. World Wide Web, 2015, pp. 811–814

[8] F. Peter. (2013, April 23) 'bogus' ap tweet about explosion at the white house wipes. billions off us markets. The Telegraph, Finance/Market. Washington

[9] Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang and Wanlei Zhou,"Rumor Source Identification in Social Networks with Time-Varying Topology", IEEE Transactions on Dependable and Secure Computing, Vol.10 No.17,pp.10-1109, 2017

[10] Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs",IEEE Transactions on Mobile Computing, Vol.10, No.9, pp.123-146, 2015.

[11] M. M. Kircher, "A woman named Isis claims she's been blocked from signing into Facebook," 2015.

[12] M. P. Viana, D. R. Amancio,andL.d. F. Costa,"On time varying networks",Journal of Informetrics, vol. 7, no. 2, pp. 371–378, 2013.

[13] Rong and Q. Mei, "Diffusion of innovations revisited: From social network to innovation network," in Proc. 22nd ACM Int. Conf. Inf. Knowl. Manag., 2013, pp. 499–508.

[14] S. Fiegerman, "Facebook, google, twitter accused of enabling isis," 2016. [Online]. Available: http://money.cnn.com/2016/12/20/ technology/twitter-facebook-google-lawsuit-i sis

[15] S. Shirazipourazad, B. Bogard, H. Vachhani, and A. Sen, "Influence propagation in adversarial setting: How to defeat competition with least amount of investment," in Proc. 21st ACM Int. Conf. Inf. Knowl. Manag., 2012, pp. 585–594.

[16] W. Chen, C. Wang, and Y. Wang, "Scalable influence maximization for prevalent viral marketing in large-scale social networks," in Proc. 16th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2010, pp. 1029–1038.