https://doi.org/10.48009/2_iis_2015_1-15

Issues in Information Systems
Volume 16, Issue II, pp. 1-15, 2015

ON SECURITY NEGOTIATION MODEL DEVELOPED FOR THE SECURITY OF THE SOCIAL NETWORKING SITES FROM THE HOSTILE USER

Ruchi Verma, Jaypee University of Information Technology, ruchi.verma@juit.ac.in
Nitin, Jaypee Institute of Information Technology, delnitin@ieee.org

ABSTRACT

The utility and attractiveness of online communication has amplified to astounding levels, so there is no arguing on the convenience offered by social networking sites such as Facebook, Twitter etc. Needless to say that computer mediated communication has defied all social, cultural and geographical boundaries, connecting the globe at a zero distance. Sadly enough, with online communication getting ingrained into our daily communication, breach of netiquettes is being done with nonchalance. In online communication, generally flaming starts with exchange of rude comments and spirals to online aggression. In order to prevent online communication from being tainted, it is essential to keep away the hostile users from communication platform. This paper presents a negotiation security model which checks and prevents online flaming. Moreover it also flags the presence of flaming in social conversation and blocks hostile users from flaming in business communication and negotiation.

Keywords: Flame Detector Model, Hidden Markov Model, Flaming, Negotiation, Mean Score, Notification.

INTRODUCTION

Though we have ascribed many benefits to online communication, there is a flip side emerging to it in the form of online aggressive behavior. Now days social networking sites are becoming a platform for business users for creating contacts, finding buyers and sellers, hosting a commercial profile and others activities to promote their businesses. Therefore, it is very important to keep the hostile users away from the online platform to maintain a healthy communication environment and promote business negotiations. This paper, presents a model which will notify the presence of flaming in online communication and block the users who indulge in flaming during online business negotiations.

FLAMING IN SOCIAL NETWORKING SITES AND FLAME DETECTOR TOOL

Social Networking Sites (SNS) were used to contact acquaintances, colleagues, friends and relatives but with the advances in website design, people also started to interact with strangers through these sites [1, 2, 3, 4, 5, 6, 7, 8]. Out of these strangers research has also shown that males have a greater tendency to flame than female participants [1]. Further, SNS are the places where the user can do all its gossips with their relatives as well as with their friends and might also do negotiation with the other business organizations. Today the popularity of SNS has increased immensely because it serves as a common platform for users to do diverse activities. Some users use it as a medium of self expression, others use is for social networking while still others use if for business communication and negotiation the augmented communication of Internet made social networking site very fashionable.

If face-to-face conversation occur in a willing atmosphere often synchronized by mutual tweaking and amendment [9, 10], argument in social networking sites by the computer mediated communication occurs in a much fewer willing atmosphere because of the special conditions strained by the intermediate itself [11]. In the social networking site, it is no way of guarantees that the information specified by the user is the authentic one. The use of counterfeit information or the identities, frequently of a dissimilar name, age, sex, address, name of the organization etc. is widespread enlarge in electronic communities [12, 13]. After analyzing the number of studies [14] instigate the happening of unpleasant behavior is overestimated, the user used to use rigorous language in different areas of the computer mediated communication. The diplomat infringe of netiquette engross the use of *flames* [1, 2, 3, 4, 5, 6, 7, 8]. Accordingly the Siegel and colleagues distinct "messages that are precipitate, often personally derogatory, ad hominem attacks directed toward someone due to a position taken in a message distributed to the group" [15]. Thus, the flame is further classified into numerous categories such as direct flame, indirect flame, straight flame and

the satirical flame [16]. Moreover, to give more attention on the flaming, the researcher creates the survey of the flaming inclination by captivating the three situation and the five status messages and making the people to click on the status which, they fond of, use to give the authentic result on the research of the performance tendency of the user [17, 18]. Therefore, the behavioral tendency of the user gives the strength of the flaming i.e. in which frame of mind the user had chosen the status [19].

A flame detector model has been proposed to detect the occurrence of flaming in online communication. This model is installed on the local system and it gets plugged into any of the social networking sites such as Facebook, Twitter etc . Flame detector model consists of three components as shown in the figure 1.It consists of social networking sites, web services and the flame detector.

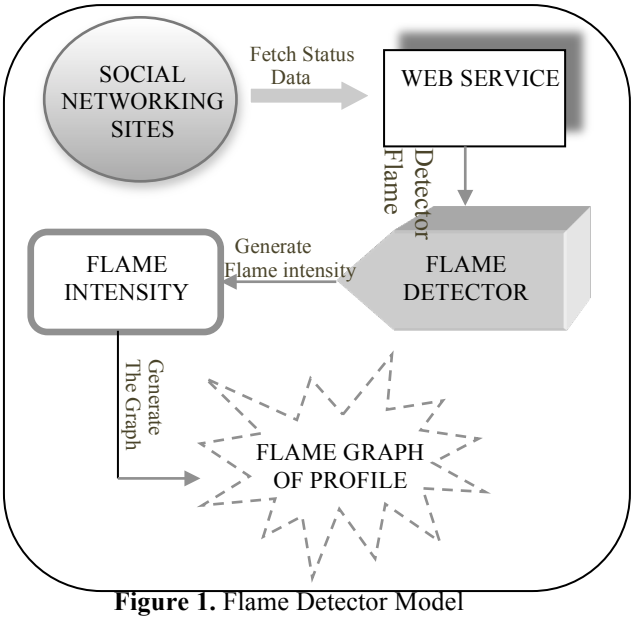

Figure 1. Flame Detector Model

As shown in the figure 1, the flame detector model has three components. The first components is the social networking site from where gets its input. The second is web services with the help of which the model extracts the status of the user account and posts it to the model as and when required. The model fetches data from the sites with the help restful services (see figure 2). The user logs in the developer site with their login id and creates an API. This enables the user to get an authorized uniform resource locator, consumer key and secret key. After getting this key, the restful services get operational and data can be fetched from the site. There is predefined thesaurus which contains words that are considered as flames. There are further categorized into five categories based on which the graph of flame intensity is generated. This graph will show the amount of flaming that has been detected in a users account. In addition to this, to avoid the hostile users from flaming there should be some security model that defends the networking sites from the flaming activities.

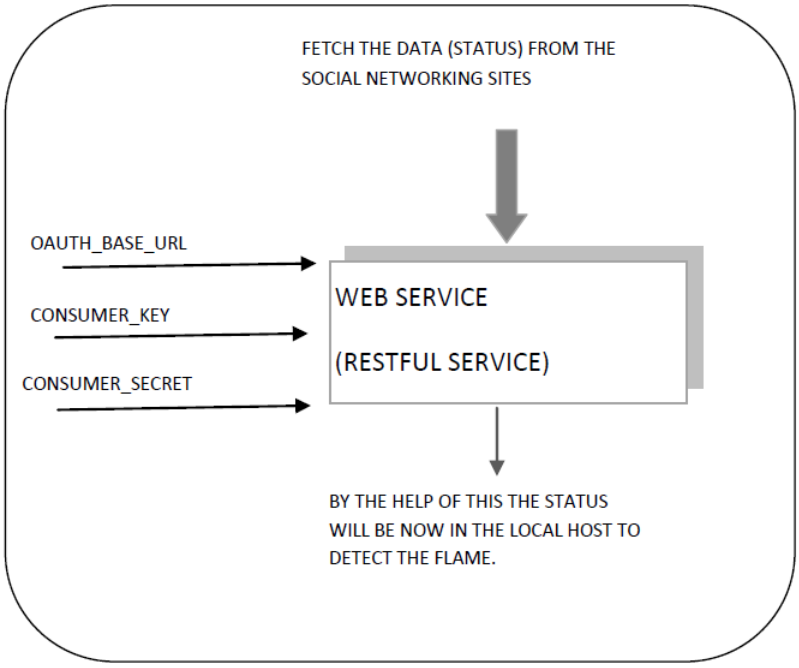

Figure 2. Web Service (Restful Service)

RESEARCH METHODOLOGY AND RESULTS

Our research centered upon the following research questions:

1. Is the Security Negotiation Model successful in blocking the users who indulge in flaming during online negotiation and business communication using Flame Detector Model?
2. Is the Security Negotiation Model using flame detector model successful in detecting the flames in communication that span over short as well as long periods of time?

A research is conducted to answer the above mentioned research questions. In the next section we have provided the architectural details of the Security Negotiation Model that we have proposed in this paper.

Security Negotiation Model

As the social networking site gets infiltrated with flaming it results in multiple users sending stimulating response to flames. This leads to infuriating exchange of flames and the users get trapped in non constructive conversation. This does not provide an enabling atmosphere for any constructive professional conversation, negotiation or business deals. There is a need to streamline online communication so that users who are interested in the business deals and negotiation can carry out an undisturbed formal conversation and users who are interested in social conversation can proceed with their informal conversation. To enable this, we introduced security negotiation model (see figure 3). This model divides the networking space into two compartments one for local gossip and the other for business communication. Before applying this model, we need to compartmentalize the server into two sections as in figure 3.

The first section is for social conversation and the second section is for business communication. In the social conversation section, communicants can freely gossip, exchange and upload photographs and videos. In the social conversation section users are free to communicate informally, write their status message, upload photographs and gossip freely. On the contrary, in the negotiation section the communication has to be done in a formal and professional manner. This will be a common platform for business communication across various cultures, businesses and professions across the world. Business community across the globe can interact, discuss, communicate and share any news or information. It provides a hygiene space for business communication and

provides excellent opportunity for businessmen to negotiate, buy and sell commodities. For this to happen it is essential that the sanctity of the business platform is maintained i.e. all users are genuine and is purely related to business.

After getting space according to their respective requirement, the users can proceed with their online communication. As soon as flaming occurs in either of the sections, it is detected by the Flame Detector Model. Once detected, it is treated depending on to which compartment the userid involved in flaming belongs. In case the flame has been detected in the social conversation section, a notification is sent to the user but in case flaming is detected in the negotiation section then it passes through the Hidden Markov Model. It is explained in detail as below.

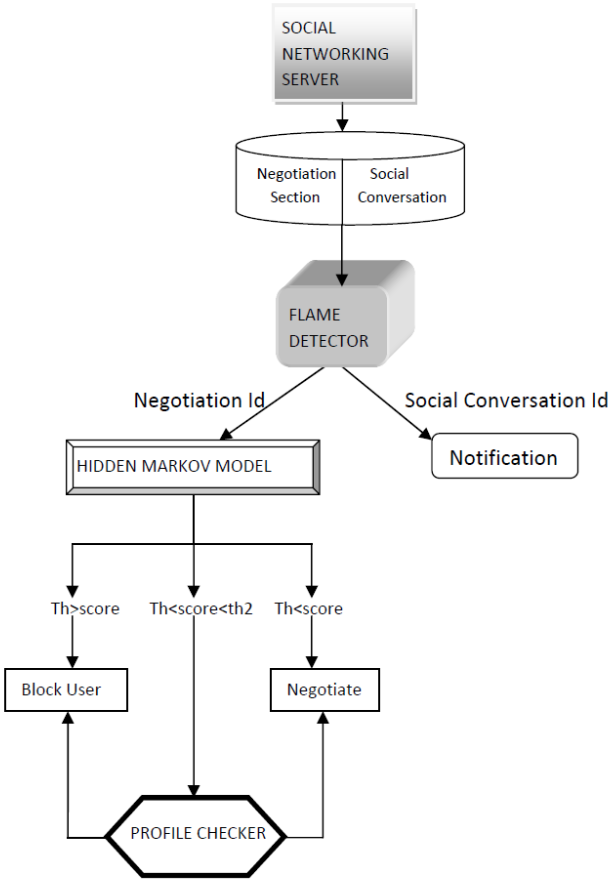

Figure 3. Architecture of Security Negotiation Model

Social Conversation Section

This section is for social networking where users can communicate with each other, create groups and freely involve in social conversation. In case there is any flaming in this section the flame detector tool creates a graph of the intensity of the flame i.e. it is low intensity or high intensity. After detecting the flame its intensity is determined by the category in which the flame word falls. The categories of the flame are predefined as hostile, aggressive, offensive and uninhibited. Thus all flaming words are detected by the flame detector tool and graph is generated. This graph will be notified to the user's profile and if the flaming rate is high then the user can block the user doing flaming or can report it to the social networking team.

Business Communication and Negotiation Section

To understand this section we will need to briefly know about the Hidden Markov Model as explained below

Hidden Markov Model

A Hidden Markov Model (HMM) is a double embedded stochastic process with two hierarchy levels. It can be used to model much more complicated stochastic processes as compared to a traditional Markov model. An HMM has a finite set of states governed by a set of transition probabilities. In a particular state, an outcome or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to an external observer [24].

In this model the HMM will save a set of records of the user over a time period of seven days. It is a continuous process and the set of latest seven records are saved. Then mean score of these set of records is calculated based on past behavior of the user. The HMM sets two threshold values at the beginning, th1as the lower threshold value and th2 as higher threshold value. The values of th1 and th1 are predefined.

After briefly understanding Hidden Markov Model, following is how a flame is treated in the negotiation section. In case the flame detector tool detects flaming in this section, the userid immediately passes through the HMM. The HMM calculates the mean score of the userid and then the mean score is matched with the two predefined threshold values th1 and th2.

If the users mean score comes below or equal to th1 then the user gets rejected as it is observed that the user is involved in very less or negligible negotiation. Thus the probability of doing negotiation is low and flaming is high. If the mean score falls between th1 and th2 then the userid passes through the profile checker. The profile checker is a part of the model where all the information, warning messages or notifications sent to the user are stored. When the HMM cannot decide on the authenticity of the user, it will send a query to the profile checker. It checks whether any warning messages or notifications have been sent to the userid. In case the number of notifications sent is high then the userid is blocked. If that is not the case then a notification is sent to the user and allowed to continue business communication. If the mean score is greater than th2 the userid comes in the high probability section indicating that the user involves in serious business communication as per the past records and the case is ignored. In the next section the Security Negotiation Model is validated through working of the Algorithm, Experimental Results and Case Studies.

Working of the Algorithm

In this section using figure (4-10) we have provided the screen shots of the actual algorithm working in the background of flame detector model.

Figure 4. Connection Window

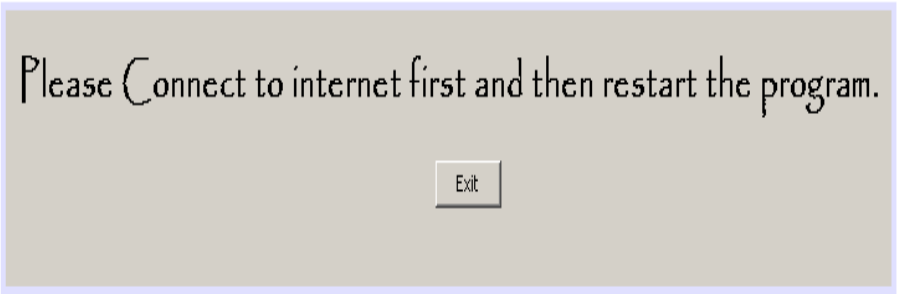

Figure 5. No Internet Connection Message

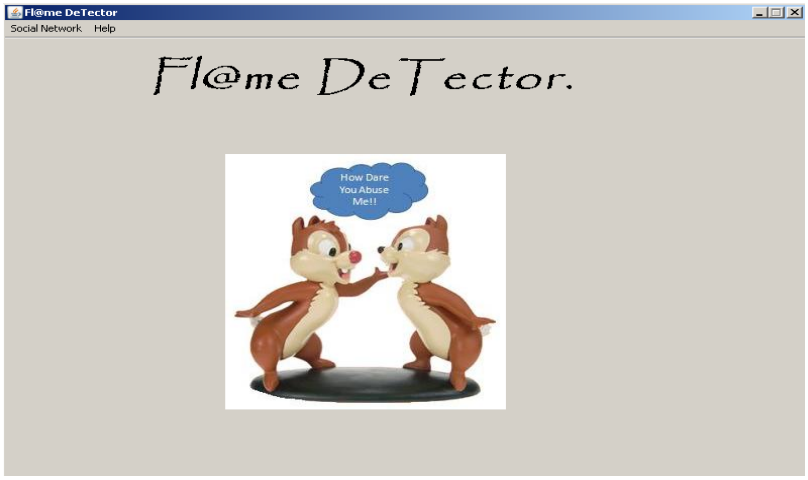

Figure 6. The Main Window of the Flame Detector Tool

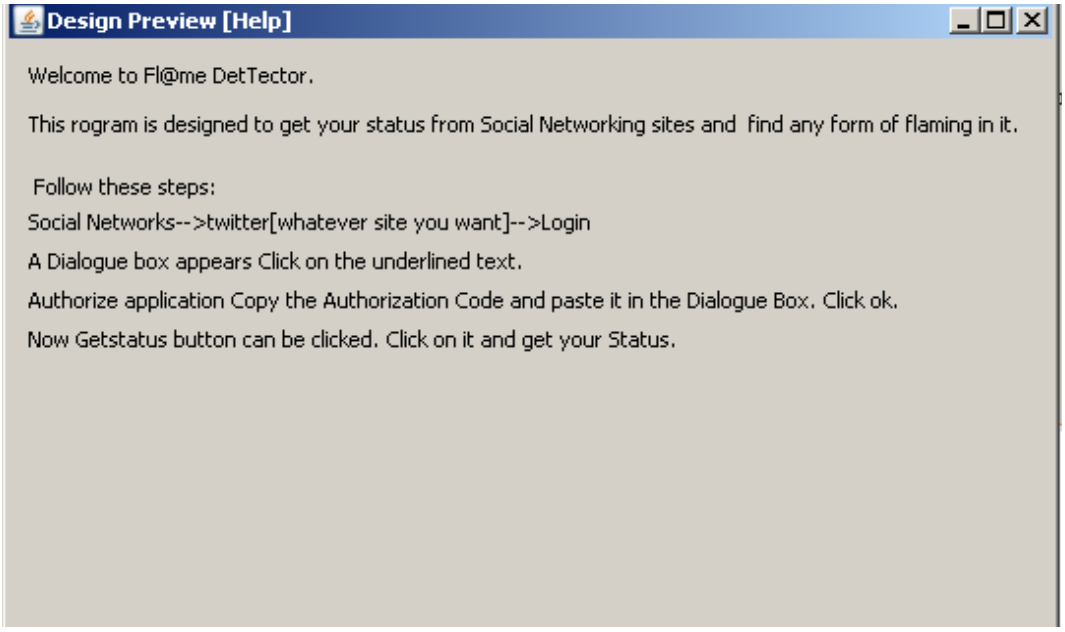

Figure 7. Important Key Information to Generate the KEYs

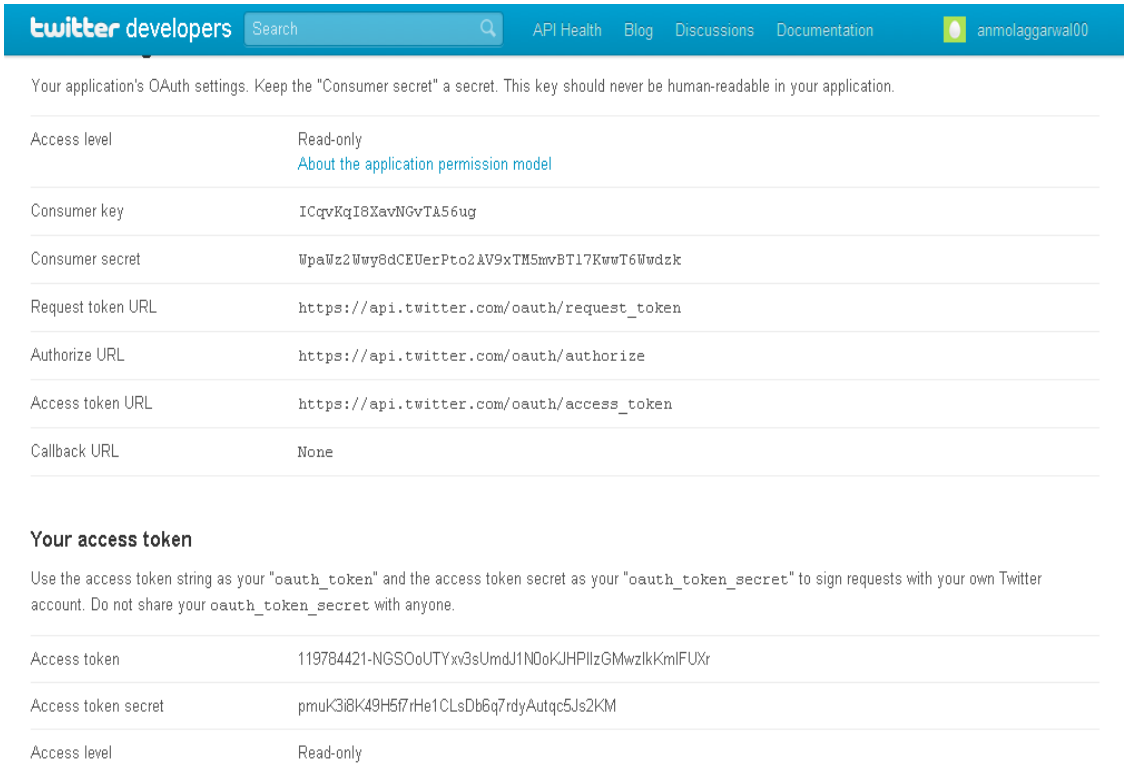

Figure 8. Various KEYs that will Help to Login into the Twitter Account

The Connection Window will appear as the first window to setup the connection. If the internet is up then the connection with the Twitter account is setup otherwise it will give the no connection message. Once the connection is established then the flame detector tool starts and the required key information is provided. The access tokens are generated and the important keys that are generated are Consumer Key, Consumer Secret, Request Token URL, Authorize URL, and Access Token URL. Finally, the access to the Twitter Account is established. There are three important keys that are generated: Access Token, Access Token Secret and Access Level. They are scanned by the Flame Detector Tool and get ready to undergo the flaming detection. All messages that are posted on the Twitter account of the subject are passed through the tool working in the background which detects the flaming words and produces the result based on their intensity.

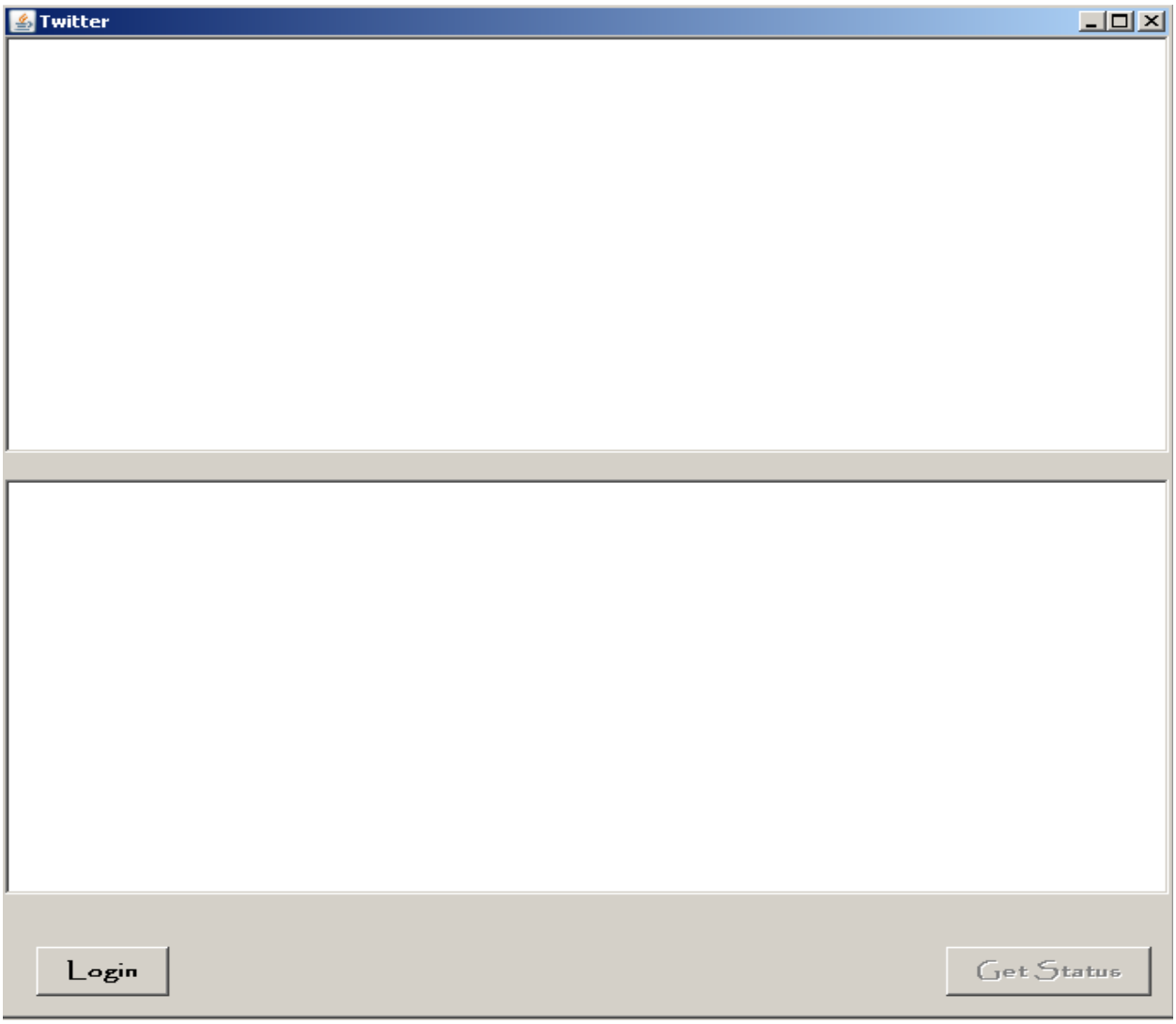

Figure 9. The Twitter Account that has Been Scanned by the Flame Detector Tool is Now Ready to Undergo the Flaming Detection

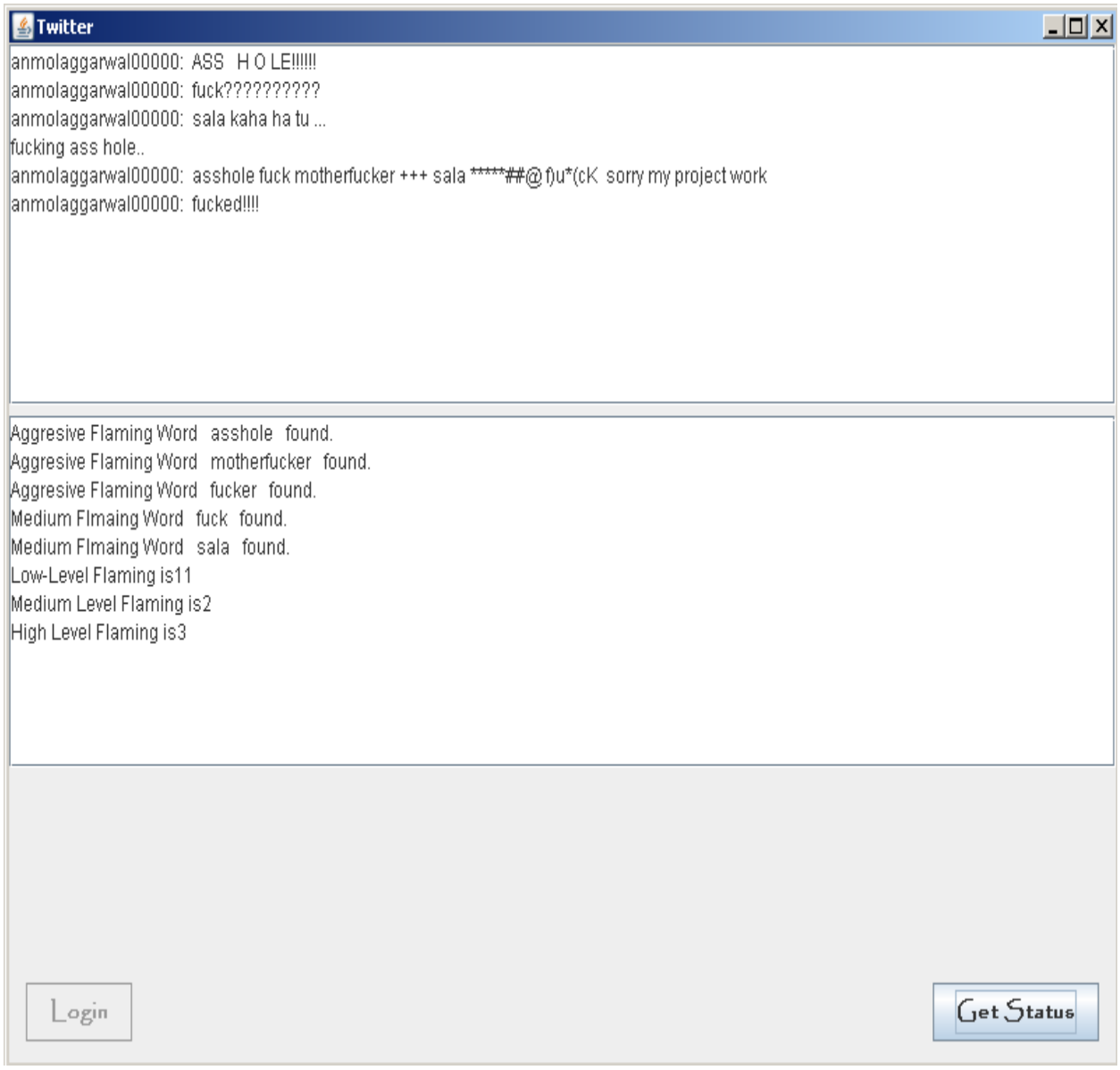

Figure 10. The Flame Detector Tool has Detected the Flaming Words and Provided the Result Based on their Intensity

Experimental Results

Assume that the parameter p(f) is the probability of flaming, p(n) is the probability of negotiation , th1 is lower threshold value , th2 is higher threshold value and the model has the capacity of storing record of a user for a period of 7 days. The record of latest seven days conversation is recorded for a user. As the days proceed, the user's record will get automatically stored in its memory and the model will reflect the record of the latest 7 days. The data that has been used here is hypothetical data and it is not outcome of any structured, semi-structured, or unstructured interviews. As per Hidden Markov Model, the value th1 and th2 will be predefined at the beginning of the experiment, th1 be set to 30% and th2 be set to 70%. Mean score is considered as the users average probability of doing negotiation. Therefore we will consider three cases, case1 when the mean score is less than th1; case 2 when the mean score is between th1 and th2; case3 when the mean score is greater than th2.

Mean score= negotiation done by the user
Lower threshold percentage (th1) = **30**%,
Upper threshold percentage (th2) = **70**%,
Probability of flaming= **p**(**f**),
Probability of negotiation= **p**(**n**),
Total number of records = T

Case Study 1

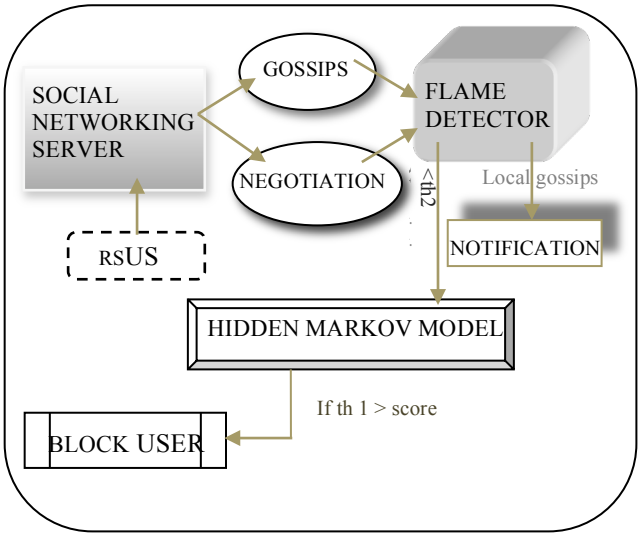

Figure 11. Security Negotiation Model to Validate Low Percentage of Negotiation Done by the User

Table 1. Table of the Past Behavior of Mr. X

Days	**Records of Flames and Negotiate**						
	1st	**2nd**	**3rd**	**4th**	**5th**	**6th**	**7th**
F or N	F	N	F	F	N	F	F

Following (refer Table 1), is the record of the behavior of the user for a period of seven days. The above table shows that the user is involved in flaming five times and in negotiation only twice. Therefore:
Probability of flaming: P(f)=5/7,
Probability of negotiation: P(n)=2/7,
Percentage of flaming: (p(f))*100 = (5/7)*100 = 71.42%,
Percentage of negotiation: (p(n))*100 = (2/7)*100 = 28.57%,
The mean score will be the percentage of negotiation i.e.: 28.57%

If the mean score is less than th1 it implies that the user involves in flaming more than negotiation, leading to a conclusion that the user does not seem interested in business or negotiation (refer Figure 11). Therefore, this user is not eligible for a negotiation account and is blocked for further communication in the negotiation section. Figure 12, shows the behavior tendency of the user against the percentage of the negotiation and flaming done by the user and it can be easily concluded that the user has low percentage of tendency of negotiation.

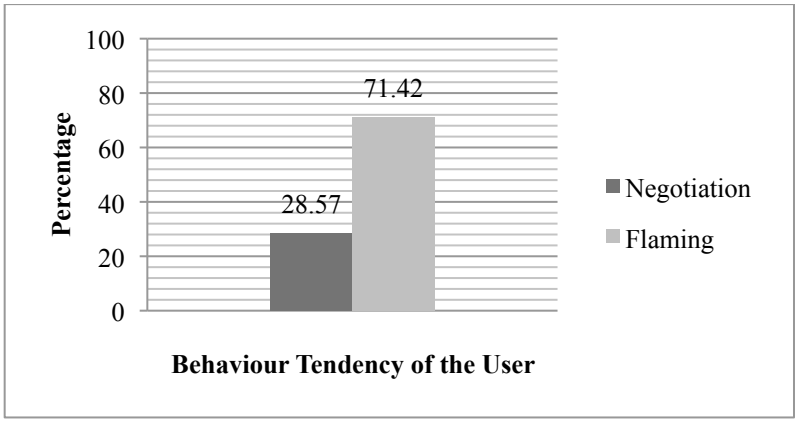

Figure 12. Graph of the Low Percentage of the Negotiation Done by the User

Case Study 2

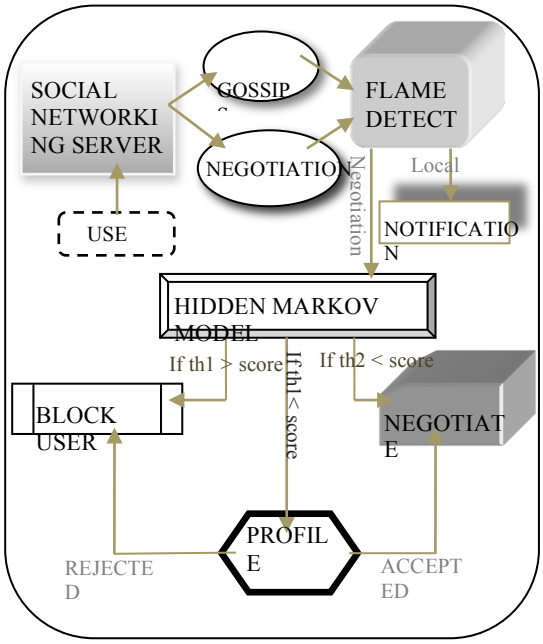

Figure 13. Security Negotiation Model to Validate Moderate Percentage of the Negotiation Done by the User

Table 2. Table of the past behavior of Mr. X

Days	Records of Flames and Negotiate						
	1st	2nd	3rd	4th	5th	6th	7th
F or N	N	N	F	F	N	N	F

Following (refer Table 2), is the record of the behavior of the user for a period of seven days: The above table shows that the user has been involved in flaming thrice and in negotiation only four times.
Percentage of flaming: (p(f))*100 = (3/7)*100 = 42.85%,
Percentage of negotiation: (p(n))*100 = (4/7)*100 = 57.14%,
The mean score will be the percentage of negotiation i.e.: 57.14%,

If the mean score falls between th1 and th2 then the userid passes through the profile checker, where all the information, warning messages or notifications sent to the user are stored (refer Figure 13). If the user has been already notified and warning messages have been sent to him then the user is blocked from further communication. If that is not the case the user is sent a notification and allowed to continue business communication. Figure 14, shows the tendency of the user against the percentage of the negotiation and flaming done by the user and it can be easily concluded that the user has moderate percentage of tendency of negotiation.

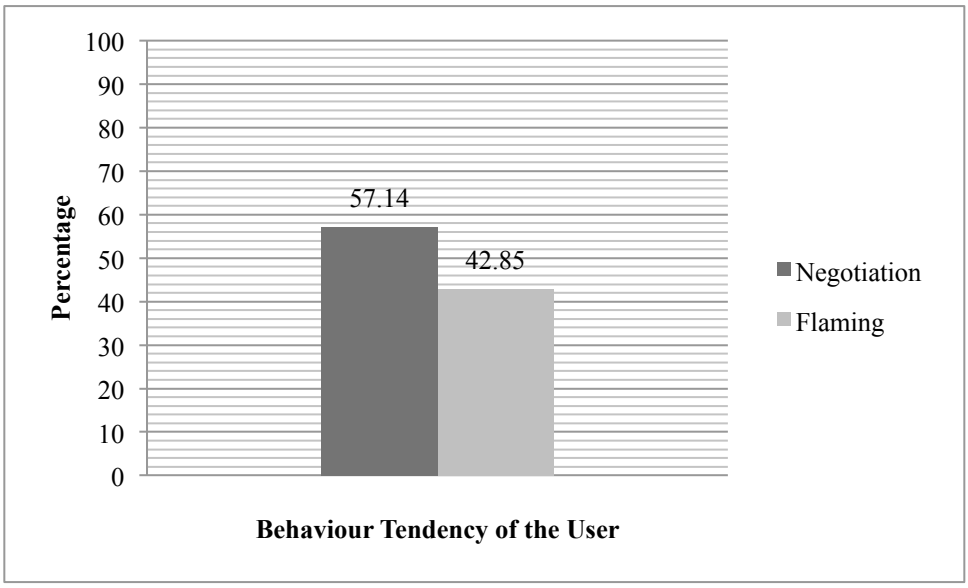

Figure 14. Graph of the Moderate Percentage of the Negotiation done by the User

Case Study 3

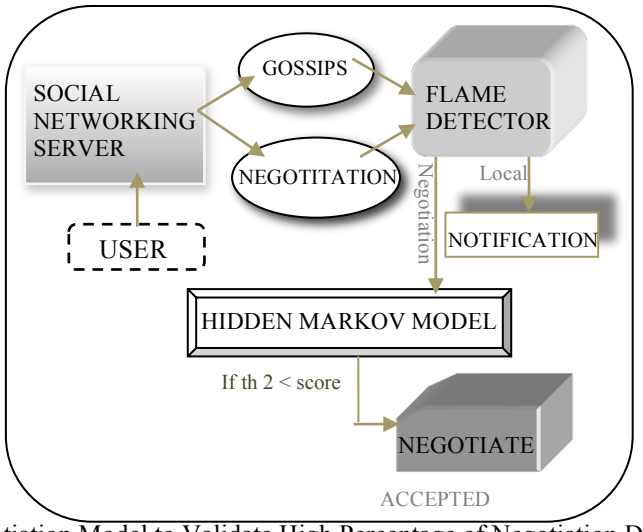

Figure 15. Security Negotiation Model to Validate High Percentage of Negotiation Done by the User

Table 3. Table of the past behavior of Mr. X

Days	Records of Flames and Negotiate						
	1st	2nd	3rd	4th	5th	6th	7th
F or N	N	N	F	F	N	N	N

Following (refer Table 3), is the record of the behavior of the user for a period of seven days: The above table shows that the user has been involved in flaming twice and in negotiation five times.
Percentage of flaming: (p(f))*100 = (2/7)*100 = 28.57%,
Percentage of negotiation: (p(n))*100 = (5/7)*100= 71.43%,
The mean score will be the percentage of negotiation i.e. = 71.43%,

In case the mean score of the user is greater than th2 then it indicates that the user involves in serious business negotiation and is allowed to continue communication (refer Figure 15). Figure 16, shows the tendency of the user against the percentage of the negotiation and flaming done by the user and it can be easily concluded that the user has high percentage of tendency of negotiation.

Table 4. The demographic details of the three users whose records we have covered for a period of 7 days are as follows

S.NO.	Nationality	Age	Gender	Online Usage
1	European	18	Male	Very active and updated user
2	American	22	Male	Very active and updated user
3	Asian	27	Female	Very active and updated user

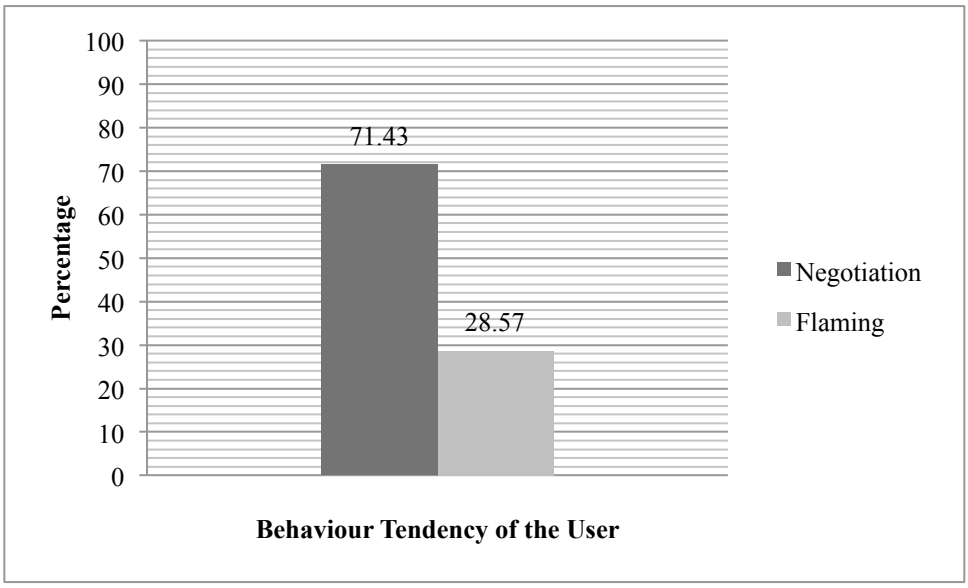

Figure 16. Graph of the High Percentage of the Negotiation Done by the User

Limitations of the Security Negotiation Model

The current tool is able to detect the flames in communication over a short period of time using the security negotiation model however it fails to perform in situations where the flaming starts in the middle of the communication that lasts for longer time period.

The database of the flaming words has to be updated regularly and since it is a very cumbersome job, therefore a mechanism needs to be devised to add the flaming words to the database automatically.

CONCLUSION

The convenience and advantages of computed-mediated communication is evident to one and all. However, as all boons have a flip side to them it is getting infiltrated with hostile and aggressive exchange of words. To keep the immense utility of online communication intact, it is essential to prevent it from getting adulterated with aggression and online misbehavior. This paper presents a security negotiation model which flags the presence of flaming in online communication and blocks flamers from business communication and negotiations. In future scope of work, we plan to take records of over 200 samples from diverse origin, gender and age.

REFERENCES

1. M. Zuckerburg, 500 million stories, South Atlantic Quarterly, vol. 92, pp. 559-568, 2010.
2. R.A. Friedman and S.C. Currall, Conflict escalation: Dispute exacerbating elements of e-mail communication conflict, *Human Relations, 56*(11), 1325-1347, 2003.
3. T.M. Harrison and L. Falvey, Democracy and new communication technologies, Communication Yearbook, 251-33, 2002.
4. E.M. Landry, Scrolling around the new organization: The potential for conflict in the on-line environment, *Negotiation Journal, 16*(2), -142, 2000.
5. M.L. Markus, Finding a happy medium: Explaining the negative effects of electronic communication on social life at work, *ACM Transactions on Information Systems, 12*(2), 119-149, 1994.
6. D.A. Moore, T.R. Kurtzberg, L.L. Thompson and M.W. Morris, Long and short routes to success in electronically mediated negotiations: Group affiliations and good vibrations, *Organizational Behavior and Human Decision Processes, 77*(1), 22-43, 1999.
7. P.B. O'Sullivan and A.J. Flanagin, Reconceptualizing "flaming" and other problematic messages, *New Media & Society, 5*(1), 69-94, 2003.
8. D.M. Boyd and N.B. Ellison, Social network sites: Definition, history, and scholarship, *Journal of Computer-Mediated Communication, 13*(1), article 11, 2007.
9. C. Goodwin and J. Heritage, Conversation analysis, Annual Review of Anthropology, 19, 83-307, 1990.
10. C. Galimberti, La conversazione [Conversation]. Milan, Guerini e Associati, 1992.
11. S.E. Brennan, Conversation with and through computers, User modelling and user-adapted Interaction, 1, 67-86, 1991.
12. P. Curtis, Communication via MUD: Social phenomena of virtual reality based on text, Sistemi Intelligenti, 8, 229-253, 1996.
13. G. Mantovani, Virtual reality as a communication environment: Consensual hallucination, fiction and possible selves, *Human Relations, 48*, 669-683, 1995.
14. J.B. Walther, J.F. Anderson and D.W. Park, Interpersonal effects in computer-mediated interaction: A meta-analysis of social and antisocial communication, *Communication Research, 21,* 460-487, 1994.
15. J. Siegel, V. Dubrovsky, S. Kiesler, and T.W. McGuire, Group processes in computer-mediated communication, *Organizational Behaviour and Human Decision Processes, 37*, 157-187, 1986.
16. Nitin, A. Bansal, S. Sharma, A. Aggarwal, K. Chaudhary, S. Goyal, K. Kumar, K. Jain, M. Bhasin, Classification of Flames in Computer Mediated Communications, *International Journal of Computer Applications, 14*(6), 21-26, 2011.
17. Nitin, A. Bansal and D. Khazanchi, Understanding Perceived Flaming Tendencies on Social Networking Sites: An Exploratory Study, Issues in Information Systems (IIS), vol. XII(1), (ISSN 1529-7314, 425-435, 2011.
18. Nitin, A. Srivastava, A. Dwivedi, K. Sood and M. Gupta, Behavioural Responses and Proclivity of Facebook Users towards Flaming, Issues in Information Systems (IIS), XIII(1), ISSN 1529-7314, pp. 25-39, 2012.
19. A.K. Turnage, Email flaming behaviors and organizational conflict. *Journal of Computer-Mediated Communication, 12,* Article 3, 2007.
20. S.S.P. Shukla and Nitin, Detecting the Flames on the Real Time Status through Flame Detector, Proceedings of the 2nd IEEE International Conference on Advances in Computing and Communications, 255-258, 2012.
21. S.S.P. Shukla, N.S. Parande, A. Singha, A. Sharma, A. Khare and Nitin, Analyzing Profile of Hostile Users through the Hybrid Model, Proceedings of the 13th International Conference on Internet Computing, 2012.

22. S.S.P. Shukla, Nitin, S.P. Singh, N.S. Parande, A. Khare and N.K. Pandey, *Flame Detector Model: a Prototype of Detecting Flame in Social Networking Sites,* Proceedings of the 14th IEEE International Conference on Computer Modeling and Simulation, 553-558, 2012.
23. Nitin, K. Nishant, P. Sharma and P. Rastogi, Layered Based Approach for Flaming in Social Networking Sites, Proceedings of the IEEE International Conference on Computational Intelligence and Communication Networks, 978-983, 2012.

A. Srivastava, A. Kundu, S. Sural, Credit Card Fraud Detection Using Hidden markov Model, *IEEE Transactions on Dependable and Secure Computing, 5*(1), 37-48, 2008.

24. Social Networking Sites, Proceedings of the IEEE International Conference on Computational Intelligence and Communication Networks, pp. 978-983, 2012.
25. Srivastava, A. Kundu, S. Sural, Credit Card Fraud Detection Using Hidden markov Model, *IEEE Transactions on dependable and Secure Computing, 5*(1), 37-48, 2008.