SPAMMER DETECTION AND FAKE USER IDENTIFICATION IN SOCIAL NETWORKS

K. Rambabu [1], A.Sai Sravani,

[1]**Assistant professor(HOD) , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- kattarambabudnr@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- sravanialapati4@gmail.com

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Face book have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased those results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content,

(ii) Spam based on URL, (iii) spam in trending topics, and (iv) fake users.

1 INTRODUCTION

It has become quite unpretentious to obtain any kind of information from any source across the world by using the Internet. The increased demand of social sites permits users to collect abundant amount of information and data about users. Huge volumes of data available on these sites also draw the attention of fake users [1]. Twitter has rapidly become an online source for acquiring real-time information about users. Twitter is an Online Social Network (OSN) where users can share anything and everything, such as news, opinions, and even their moods. Several arguments can be held over different topics, such as politics, current affairs, and important events. When a user tweets something, it is instantly conveyed to his/her followers, allowing them to outspread the received information at a much broader level [2]. With the evolution of OSNs, the need to study and analyze users' behaviors in online social platforms has intensity. Many people who do not have much information regarding the OSNs can easily be tricked by the fraudsters.

Literature Survey

Performing a literature survey on spammer detection and fake user identification in social networks involves reviewing existing research and studies on methods, techniques, and algorithms used to identify and mitigate spam and fake users. Here's a general approach and some key points to consider:

1. **DEFINE THE SCOPE**:

   Specify the types of social networks (e.g., Twitter, Face book, Instagram) and the types of spam/fake users (e.g., fake accounts, bots, malicious users).

2. **SEARCH STRATEGY:**

   Use academic databases (like Google Scholar, IEEE Xplore, ACM Digital Library) to search for relevant papers using keywords such as "spammer detection", "fake user identification", "social network analysis", "machine learning", and "data mining".

3 IMPLEMENTATION STUDY

Existing System:

Investigated issues of detecting spammers on Twitter. The proposed method combines characteristics withdrawal from text content and information of social networks. The authors used matrix factorization to determine the underline feature matrix or the tweets and then came up with a social regularization with interaction coefficient to teach the factorization of the underline matrix. Subsequently, the authors combined knowledge with social regularization and factorization matrix processes, and performed experiments on the real-world Twitter dataset, i.e., UDI Twitter dataset.

Disadvantages:

- There is no filtering system based on a preprocessing schedule and on Naïve Bayes algorithm to discard the tweets containing inaccurate information,.
- Less security due No URL Based Spam Detection.

Proposed System & alogirtham

In the proposed system, the system elaborates a classification of spammer detection techniques. The system shows the proposed taxonomy for identification of spammers on Twitter. The proposed taxonomy is categorized into four main classes, namely, (i) fake content; (ii) URL based spam detection, (iii) detecting spam in trending topics, and (iv) fake user identification. Each category of identification methods relies on a specific model, technique, and detection algorithm.

4.1 Advantages:

The average numbers of verified accounts that were either spam or non-spam and (ii) the number of followers of the user accounts.

The fake content propagation was identified through the metrics that include: (i) social reputation, (ii) global engagement, (iii) topic engagement, (iv) likability, and (v) credibility. After that, the authors utilized regression prediction model to ensure the overall impact of people who spread the fake content at that time and also to predict the fake content growth in future.

IMPLEMENTATION

MODULES:

ADMIN

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View and Authorize Users, Add and View Spam Filters ,View All User Posted Tweets, View All User Tweets Based On URLs,View Friend Request and Response, View All Tweets with Re-Tweets, View All Tweets , Re-Tweets and Comments, View All Spammers Detection, View All Fake User Identification, View Fake User Identification Results, View Fake Tweet Identification results

USER:

In this module, there are n numbers of users are present. User should register before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like My Profile, Search Friends ,Create Tweets, View My Friends, View Friend Requests, Search Tweets and Comment ,View My Tweets and Comments, View Friend's Retweets and Give Comments.

5 RESULTS AND DISCUSSION

SCREENSHOTS

5.3.1 HOMEPAGE:

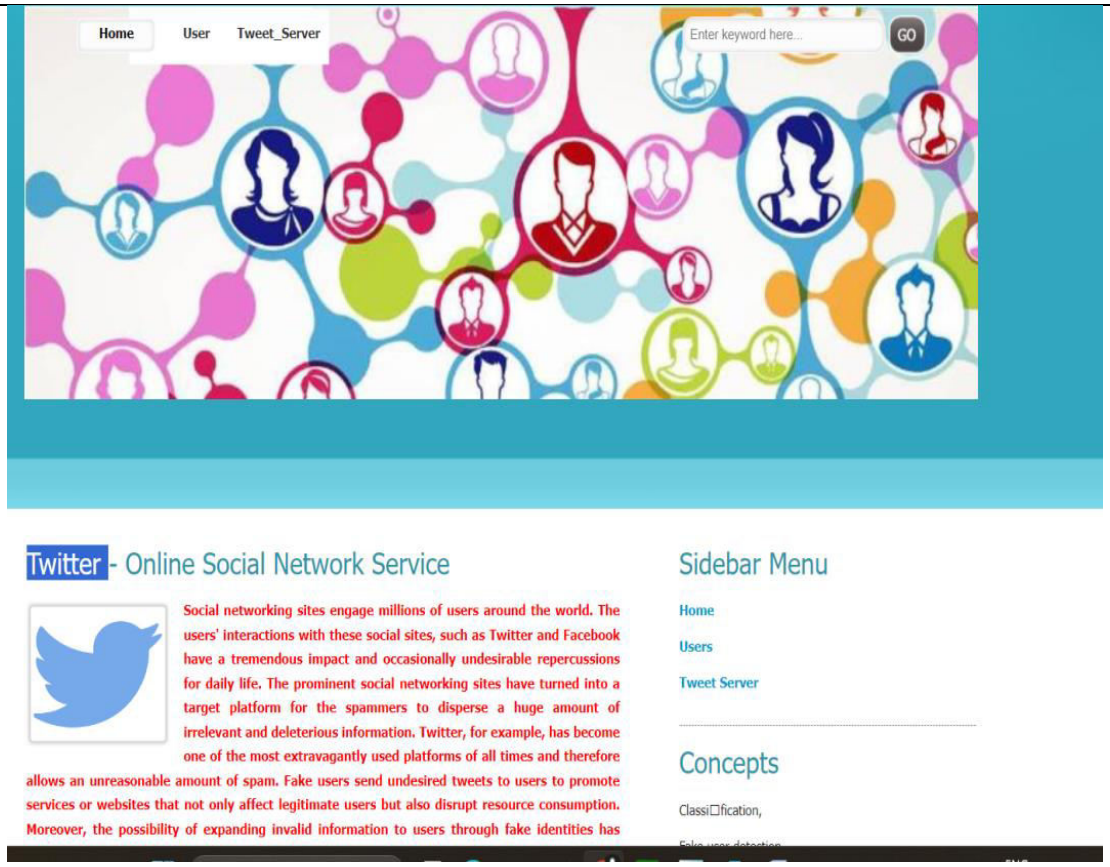


Figure 5.1 : Homepage

5.3.2 LOGIN PAGE:

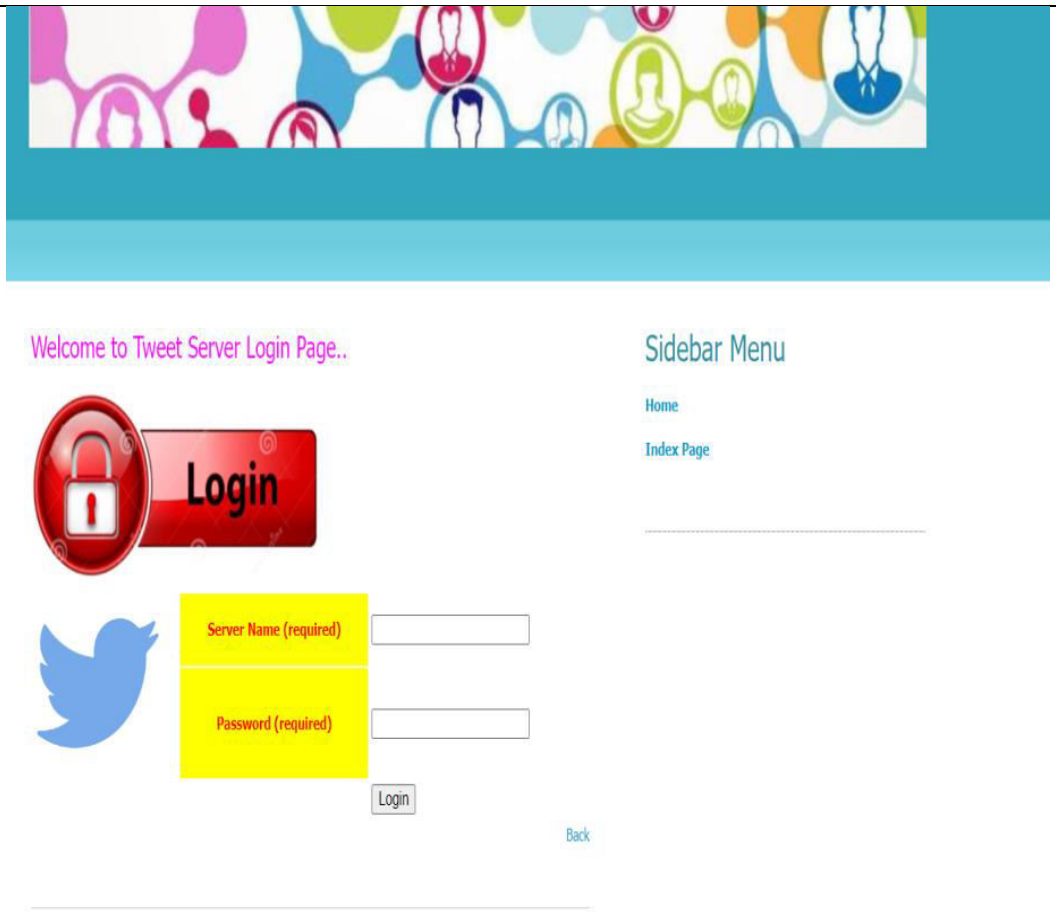


Figure 5.2: Login Page

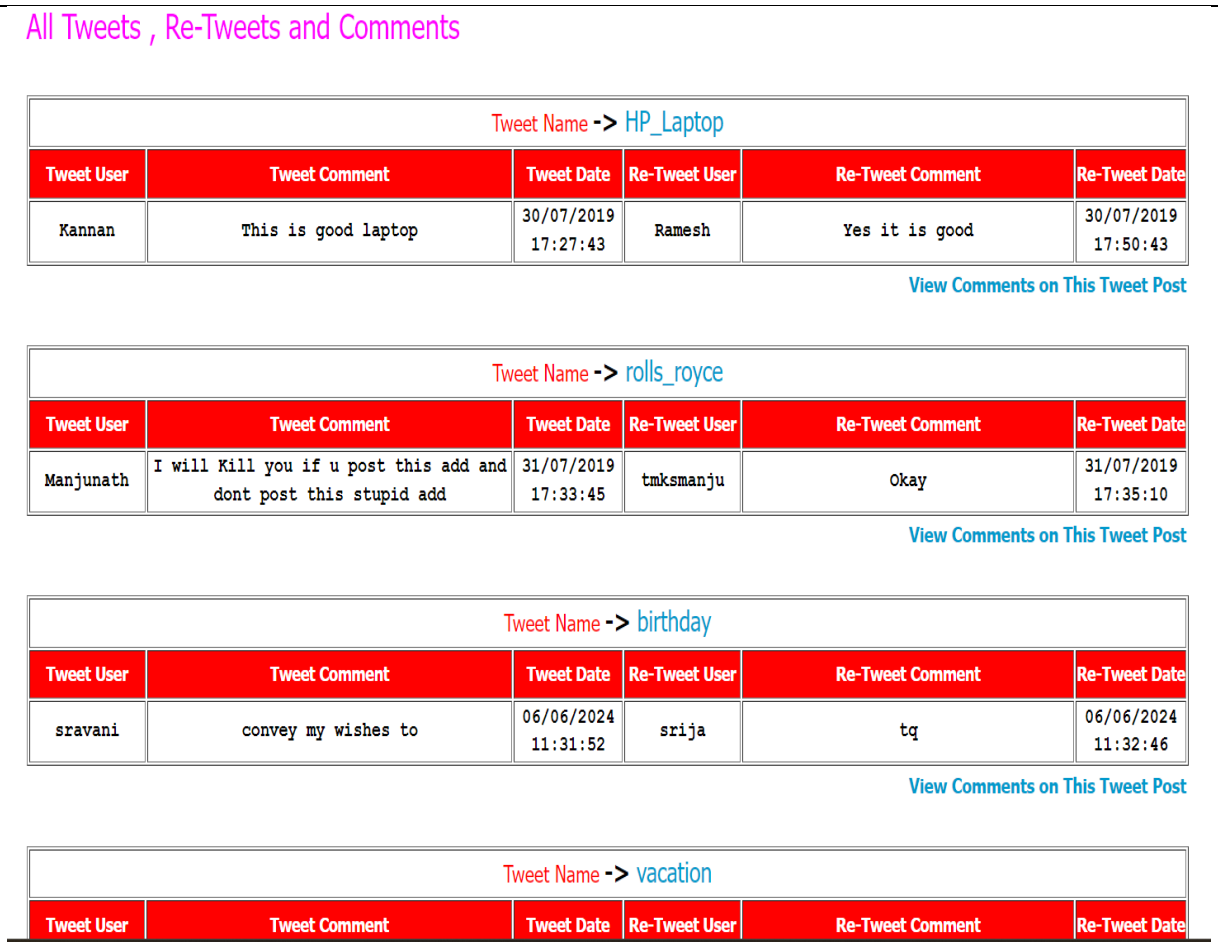
5.3.3 VIEW AUTHORIZE USERS DETECT ACCOUNT STATUS::

View and Authorize Users and Detect Account Status..

ID	User Image	User Name	Email	Mobile	Address	Status	Account Status
1		Kannan	Kannan.123@gmail.com	9535866270	#7827,4th Cross,Rajajinagar	Authorized	Normal
2		Ramesh	Ramesh.123@gmail.com	9535866270	#728,4th Cross,Rajajinagar,Bangalore	Authorized	Fake User

Figure 5.3: View Authorize Users Detect Account Status

5.3.4: ALL TWEETS,RE-TWEETS&COMMENTS


All Tweets , Re-Tweets and Comments

Tweet Name -> HP_Laptop

Tweet User	Tweet Comment	Tweet Date	Re-Tweet User	Re-Tweet Comment	Re-Tweet Date
Kannan	This is good laptop	30/07/2019 17:27:43	Ramesh	Yes it is good	30/07/2019 17:50:43

View Comments on This Tweet Post

Tweet Name -> rolls_royce

Tweet User	Tweet Comment	Tweet Date	Re-Tweet User	Re-Tweet Comment	Re-Tweet Date
Manjunath	I will Kill you if u post this add and dont post this stupid add	31/07/2019 17:33:45	tmksmanju	Okay	31/07/2019 17:35:10

View Comments on This Tweet Post

Tweet Name -> birthday

Tweet User	Tweet Comment	Tweet Date	Re-Tweet User	Re-Tweet Comment	Re-Tweet Date
sravani	convey my wishes to	06/06/2024 11:31:52	srija	tq	06/06/2024 11:32:46

View Comments on This Tweet Post

Tweet Name -> vacation

Tweet User	Tweet Comment	Tweet Date	Re-Tweet User	Re-Tweet Comment	Re-Tweet Date

Figure 5.4: All Tweets,Re-Tweets&Comments

5.3.5 ALL FRIEND REQUEST/RESPONSE

All Friend Requests/Response..

Id	Request From	Requested User	Request To	Request To Name	Status	Date
1		Kannan		Ramesh	Accepted	30/07/2019 17:03:36
2		Suresh		Kannan	Accepted	31/07/2019 12:09:44
3		Manjunath		Kannan	Accepted	31/07/2019 17:18:07
4		Manjunath		Uma	Accepted	31/07/2019 17:18:14
5		tmksmanju		Manjunath	Accepted	31/07/2019 17:29:17

Figure 5.5: All Friend request/Response

5.3.6 : VIEW FAKE USER IDENTIFICATION RESULTS

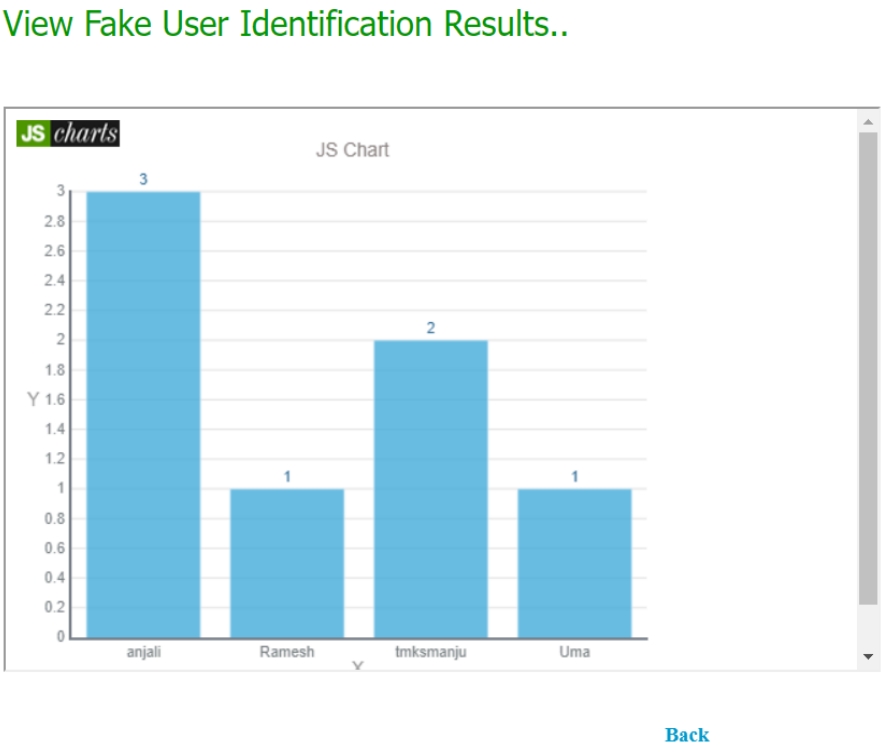


Figure 5.6: View Fake User Identification Results

5.3.7: ADD FILTER DETAILS

Figure 5.7: Add Filter Details

5.3.8 : ALL USER POSTED TWEETS

All User Posted Tweets..

ID	Tweet Image	Tweet Name	Tweet Description	Tweet Uses	Date	Posted By
11		football	ss	ss	26/05/2024 10:24:03	amar
14		election	polictics	election day	26/05/2024 11:20:35	anjali
7		cricket	india played very well	cricket	16/05/2024 11:14:01	dinesh
3		Dell_Laptop	Dell laptop is one of the best laptops which is manufactured by Dell Organization.	to know about dell laptop.	31/07/2019 12:06:02	Kannan
			world cup	won the match		

Figure 5.8: All User Posted Tweets

5.3.9 :VIEW FAKE USER IDENTIFICATION:

View Fake UserIdentification..

ID	User Name	Tweet Name	Purpose	Date and Time	Fake URL
1	Ramesh	HP_Laptop	Tried to Create Same Tweet Again	31/07/2019 13:35:23	http://localhost:9090/Spammer%20Detection%20and%20Fake%20User%20Identification%20on%20Social%20Networks/U_CreateTweetStatus.jsp
2	Uma	Sandesk_Pendrive	Tried to Create Same Tweet Again	31/07/2019 16:33:20	http://localhost:9090/Spammer%20Detection%20and%20Fake%20User%20Identification%20on%20Social%20Networks/U_CreateTweetStatus.jsp
3	tmksmanju	rolls_royce	Tried to Create Same Tweet Again	31/07/2019 17:36:08	http://localhost:9090/Spammer%20Detection%20and%20Fake%20User%20Identification%20on%20Social%20Networks/U_CreateTweetStatus.jsp
4	tmksmanju	rolls_royce	Tried to Create Same Tweet Again	31/07/2019 17:36:54	http://localhost:9090/Spammer%20Detection%20and%20Fake%20User%20Identification%20on%20Social%20Networks/U_CreateTweetStatus.jsp
5	anjali	election	Tried to Create Same Tweet Again	26/05/2024 11:20:37	http://localhost:8080/sravani/U_CreateTweetStatus.jsp
6	anjali	election	Tried to Create Same	26/05/2024	http://localhost:8080/sravani/U_CreateTweetStatus.jsp

Figure 5.9: View Fake User Identification

5.3.10: USER REGISTRATION

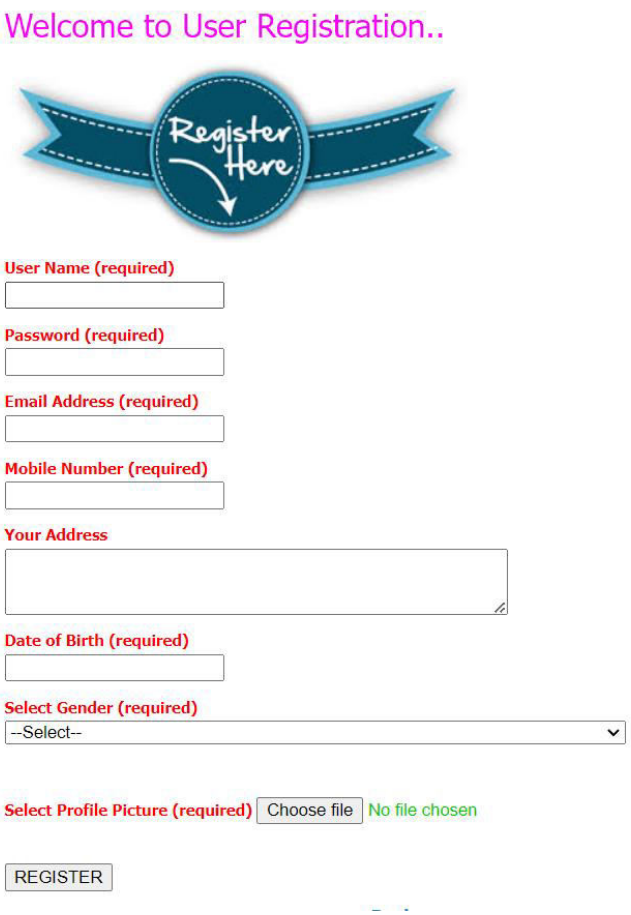


Figure 5.10: User Registration

5.3.11: USER'S PROFILE:

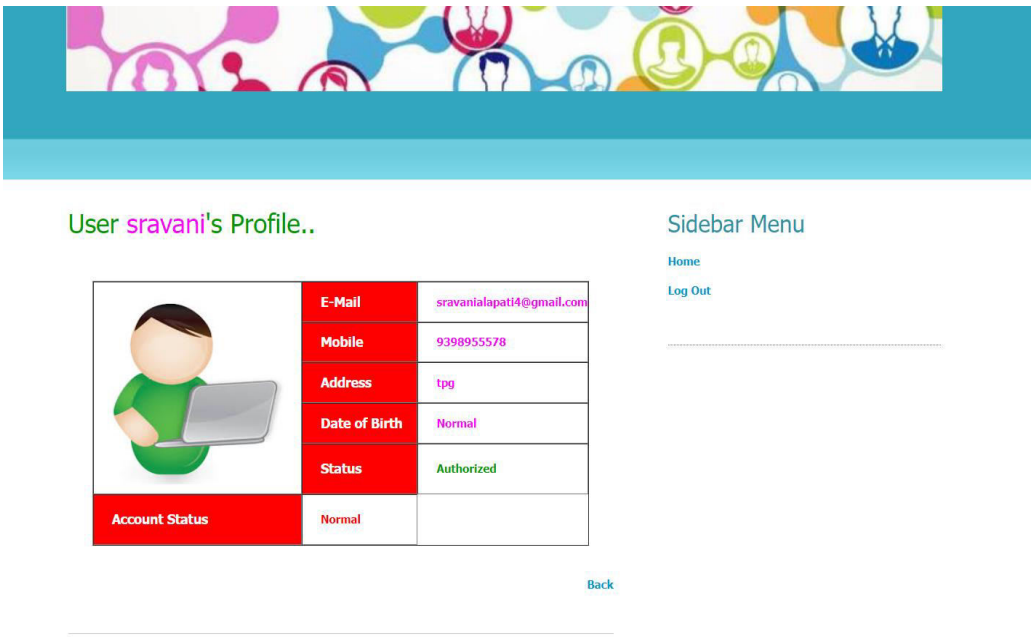


Figure 5.11: User's Profile

5.3.12 : SEARCH FRIENDS:

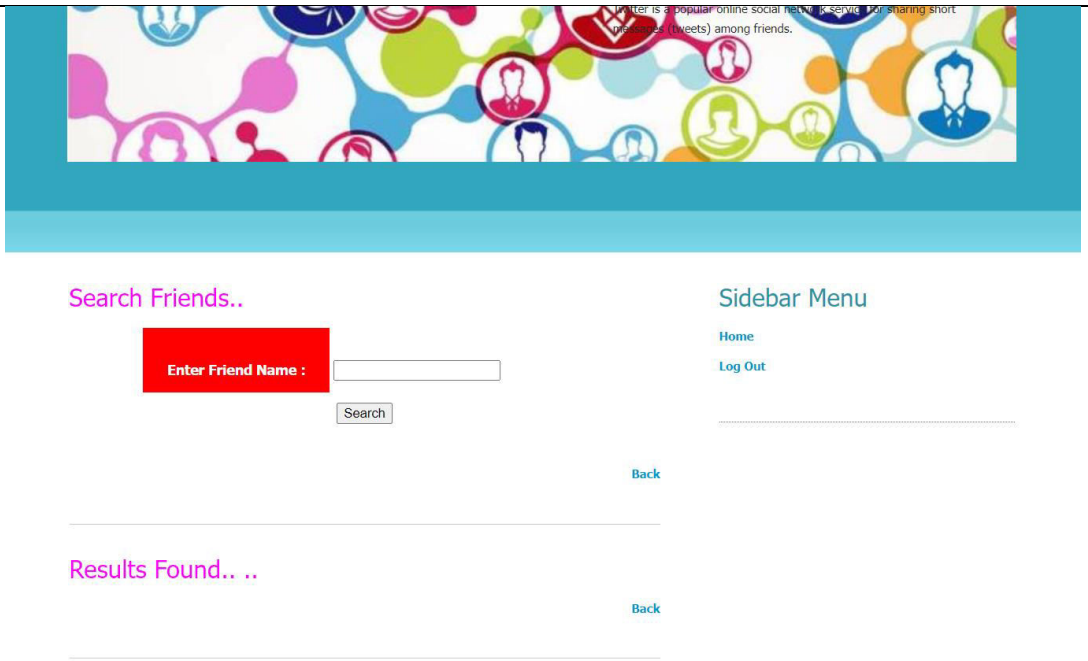


Figure 5.12: Search Friends

5.3.13 : POSTING TWEETS:

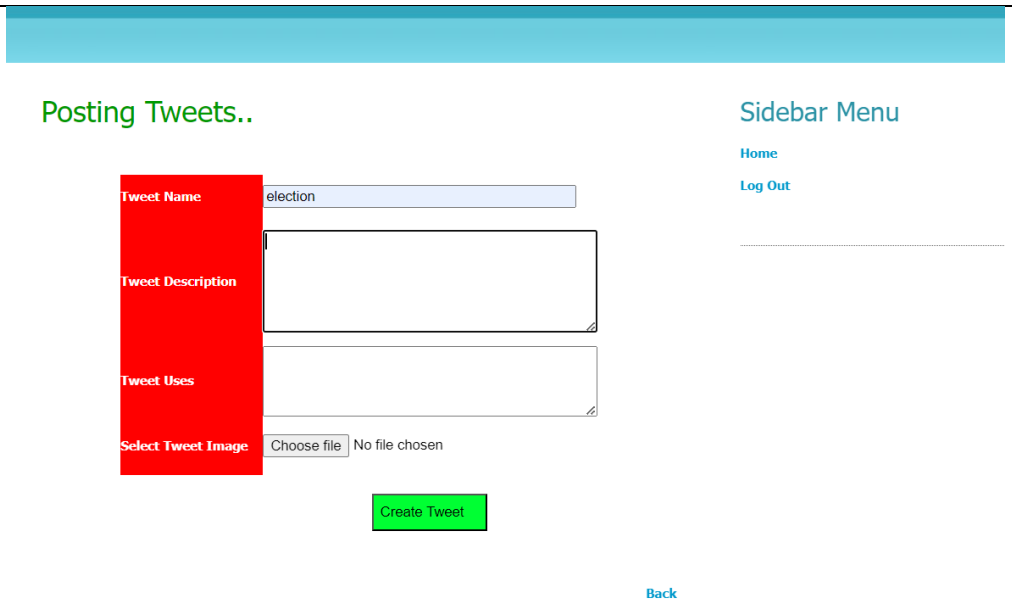


Figure 5.13: Posting Tweets

5.3.14 : USER FRIENDS

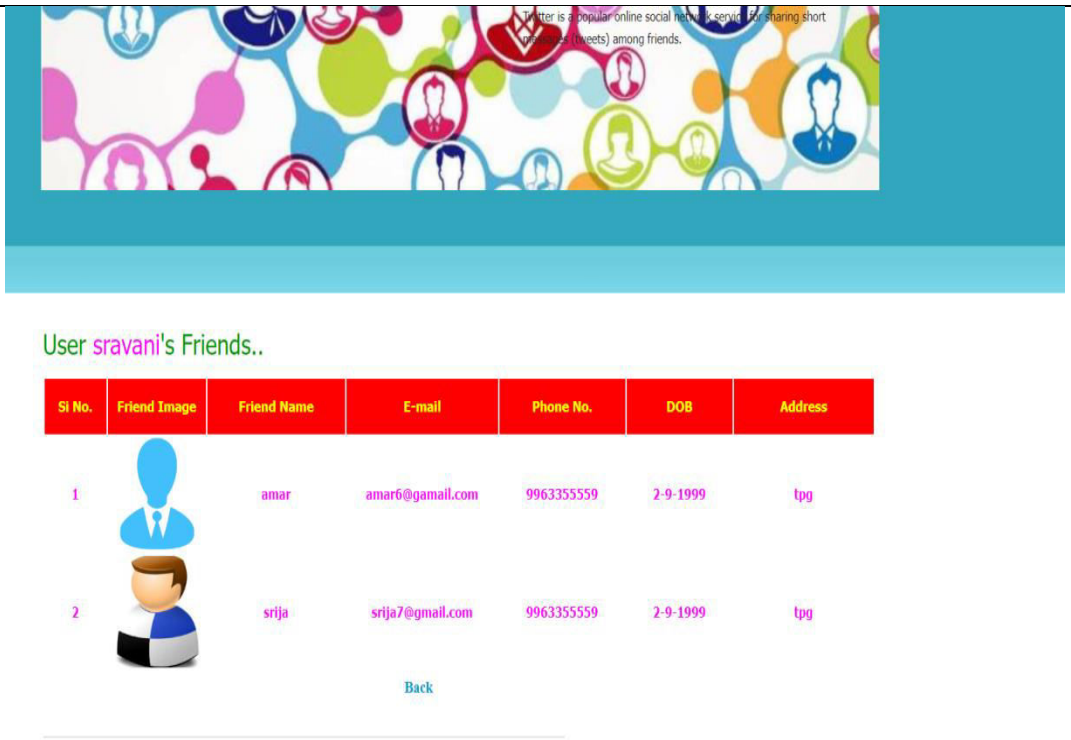


Figure 5.14: User Friends

5.3.15: FRIENDS REQUESTS TO USERS:

Friend Requests To sravani..

Username	E-mail	Mobile	Address	Gender	Status
srija	srija7@gmail.com	9963355559	tpg	FEMALE	Accepted

Figure 5.15: Friends Requests To Users

5.3.16: ALL MY POSTS TWEETS AND IT'S COMMENTS:

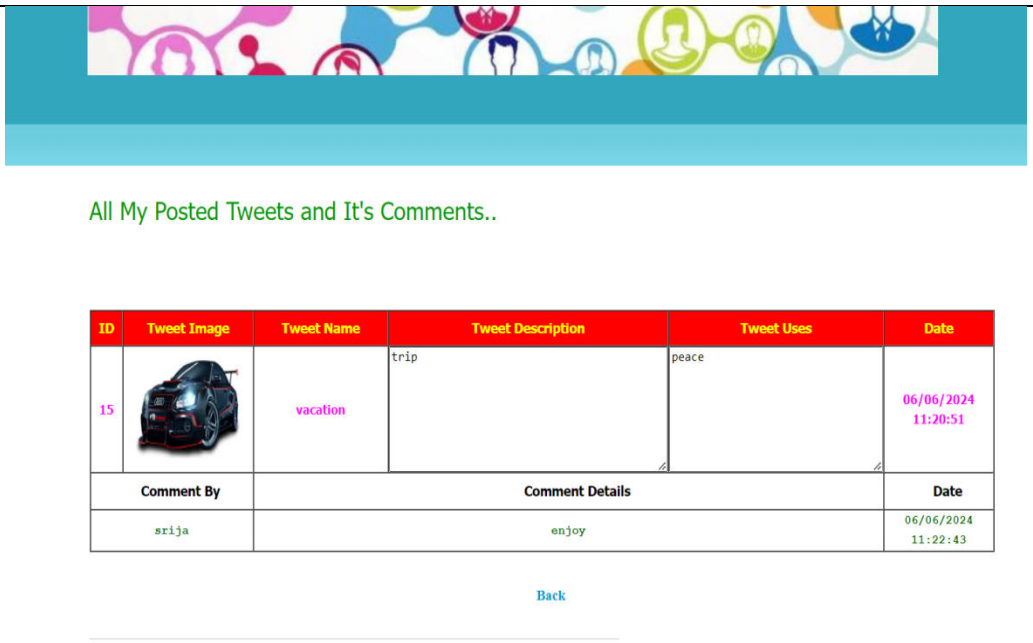


Figure 5.16: All My Posts Tweets and It's Comments

5.3.17 : RE-TWEETS-FRIENDS TWEETS:

Re-Tweet on Friends Tweets..

ID	Tweet Name	Retweeted Friend Name	Friend ReTweeted Details	Date	Re-Tweet
19	cricket	amar	nice	26/05/2024 11:11:29	Enter your comment here Post
18	computer	srija	nice srija	17/05/2024 15:32:41	Enter your comment here Post
22	vacation	srija	enjoy	06/06/2024 11:22:43	Enter your comment here Post

Back

Figure 5.17: Re-Tweets-Friends Tweets

5.3.18 : SEARCH TWEETS COMMENTS

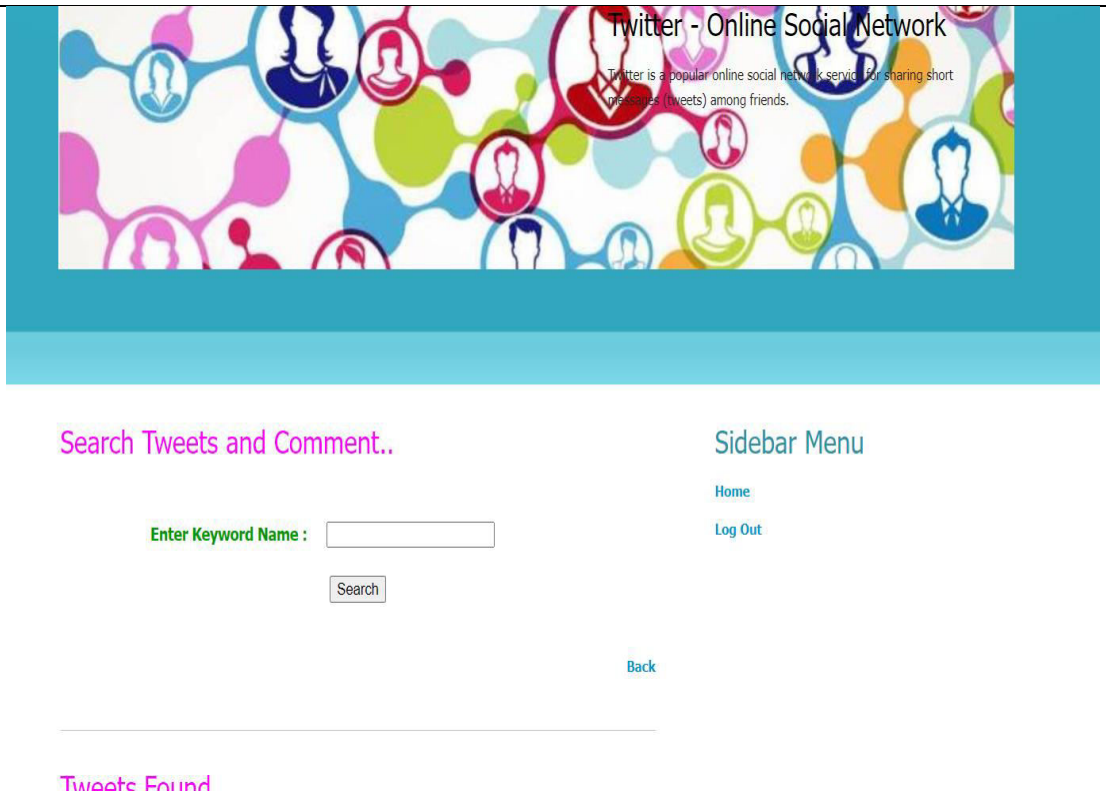


Figure 5.18: Search Tweets Comments

6. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper, we performed a review of techniques used for detecting spammers on Twitter. In addition, we also presented a taxonomy of Twitter spam detection approaches and categorized them as fake content detection, URL based spam detection, spam detection in trending topics, and fake user detection techniques. We also compared the presented techniques based on several features, such as user features, content features, graph features, structure features, and time features. Moreover, the techniques were also compared in terms of their specified goals and datasets used. It is anticipated that the presented review will help researchers find the information on state-of-the-art Twitter spam detection techniques in a consolidated form.

Despite the development of efficient and effective approaches for the spam detection and fake user identification on Twitter [34], there are still certain open areas that require considerable attention by the researchers. The issues are

briery highlighted as under: False news identification on social media networks is an issue that needs

to be explored because of the serious repercussions of such news at individual as well as collective level [25]. Another associated topic that is worth investigating is the identification of rumor sources on social media. Although a few studies based on statistical methods have already been conducted to detect the sources of rumors, more sophisticated approaches, e.g., social network based approaches, can be applied because of their proven effectiveness.

7. REFRENCES

[1] B. Erçahin, Ö. Akta³, D. Kilinç, and C. Akyol, ``Twitter fake account Detection," in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388392.

[2] F. Benevenuto, G. Magno, T. Rodriguez, and V. Almeida, ``Detecting Spammers on Twitter," in Proc. Collaboration, Electron. Messaging, Anti-Abuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12.

[3] S. Gharge, and M. Chavan, ``an integrated approach for malicious tweets Detection using NLP," in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 2017, pp. 435438.

[4] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ``Twitter spam detection: Survey Of new approaches and comparative study," Comput. Secure. vol. 76, pp. 265284, Jul. 2018.

[5] S. J. So man, ``A survey on behaviors exhibited by spammers in popular Social media networks," in Proc. Int. Conf. Circuit, Power Comput. Tech-nol. (ICCPCT), Mar. 2016, pp. 16.

[6] A. Gupta, H. Lamba, and P. Kumara guru, ``1.00 per RT #Boston Marathon # Prayforboston: Analyzing fake content on Twitter," in Proc. crime Researchers Summit (eCRS), 2013, pp. 112.

[7] F. Concone, A. De Paola, G. Lo Re, and M. Morana, ``Twitter analysis for real-time malware discovery," in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 16.

[8] N. Shari, M. Jalali, and M. H. Moat tar, ``Detecting spam tweets in Twitter using a data stream clustering algorithm," in Proc. Int. Conga. Technol., Commun. Knows. (ICTCK), Nov. 2015, pp. 347351.

[9] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, ``Statistical Features-based real-time detection of drifted Twitter spam," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914925, Apr. 2017.

[10] C. Buntain and J. Go beck, ``automatically identifying fake news in popular

Twitter threads," in Proc. IEEE Int. Conf. Smart Cloud (Smart Cloud),
Nov. 2017, pp. 208215.