Popularity Based Mechanism to Distinguish Malicious Posts in Facebook Social Network

Sanjeev Dhawan, Kulvinder Singh, Ekta

Faculty of Computer Science & Engineering, Student of M.Tech. (Software Engineering), Department of Computer Science & Engineering, University Institute of Engineering and Technology (U.I.E.T), Kurukshetra University, Kurukshetra (K.U.K)-136119, Haryana, INDIA.

Abstract: Social Networking sites are gaining much popularity in these days. Facebook is one of the most popular Social Networks. Facebook provides a platform where people can share their emotions with updating status and sharing pictures with their loved ones. People can make more and more friends and can exchange their views with them. Facebook also provides a platform for the companies and organizations to advertise their products or services. Celebrities also use Facebook to interact their fans and post their latest updates about the events or shows. With the increase of users in Facebook there are so many challenges arising day by day. Sometimes, users on Facebook may post unwanted posts or some harmful post on Facebook pages. In this paper, proposed a popularity based mechanism to distinguish malicious posts in Facebook. To implement this mechanism Facebook page dataset is collected using Netvizz. Netvizz is a Facebook application which is used to collect the data of user’s like page data, group data, liked pages data etc. gephi tool is used to visualize the dataset. This mechanism is implemented in java using NetBeans IDE platform to distinguish malicious posts in Facebook dataset. To distinguish the malicious posts different parameters are used like shares of posts, comments on posts and likes on posts.

Keywords: Facebook, Malicious post, Benign post, Netvizz , Gephi.

I. INTRODUCTION

Social Networks are the most popular platforms to communicate with friends, relatives and colleagues etc. Social Networks are also providing platform for the advertisements. Facebook is one of the most popular or simplest Social Network platforms. Celebrities are using Facebook by creating their pages to provide latest updates and upcoming events. Facebook pages are easiest and fastest medium to communicate with large amount of audiences. Posts and information of the pages are public and any Facebook user can access the information provided by the page. In page audiences can post their messages or photos on page’s wall. It gives opportunity to users to ask or send their messages direct to their favorite celebrities or person’s wall. But many times some users make unwanted or malicious post on page’s wall. Many researchers are doing their research to provide useful and helpful techniques to detect or prevent of these kinds of malicious posts and spam’s. To handle this type of issue different authors proposed various techniques like Web Defensio, Social Privacy Protector (SPP), Frappe etc. Web Defensio identified a post that is malicious or benign. This technique is used to monitor contents on users’ profile [1]. Social Privacy Protector is used to identify the fake accounts and also used to improve the security and the privacy of the user [2]. Frappe detects malicious applications based on some threshold value like popularity scores of application [3].

II. RELATED WORK

As Facebook social network is growing its users are increasing at higher rate and they producing huge amount of data in the form of messages, posts, sharing images etc so it is important to detect malicious post or malicious content in the Facebook social network. Therefore, many researchers are doing their research to provide useful and helpful solution to prevent Facebook users’ from malicious posts, malware content etc. In this way, Gao et al. [4] examined posts of 3.5 million Facebook users and determined that 10% of posts on Facebook wall were spam. Author also described a method to identify and distinguish spam campaigns. In a similar study, Grier et al. [5] examined post on twitter and found out 8% of links posted on Twitter were spam. Furthermore, a complete method that detects malicious content in Facebook was presented by Robertson et al. [6]. This method efficiently detects malicious web content. In another research, Thomas et al. [7] explained that the majority of balanced accounts in Twitter were produced by spammers as opposite to compromised users. Moreover Nimeh et al. [1] developed a Defensio technique which monitors post on users’ wall and determine...
whether they are malicious, spam or legitimate. This technique only identified URL post only. Similar to this technique Halim et al. [8] described the technique which detects people those were involved in malicious activities on Facebook. This technique had two stages. Firstly, semantic analysis was performed to categorize the malicious posts and secondly, spatiotemporal analysis was done and then compare between the friend graph and the spatiotemporal graph. Furthermore, Rahman et al. [9] developed a Facebook application that is MyPageKeeper which protects Facebook user from Socware and alert user when Socware come out on users’ wall. MyPageKeeper efficiently and accurately identify socware at low cost. In another work Rahman et al. [10] developed malware detection technique which identify malware content on Facebook. Author used SVM classifier to detect malicious content. Similarly, Maharaj et al. [11] collected real dataset from Facebook by using netvizz application and examined connection with different communities and visualized these connections by using Gephi tool. Subsequently, Prateek et al. [12] proposed an general feature set that detect malicious content on Facebook based on entity profile, textual content, metadata, and URL features in real time. This feature set achieved an accuracy of 86.9% to detect malicious web content. Moreover, Sanjeev and Ekta [13] compared different fake profile detection techniques with their pros and cons. In addition, Ekta and Sanjeev [14] classified Diabetes dataset for predicting how many people is infected from diabetes by using NaïveBayes classifier and Ranker algorithm. A part from this, Ekta et al. [15] collected real dataset from Facebook using netvizz application and visualized this dataset in Gephi tool and grouped different users’.

III. TOOLS USED

Gephi is used for the visualization of the data. Gephi is an open source tool which is freely available at www.gephi.org [16]. It can process complex data and give visualized results of the data. It comes with layouts for the visualization of the data like Force Atlas, Force Atlas 2 etc. Gephi can process different formats of Graph file like .gdf and .csv etc. To import dataset in Gephi tool Netviz application is used which is easily available on Facebook. With the help of Netviz user’s personal data, group data, liked pages data on Facebook can be downloaded easily. NetBeans IDE (Integrated Development Environment) is basically an open source software tool. It provides a GUI builder and programming environment. It is easy to use and helps to create Java applications. It also gives built-in support for developing in Java, C, C++, XML, and HTML [17].

IV. PROPOSED MECHANISM

Collect the real dataset and compute table having the information of the posts like shares, comments and likes. Now calculate the popularity of each post using the formula on the basis of likes, shares and comments parameters.

Formula for calculating popularity index of the posts: \( \frac{\text{Likes} + \text{Shares}}{\text{Comments}} \).

![Fig. 1: Flowchart of Proposed Mechanism](image-url)
After calculating the popularity for each post then provides a threshold to determine the malicious or benign posts. If popularity of posts is greater than the provided threshold value then it will be benign post. If the popularity of the posts is less than the threshold value then post will be consider as malicious post.

V. ANALYSIS AND RESULTS

Facebook page dataset is collected by using Netvizz application in Facebook. By using Netvizz user’s personal data, group data, page data, like pages data etc. can be downloaded easily. All the posts from the celebrity page are extracted into the dataset. The dataset downloaded is in GDF file format then visualized and analyzed. This dataset contains name of post, number of likes on posts, number of comments on posts, and number of shares of post.

Fig. 2: Visualization of Facebook Dataset in Gephi collected by Netwizz

Fig. 2 shows the visualization of real dataset after importing in Gephi. To visualize and distinguish malicious posts dataset was collected using Netvizz Facebook application. In this there posts are represented using different colours.

A. Graph Distance report

The average graph-distance between all pairs of nodes. Connected nodes have graph distance 1. The diameter is the longest graph-distance between any two nodes in the network.

| Diameter: 6 |
| Radius: 0 |
| Average Path length: 3.354466568431128 |
| Number of shortest paths: 158802 |

A.1 Betweenness Centrality Distribution

Measure how often a node appears on shortest paths between nodes in the network.

![Betweenness Centrality Distribution](image)

Fig. 3: Depicts Betweenness Centrality Distribution
B. Modularity Report

Modularity algorithm is community detection algorithm and finds those nodes are connected closely than other nodes in the network.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomize</td>
<td>On</td>
</tr>
<tr>
<td>Use edge weights</td>
<td>On</td>
</tr>
<tr>
<td>Resolution</td>
<td>1.0</td>
</tr>
<tr>
<td>Number of Communities</td>
<td>14</td>
</tr>
</tbody>
</table>

D. Input

Facebook dataset downloaded from Netvizz and convert it into the CSV format.

![Input dataset of Facebook](image)

E. Output

This output file contains popularity which is calculated by likes, comments and shares. On the basis of their popularity distinguish posts into classes called benign and malicious.
VI. CONCLUSION AND FUTURE WORK

Facebook is gaining more popularity day by day. Facebook is also providing platform for the celebrities and organizations to communicate with their audiences. Celebrities and create pages for their audiences to update...
their latest updates. These pages are public where page can post as well as users can post their views or their messages on page’s wall. Sometimes user can post unwanted contents or malicious content on page’s wall by mistake or intentionally. These malicious posts should be detected to provide healthy communication between user and their liked pages. In this paper popularity based mechanism is proposed to distinguish malicious posts. Facebook page dataset is downloaded and visualized using Gephi tool. Different parameters are used to calculate the popularity of the posts like shares of post, likes on post, and comments on post in proposed mechanism. This proposed mechanism is implemented in Java using Netbeans. And then results are visualized in Gephi tool. This proposed mechanism distinguished the malicious posts and benign posts from the dataset. In Results 87% posts are distinguished as benign posts and rest are malicious posts. In future more efficient technique will be proposed by using clustering.

VII. REFERENCES


