INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Node Tracking on Dynamic Social Network using Greedy approach

Ketaki Date, Anshuman Rao, Shailesh Shelar, Shubham Shirke, Prof. Vikas Nandgaonkar

BE Students, Department of Computer Engineering, PCET'S NMIET, Maharashtra, India

Assistant Professor, Department of Computer Engineering, PCET'S NMIET, Maharashtra, India

ABSTRACT: A social network site plays a very important role in spreading information and influencing the whole world. A Set of influencers has to be found on social media and they must be targeted first. The spread of influence will be increased but finding out the utmost influential nodes in the network is the main problem. There is an Algorithm used which is called as Greedy algorithm and that is used for mining top-K influential nodes. It is divided into two components: dividing the post of the social network into different states by taking into account information that has spread and selecting states to find influential nodes by dynamic programming.

One more serious problem in the social network is that there are so many malicious attacks spread by the people and that malicious contents are hidden behind some attractive posts i.e. viral marketing techniques in the promotion of new products or posts like how much luckiest you are today or what does your name mean or post which states to give you iPhone in a lesser prize or giving them free samples of the product etc. such posts on the social network may be harmful to users which have the negative intention of stealing the personal information from the user. So attackers take an advantage of such usage history of ads i.e. rating of such posts. The system analyses those product's impact on social media users and predicts the positive or negative category for that posts which is beneficial for future users on social media. So we need to find out those posts and block them.

KEYWORDS: Influential Node Tracking, Malicious Posts, Greedy algorithm.

I. INTRODUCTION

Today's Social Networks are becoming fast and dynamic platforms for sharing posts as well as it has become a globalized market for the advertisement of products.Social Media is used by millions of users all over the world, but there are some posts on the social networks that may be harmful to users which have a negative intention of stealing personal information user. So we have to protect the users from such type of Harmful Post as well as we need to find out Owner of this post. Viral marketing techniques in the promotion of new products or posts like how much luckiest you are today or what does your name mean or post which states that giving you iPad in a less prize or promising them to give free samples of products to use. Such posts in a social network may be harmful to users which has the negative intention of stealing the personal information user. So they take advantage of such usage history of ads i.e. rating of such posts the system analyses that product's impact on social media users and predicts the positive or negative category for that posts which is beneficial for future users on social media.

II. PROBLEM STATEMENT

To implement a novel problem, namely Influential Node Tracking problem on the social network, as an extension of Influence Maximization problem to dynamic networks by means of post or ads, which aims at tracking a set of influential nodes dynamically such that the influence spread is maximized at any moment it may be positive or negative by taking reviews. Online social networks are extensively used for communication. Users can share information with friends, but there are some people on the social network who misuse the features of these social platforms and spread malicious content. They do this by uploading the malicious post to other user page. These contents spread at a fast rate. No, any mechanism has been invented to detect malicious posts immediately and remove them.

III. PURPOSE

Here we are developing a system of efficient categorization technique for identifying whether a post generated by a third party application is malicious or not. Now detecting malicious URLs has become an essential task in network security intelligence. To maintain efficiency of web security, these malicious URLs have to be detected, identified as well as their corresponding links should be found out. Hence users get protected from it and effectiveness of network security gets increased. Any content which they want to spread can be uploaded i.e. malicious posts on social media. The data that contains malicious content is posted to other user's wall in different form. If the user clicks on the posts, it will take him to another page. The post is made interesting, so that the users get attracted to it. This can be adult content or free downloading sites. So it needs software that can identify and block that malicious content directly.

IV. PROPOSED SYSTEM

In this section, we are going to provide a brief introduction about today's Social Networks are becoming fast and dynamicplatforms for sharing post as well as it has become a globalized market for the advertisement of products. Social Media is used by millions of users all over the world. But there are some posts in a social network may be harmful to users which has negative intention of stealing personal information from user. So we have to protect users from such type of Harmful Post as well as we need to find out Owner of this post. Viral marketing techniques like promotion of new products or how much lucky you are today or the meaning of our name or post which states to give you any electronic item like mobile in a lesser prize or giving them free samples of the product's etc. so these posts in social network can cause harm to users those may steal personal information of user. So attackers take an advantage of such history of ads i.e. rating of such posts the system analyses the that products impact on social media users and predicts the positive or negative category for that posts which is beneficial for future users on social media. The system which will be developed will identify whether the post is malicious or its safe. Detection of malicious posts or ads has now become a necessary task for the purpose of network security. To maintain efficiency of web security, these malicious URLs have to be detected, identified as well as their corresponding links should be found out. Hence due to thisusers get alerted and protected from it and the effectiveness of network security gets increased. The malicious users can upload malicious posts on social media. The content that contains malicious data is posted to other user's walls under a different form. The user mistakes the posts for real content and clicks the post, which will take him to another page. Hence the malicious users get benefit from the user's mistake. In order to get the attention of the user, the malicious user will include keywords or descriptions of pages that will be of interest to the user. These can be any ad or sites that allowed free downloading. So we need some method or a system which bans such activity just by identifying it.
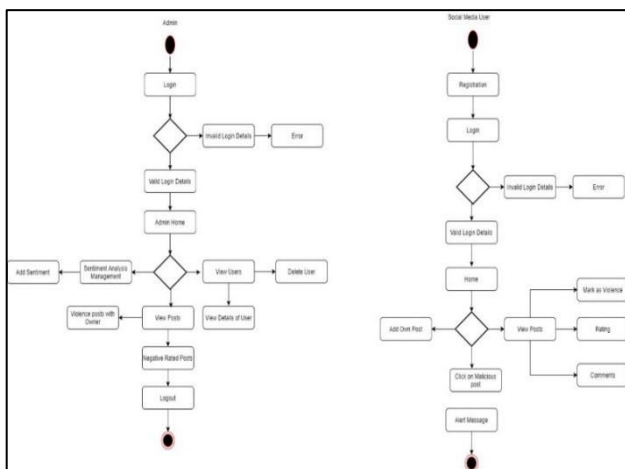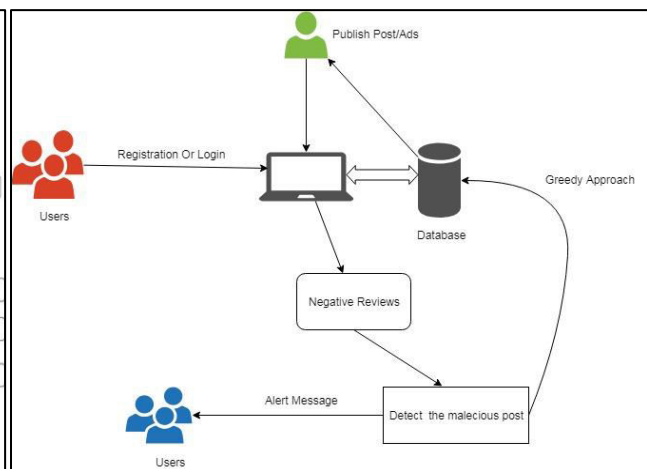

Fig.1.Use case diagram

Fig. 2. Architecture Diagram

V. CONCLUSION AND FUTURE WORK

The technology has many advantages in today's world. It has influenced behavior of humans and social interactions. The main idea of this system is to develop a project that detects malicious posts, ads, comments and also the profile of user that is trying to spread negativity. Our main focus is to breakdown each post in terms and differentiate them automatically to the terms that are already termed as suspicious which are already present in our database by using the method of similarity distance calculation. Hence malicious activities and fraud activities will get reduced.

In future we plan to develop the system which can do automatic classification and increase execution time of the system. We will use some more resources and knowledge to improve precision rates, the semantic of exchanged information will be used to identify more suspicious profiles of people who are trying to spread negativity, post fraud ads and carry out malicious activities.

REFERENCES

1. W. Chen, Y. Wang and, S. Yang, Efficient influence maximization in social network,in KDD, 2009, pp. 199208.
2. P. Domingosand M. Richardson, Mining the network value of customers, in KDD,2001, pp. 5766.
3. SD. Kempe, J. Kleinberg, and, E. TardosMaximizing the spread of inffluence througha social network, in KDD, 2003, pp. 137146.
4. M. Kimura and K. Saito, Tractable models for information diffusion in social networks,in PKDD, 2006, pp. 259271.
5. W.Yu, G.Cong, G.Song, and K.Xie, Community-based greedy algorithm for miningtop-k influential nodes in mobile social networks, in KDD, 2010, pp. 10391048.
6. W.Chen, C.Wang, and Y.Wang, Scalable influence maximization for prevalent viralmarketing in large-scale social networks, in KDD, 2010, pp. 10291038.
7. W. Chen,W. Lu, and N. Zhang, Time-critical influence maximization in social networkswith time-delayed diffusion process, in AAAI, 2012.
8. W. Chen, Y. Yuan, and L. Zhang, Scalable influence maximization in social networksunder the linear threshold model, in Data Mining (ICDM), 2010 IEEE 10th International Conference on. IEEE, 2010, pp. 8897.

INTERNATIONAL JOURNAL
OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING