# SECURE SOCIAL NETWORK: INFLUENTIAL NODE TRACKING USING GREEDY APPROACH ALGORITHM

AkshayDhumal, Prashant Bhosale, Ajay Jogdand, Aniket Mahajan, Dr. Brijendra Gupta
Siddhant Collegeof Engineering, Sudumbare,Pune

**Abstract:** -As each social network structure and strength of influence between people evolve constantly, it needs to trace the cogent nodes beneath a dynamic setting. To address this downside, The System explore the cogent Node trailing (INT) downside as AN extension to the standard Influence Maximization downside (IM) beneath dynamic social networks. Whereas Influence Maximization downside aims at characteristic a set of k nodes to maximize the joint influence beneath one node or user. INT downside focuses on trailing a group of cogent nodes that keeps maximizing the influence because the network evolves by means that of posts or ads. Utilizing the smoothness of the evolution of the network structure, The System propose AN economical algorithmic rule, edge Interchange Greedy (UBI) and a variant, UBI+. Rather than constructing the seed set from the bottom, this begin from the cogent seed set system realize antecedently and implement node replacement to boost the influence coverage. What is more, the system conjointly focuses on detection of posts for his or her positive or negative views by analyzing the usage history of that posts or ads or product.

**Keyword:**-Social Networks, Community Detection, Influence Maximization.

**Introduction:** -A social network, the graph of relationships and interactions among a bunch of people, plays an elementary role as a medium for the unfold of data, ideas, and influence among its members. Models for the processes by that concepts and influence propagate through a social network are studied during a range of domains, including the diffusion of medical and technological innovations, the sudden and widespread adoption of assorted ways in game-theoretic settings, and the effects of word of mouth i.e. microorganism promoting techniques within the promotion of recent products or posts like what proportion luckiest nowadays or what will your name meant or post that states the supplying you with iPad in lesser prize or giving them free samples of the product etc. such posts in social network could also be harmful to users that has the negative intention of stealing the private info user. That the takes the advantage of such usage 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 class for that posts that is helpful for future users on social media. Social network sites like Facebook, Twitter, and Google+ are experiencing unimaginable growth in users. There are over 1,000,000 users as of currently. Besides simply making a profile and linking with friends, the social networks are currently building platforms to run their web site. These platforms are engineered supported the user profile details. These social applications are shortly changing into Associate in nursing example of on-line communication that makes use of the user's personal info and activities in social links for numerous services. The Social networks are fashionable suggests that of communication among the web users. On-line Social Networks (OSNs) witness an increase in user activity whenever an event takes place. Malicious entities exploit this spur in user-engagement levels to spread malicious content that compromises system name and degrades user expertise and has recently been according to face a lot of abuse through scams and different type of malicious content, particularly throughout news creating events. Individuals are heavily relaying on on-line interactions. the web is giving completely different choices to make and maintain contacts

and relations for the user. With the introduction of social media network these choices became even easier to be used. Because of this serious use of social media network a particular cluster of web users referred to as cybercriminal create use of this chance for threads. Cybercriminals use completely different suggests that to make spams fraud and different attacks on the users. Another suggests that of attack by cybercriminals is the misuse of videos, pictures and links showed by the user. Attackers transfer malicious posts within the season of special events and disasters. They're going to transfer malicious posts that are associated with these events and misguide users to click those links. Users UN agency click the links by mistake act as Associate in Nursing someone to the assaulter as a result of the malicious posts would mechanically re- posts the malicious contents like links, images or videos on the user profile. Another fashionable version of this attack ends up in user profiles to "like" a Facebook page while not their data. In some cases the, spammed posts can lead the users to survey sites which can lead to cyber criminals getting profit. Finally, a true world resolution within the style of a REST based mostly API and a browser plug-in to spot malicious Facebook application and posts in real time i.e. FraAppe and My Page Keepe. Once a Facebook user installs.

**Literature Survey:-**

**Paper1:-** Community-based greedy algorithm for mining top-k influential nodes in mobile social networks.

**Authors:** W.Yu, G.Cong, G.Song, and K.Xie.

**Description: -** With the proliferation of mobile devices and wireless technologies, mobile social network systems are increasingly available. A mobile social network plays an essential role as the spread of information and influence in the form of "word-of-mouth". It is a fundamental issue to find a subset of influential individual sin a mobile social network such that targeting them initially (e.g. to adopt a new product) will maximize the spread of the influence (further adoptions of the new product). The problem of finding the most influential nodes is unfortunately NP-hard. It has been shown that a Greedy algorithm with provable approximation guarantees can give good approximation; However, it is computationally expensive, if not prohibitive, to run the greedy algorithm on a large mobile network. In this paper system propose a new algorithm called community based Greedy algorithm for mining top-K influential nodes. The proposed algorithm encompasses two components: 1) an algorithm for detecting communities in a social network by taking into account information diffusion; and 2) a dynamic programming algorithm for selecting communities to find influential nodes. We also provide provable approximation guarantees for our algorithm. Empirical studies on a large real-world mobile social network show that our algorithm is more than an order of magnitudes faster than the state-of-the-art Greedy algorithm for finding top-K influential nodes and the error of our approximate algorithm is small.

**Paper2:-**Salable influence maximization in social networks under the linear threshold
Model.

**Authors:** W. Chen, Y. Yuan, and L. Zhang.

**Description:** Influence maximization, defined by Kempe, Kleinberg, and Tardos, is the problem of finding a small set of seed nodes in a social network that maximizes the spread of influence under certain influence cascade models. The scalability of influence maximization is a key factor for enabling prevalent viral marketing in large scale online social networks. Prior solutions, such as the greedy algorithm of Kempe et al. (2003) and its improvements are slow and not scalable, while other heuristic algorithms do not provide consistently good performance on influence spreads. In this paper, system design a new heuristic algorithm that is easily scalable to millions of nodes and edges in our experiments. Our algorithm has a simple tunable parameter for users to control the balance between the running time and the influence spread of the algorithm. Our results from extensive simulations on several real-world and synthetic networks demonstrate that our algorithm is currently the best scalable

solution to the influence maximization problem: (a) our algorithm scales beyond million-sized graphs where the greedy algorithm becomes infeasible, and (b) in all size ranges, our algorithm performs consistently well in influence spread it is always among the best algorithms, and in most cases it significantly outperforms all other scalable heuristics to as much as 100increase in influence spread.

**Paper3:- Simulated** Annealing Based Influence Maximization in Social Networks.

Authors: Qingye Jiang, Guojie Song,Gao Cong, YuWang,Wenjun Si,Kunqing Xie

Description: The problem of influence maximization, i.e., mining top-k influential nodes from a social network such that the spread of influence in the network is maximized, is NP-hard. Most of the existing algorithms for the problem are based on greedy algorithm. Although greedy algorithm can achieve a good approximation, it is computational expensive. In this paper, system propose a totally different approach based on Simulated Annealing (SA) for the influence maximization problem. This is the first SA based algorithm for the problem. Additionally, system propose two heuristic methods to accelerate the convergence process of SA, and a new method of computing influence to speed up the proposed algorithm. Experimental results on four real networks show that the proposed algorithms run faster than the state-of-the-art greedy algorithm by 2-3 orders of magnitude while being able to improve the accuracy of greedy algorithm.

**Paper4:-**Irie: Scalable and robust influence maximization in social networks.

**Authors:** K. Jung, W. Heo, and W. Chen.

Description:- Influence maximization is the problem of selecting top k seed nodes in a social network to maximize their influence coverage under certain influence diffusion models. In this paper, system propose a novel algorithm IRIE that integrates the advantages of influence ranking (IR) and influence estimation (IE) methods for influence maximization in both the independent cascade (IC) model and its extension IC-N that incorporates negative opinion propagations.

Through extensive experiments, system demonstrate that IRIE matches the influence coverage of other algorithms while scales much better than all other algorithms. Moreover IRIE is much more robust and stable than other algorithms both in running time and memory usage for various density of networks and cascade size. It runs up to two orders of magnitude faster than other state of theart algorithms such as PMIA for large networks with tens of millions of nodes and edges, while using only a fraction of memory.

**Paper5:-**Graph evolution: Densification and shrinking diameters.

**Author:-**Jure Leskovec, Jon Kleinberg, Christos Faloutsos.

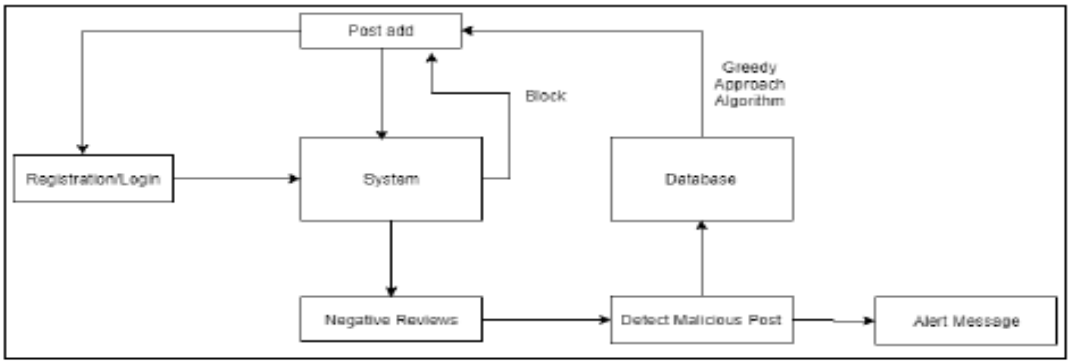
**Description:-**How do real graphs evolve over time? What are “normal” growth patterns in social, technological, and information networks? Many studies have discovered patterns in static graphs, identifying properties in a single snapshot of a large network, or in a very small number of snapshots; these include heavy tails for in- and out-degree distributions, communities, small-world phenomena, and others. However, given the lack of information about network evolution over long periods, it has been hard to convert these findings into statements about trends over time. Here we study a wide range of real graphs, and we observe some surprising phenomena. First, most of these graphs density over time, with the number of edges growing super-linearly in the number of nodes. Second, the average distance between nodes often shrinks over time, in contrast to the conventional wisdom that such distance parameters should increase slowly as a function of the number of nodes (like O(log n) or O(log(log n)). Existing graph generation models do not exhibit these types of behavior, even at a qualitative level. We provide a new graph generator, based on a “forest fire” spreading process, that has a simple, intuitive justification, requires very few parameters (like the “flammability” of nodes), and produces graphs exhibiting the full range of properties observed both in prior work and in the present study. We also notice that the “forest fire” model exhibits a sharp transition between sparse graphs and graphs

that are deifying. Graphs with decreasing distance between the nodes are generated around this transition point. Last, we analyze the connection between the temporal evolution of the degree distribution and densification of a graph. We find that the two are fundamentally related. We also observe that real networks exhibit this type of relation between densification and the degree distribution.

**Proposed System:-**

In this work system goes to develop a system of economical categorization technique for characteristic whether or not a post generated by a 3rd party application is malicious or not. Police investigation malicious URLs is currently a vital task in network counterintelligence. To take care of potency of net security, these malicious URLs ought to be detected, known additionally as their corresponding links ought to be discovered.

**Architecture**:-




**Math module:-**

Let W be the set of whole system which consists of the input, process and output of the system.

W = input, process, output.

Where, input = is the set of inputs given to the system to achieve the problem statement.

Process = is the procedure or the algorithm applied to the system which gives the expected output.

Output = is the output of the system

Input = S, U, A, R, P, N, Avg.

Therefore users get shielded from it and effectiveness

Of network security gets accrued. The malicious users will transfer a content he needs to unfold i.e. malicious posts on social media. The content that contains malicious information is denote to alternative users wall beneath a special type. The user mistakes the posts for a true content and clicks the post, which is able to take him to a different page. Therefore the malicious user will have the benefit of this method. In order to urge the eye of the user, the malicious user can embody keywords or description of pages that may be of interest to the user. These are often adult content or free downloading sites. Thus it wants a method that illegal such associate in Nursing activity by simply characteristic and obstruction that malicious content directly.

Let,

1. S = be the social media system like Facebook.

2. U = be the set of users on social media.

U = u1, u2, u3,. .. . . . . ..un.

3. A = be the set of ads or post on social media.

A = a1, a2, a3, . . . .. . . .an.

4. R = ratings given to ad A by user U

R = r1, r2, r3, . .. . . . .. .rn.

5. P be the positive category of ads .

SCOE, Department of Computer Engineering 2019 4

6. N be the negative category of ads.

7. Avg is the average calculated by usage history particular ad A

Step 1. User 'Ui' will registered to 'S'.

Step 2. User 'Ui' will see the post of ads 'Ai' on this timeline.

Step 3. User will give rating 'Ri' (rating are like 1 to 5 points).

Depending on the usage history of particular ad 'Ai' by users system will apply the efficient algorithm to detect the influence and the category of that ad.

Here, the category may be P or N which is calculated by average of particular app being used by users.

Avg = (sum of R ) / total number of that ads users

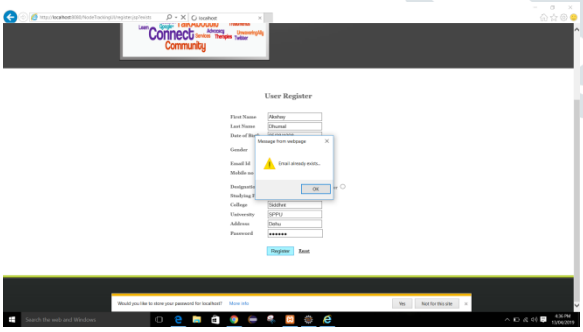
If avg Avg is greater than threshold average value then that ad post is considered as positive category elseit is negative.

Step 4. As per Negative Rating System will notify to new user. i.e. Alert about malicious Post.

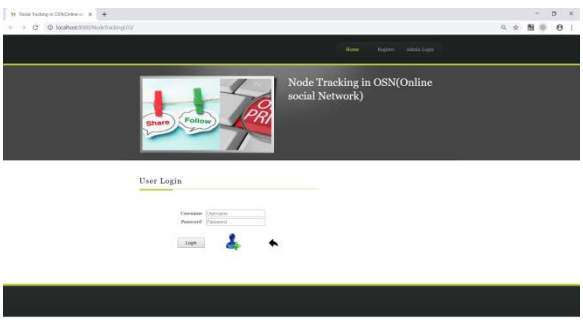
Step 5. System will Block that Post.

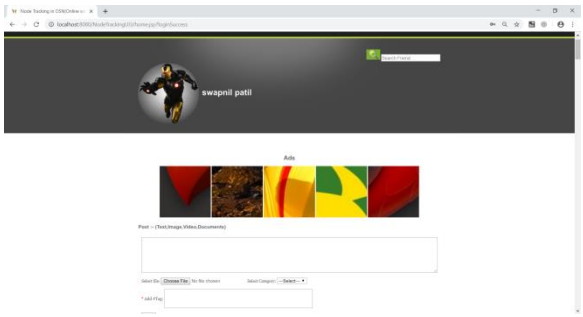
**Result:**

1. **User Registration**




2. **User Login**

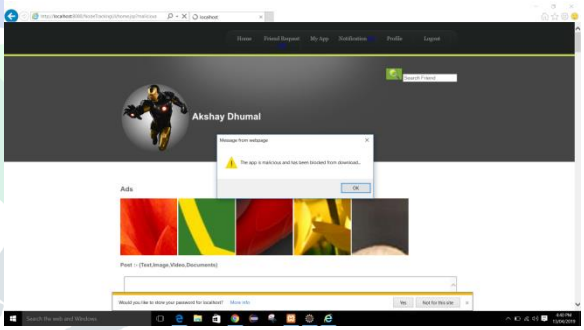











**Conclusion:** - Exploring a completely unique drawback, specifically important Node following drawback, as associate extension of Influence Maximization drawback to dynamic networks, that aims at tracking a collection of important nodes dynamically such the influence unfold is maximized at any moment. Categorization of post ads by their usage history i.e. positive or negative. The advances in digital and transmission technology ar considerably impacting human behaviors and social interactions. The most plan of our international scientific research is to develop associate automatic system for police work suspicious profiles within the social media,

through that we are able to uncover suspicious behavior and interests of users as well. The aim of our approach is to decompose every post in terms and compare them mechanically to predefined suspicious terms information by victimization similarity distance calculation. During this paper, we've got centered to gift techniques for police work suspicious posts in social network victimization similarity approach in text analysis. Our approach relies on similarity with scrutiny social network condemned posts with a suspicious predefined information. For future work, we have a tendency to commit to improve the system in term of execution time, developing machine-controlled classification and victimization different information resources so as to boost the preciseness rates, the linguistics of changed information are accustomed determine a lot of important suspicious profiles.

**Reference:-**

[1] W. Chen, Y. Wang, and S. Yang, Efficient influence maximization in social network, in KDD, 2009, pp. 199208.
[2] P. Domingos and M. Richardson, Mining the network value of customers, in KDD, 2001, pp. 5766.
[3] D. Kempe, J. Kleinberg, and E. Tardos, Maximizing the spread of influence through a 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 mining top-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 viral marketing in large-scale social networks, in KDD, 2010, pp. 10291038.
[7] W. Chen,W. Lu, and N. Zhang, Time-critical influence maximization in social networks with time-delayed diffusion process, in AAAI, 2012.
[8] W. Chen, Y. Yuan, and L. Zhang, Scalable influence maximization in social networks under the linear threshold model, in Data Mining (ICDM), 2010 IEEE 10th International Conference on. IEEE,2010, pp. 8897.
[9] N. Du, L. Song, M. Gomez-Rodriguez, and H. Zha, Scalable influence estimation in continuous-time diffusion networks, in Advances in neural information processing systems, 2013, pp. 31473155.
[10] J. Leskovec, J. Kleinberg, and C. Faloutsos, Graphs over time:densification laws, shrinking diameters and possible explanations,in KDD, 2005, pp. 177187.