Controlling The Spread Of False Information Through Social Media Platforms

Dr. Animoni Nagaraju [1], Gade Shreya (20S11A1237) [2],Kaja Bhavani Shankar (20S11A1210) [3],Kodimyala Sathwik (20S11A1235) [4],Thati Sumanth Rayudu (20S11A1242) [5],
PROFESSOR & HOD [1], UG STUDENTS [2,3,4,5],
DEPARTMENT OF DATA SCIENCE AND INFORMATION TECHNOLOGY [1]
DEPARTMENT OF INFORMATION TECHNOLOGY[2,3,4,5],
MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE,
Maisammaguda, Medchal (M), Hyderabad-500100, Telangana.

ABSTRACT

In recent years, online social media has flourished, and a large amount of information has spread through social platforms, changing the way in which people access information. The authenticity of information content is weakened, and all kinds of misinformation rely on social media to spread rapidly. Network space governance and providing a trusted network environment are of critical significance. In this article, we study a novel problem called activity minimization of misinformation influence (AMMI) problem that blocks a node set from the network such that the total amount of misinformation interaction between nodes (TAMIN) is minimized. That is to say, the AMMI problem is to select K nodes from a given social network G to block so that the TAMIN is the smallest. We prove that the objective function is neither submodular nor super modular and propose a heuristic greedy algorithm (HGA) to select top K nodes for removal. Furthermore, to evaluate our proposed method, extensive experiments have been carried out on three real-world networks. The experimental results demonstrate that our proposed method outperforms comparison approaches.

Introduction:

In recent years, with the rapid development of mobile communication technology, various information exchanges and interactive platforms have emerged, such as YouTube, Sina Weibo, and Facebook. Currently, social networking platforms play a key role in largescale information dissemination. On the one hand, the spread of positive content (hot topics, opinions, knowledge, and so on) on online social networks (OSNs) has enriched people's entertainment life. Negative contents (rumor, cyber violence, misinformation, and so on) are spread on OSNs, which may cause great harm to others and may even cause social panic [1]. For example, in October 2017, a devastating wildfire broke out in California, and the government not only relieved residents but also was treated with misinformation about wildfire on OSNs. Although misinformation was controlled by the government, initial and similar false news or misinformation was shared on Facebook more than 130 000 time [2]. Another incident occurred in August 2012 when misinformation about the earthquake spread in Ghazni, Ghazni province, Afghanistan, where thousands of people from the city and other nearby areas left their houses for a long time [3]. In order to better cultivate a healthy network ecological environment and improve the reliability of the information, it is an urgent problem to propose an effective tactic to limit or block the dissemination of misinformation. Controlling the dissemination of misinformation in OSNs has attracted the attention of many researchers [4]–[7], which finds applications in multiple domains, such as social media [8], epidemiology [9], and public health [10]. Since information dissemination can be regarded as a viral infection process [11], most early scholars used epidemiological models to describe this phenomenon [9], [12]–[16]. The misinformation dissemination on social networks and the spread of the epidemic are not exactly the same. In addition to negative information such as misinformation themselves, individuals who are exposed to misinformation can also see extra content, such as the number of people who have seen it and the number of comments on misinformation in the global network. When individuals see misinformation and their extra content, they will have a greater willingness to join the discussion or share it and strengthen the dissemination of misinformation. For example, online users who see misinformation and their extra contents will produce "Everyone is discussing, I want to express my opinion," "Your opinions are nor right, I want to correct their wrong statements," and other ideas and then participate in the misinformation discussion, making misinformation a hot topic of discussion, attracting more people to join the discussion process, and forming a vicious circle.

Therefore, we need to take an operational strategy that reduces the total amount of misinformation interaction between users on OSNs and reduce the heat of misinformation dissemination, so as to control the dissemination of misinformation. Previous studies have investigated the negative information influence, minimizing the problem from a different perspective. Some studies show that discovering and blocking K uninfected users to minimize the size of the ultimately contaminated user [17]. Other studies either based on a greedy strategy to block a limited number of links to limit the dissemination of negative information [18] or adopt the "good" campaign to fight misinformation spread so as to minimize the number of users with misinformation [19]. Furthermore, there are a lot of expansive studies about the influence dissemination phenomenon of negative content on OSNs [20]–[22]. Research on the existence of negative information such misinformation propagation [17]–[22] assumes that the probability of influence of misinformation is constant throughout the misinformation spread, ignoring the reinforcement of misinformation in the process of misinformation communication in OSNs, and did not consider the intimate relationship (the amount of misinformation interaction between users). This article considers the amount of misinformation interaction between users and studies on the nodes blocking strategy of the dissemination of misinformation in OSNs. In this article, our goal is to minimize the total amount of misinformation interaction between users by blocking some users in OSNs. More concretely, given a social network G, the source S of misinformation dissemination, and a positive integer parameter K, we aim to identify and block the nodes subset V containing K nodes from the original network according to the amount of misinformation interaction between users so that the total amount of misinformation interaction between nodes (TAMIN) is smallest after blocking the subset V of nodes under independent cascade (IC) model. It is worth noting that by blocking some nodes to prevent the spread of misinformation, the actual meaning is to prevent the spread of misinformation by closing the part of the user account that spreads misinformation or will spread misinformation. The main contents of this article are as follows. We formalize activity minimization of misinformation influence (AMMI) problem. First, it has been proven that the AMMI problem is NP-hard, which proves that the objective function calculation of the AMMI problem is #P-hard. We construct the interaction loss value parameter LF of the misinformation between users, use this parameter to convert the minimized objective function into the maximum objective function, and prove the objective function is neither submodular and supermodular. We proposed a heuristic greedy algorithm (HGA) to solve the AMMI problem. We evaluate the performance of our proposed HGA in experiments using data sets from three real-world social networks and make comparisons with other popular methods. Experimental results demonstrate that our proposed HGA is superior to other existing methods.

LITERATURE SURVEY

Online Social Networks and Insights into Marketing Communications: Even though online social network services have become enormously popular among public, there is a laxity of empirical investigations on the individual's level in this domain. This paper examines the impact of personality factors such as extraversion, selfesteem, opinion seeking and opinion leadership on brand communication and online social behaviors. Our results show that gender and extroversion predict online social network size and time spent online; that opinion seekers spend more time online and have larger networks relative to opinion leaders; and that opinion leaders are more likely to communicate their brand use online. We also find the mediating role of opinion leadership and opinion seeking in explaining the impact of general personality traits on online brand communication and social networking. Directions for future research are provided and some practical implications are discussed.

Facebook Profiles Reflect Actual Personality, Not Self Idealization: More than 700 million people worldwide now have profiles on on-line social networking sites (OSNs), such as MySpace and Facebook (ComScore, 2008); OSNs have become integrated into the milieu of modern-day social interactions and are widely used as a primary medium for communication and net-working (boyd & Ellison, 2007; Valkenburg & Peter, 2009). Despite the increasing integration of OSN activity into everyday life, however, there has been no research on the most fundamental question about OSN profiles: Do they convey accurate impressions of profile owners? This study examined whether profiles in online social networking sites (OSNs) convey accurate impressions of profile owners. Participants were 236 OSN users from the most popular OSNs in the United States (Facebook, N = 133) and Germany (StudiVZ, SchuelerVZ; N = 103). In the U.S. sample, profile owners' self-reports and reports from four well-acquainted friends were obtained using the Ten Item Personality Inventory (TIPI; Gosling, Rentfrow, &

Swann, 2003). In the German sample, self-reports on the short form of the Big Five Inventory (BFI-10; Rammstedt & John, 2007) and the NEO Five-Factor Inventory (Costa & McCrae, 1992) were combined. Our results were consistent with the extended real-life hypothesis and contrary to the idealized virtual-identity hypothesis. Observer accuracy was found, but there was no evidence of self-idealization (see Table 1), and ideal-self ratings did not predict observer impressions above and beyond actual personality. (PsycINFO Database Record (c) 2016 APA, all rights reserved).

The Big Five personality dimensions and job performance: A meta-analysis Emotional Stability, Agreeableness, Conscientiousness, and Openness to Experience) to three job performance criteria (job proficiency, training proficiency, and personnel data) for five occupational groups (professionals, police, managers, sales, and skilled/semi-skilled). Results indicated that one dimension of personality, Conscientiousness, showed consistent relations with all job performance criteria for all occupational groups. For the remaining personality dimensions, the estimated true score correlations varied by occupational group and criterion type. Extraversion was a valid predictor for two occupations involving social interaction, managers and sales (across criterion types). Also, both Openness to Experience and Extraversion were valid predictors of the training proficiency criterion (across occupations). Other personality dimensions were also found to be valid predictors for some occupations and some criterion types, but the magnitude of the estimated true score correlations was small ($\rho < .10$). Overall, the results illustrate the benefits of using the 5-factor model of personality to accumulate and communicate empirical findings. The findings have numerous implications for research and practice in PERSONNEL PSYCHOLOGY, especially in the subfields of personnel selection, training and development, and performance appraisal.

Autonomy as a moderator of the relationships between the Big Five personality dimensions and job performance: Investigated the moderating role of autonomy on the relationships between the Big Five personality dimensions and supervisor ratings of job performance. Based on data from 146 managers, results indicate that 2 dimensions of personality, Conscientiousness (r.25) and Extraversion (= r.14), were significantly related to job performance. Consistent with expectations, the validity of Conscientiousness and Extraversion was greater for managers in jobs high in autonomy compared with those in jobs low in autonomy. The validity of Agreeableness was also higher in high-autonomy jobs compared with low-autonomy ones, but the correlation was negative. These findings suggest that degree of autonomy in the job moderates the validity of at least some personality predictors. Implications for future research are noted. (PsycINFO Database Record (c) 2016 APA, all rights reserved) = 5. The right relationship is everything: Linking personality preferences to managerial behaviours: Individual differences and personality factors have reemerged as some of the more important research topics in the applied organizational sciences. With the increasing prevalence of executive coaching and the use of personality assessments, more research needs to be done on the impact of personality variables on managerial behaviours in the workplace. The following study provides an applied analysis of personality preferences and behavioural ratings collected for a developmental multirotor feedback intervention based on 343 senior managers and others in a research-driven global health services organization. Results revealed modest personality-behaviour relationships, many of which were consistent with Myers-Briggs Type Indicator theory and research; differences by observer perspective were also evident. Implications for HRD practice are discussed. © 2000 by Jossey-Bass, A Publishing Unit of John Wiley & Sons, Inc.

Existing System:

The misinformation dissemination on social networks and the spread of the epidemic are not the same. In addition to negative information such as misinformation themselves, individuals who are exposed to misinformation can also see extra content, such as the number of people who have seen it and the number of comments on misinformation in the global network. When individuals see misinformation and their extra content, they will have a greater willingness to join the discussion or share it and strengthen the dissemination of misinformation. For example, online users who see misinformation and their extra contents will produce “Everyone is discussing, I want to express my opinion,” “Your opinions are nor right, I want to correct their wrong statements,” and other ideas and then participate in the misinformation discussion, making misinformation a hot topic of discussion, attracting more people to join the discussion process, and forming a vicious circle. Therefore, we need to take an operational strategy that reduces the total amount of misinformation interaction between users on OSNs and reduce the heat of misinformation dissemination, so as to control the dissemination of misinformation.

Disadvantages of Existing System:

- There is no filtering system to find Privacy Attack.
- Less security due No URL Based attack Detection.

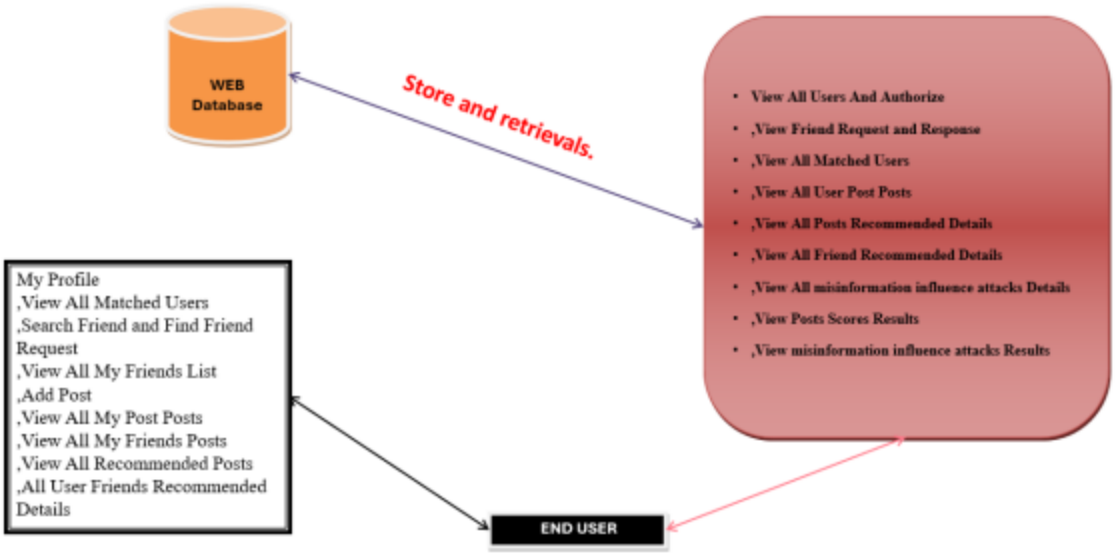
Proposed System

1. Our goal is to minimize the total amount of misinformation interaction between users by blocking some users in OSNs. We proposed a heuristic greedy algorithm (HGA) to solve the AMMI problem. We evaluate the performance of our proposed HGA in experiments using data sets from three real-world social networks and make comparisons with other popular methods. In the proposed system, First, to the best of our knowledge, the system is the first researchers studying such advanced privacy attacks as misinformation influence attacks against friend search engine in OSNs.
2. Second, in-depth analysis has been provided on querying a small-scale complete graph as well as a general network in various scenarios, which well explains the fundamental reasons of why and how the proposed attack is designed. We observe the defence scheme's [4] asymmetric disclosure of users' symmetric friendships. By taking advantage of it, we design an advanced misinformation influence attack, in which multiple malicious requestors closely coordinate with one another to launch their queries on different but related users in well-designed orders. The design logic can be generally applied to launch attacks against any friendship privacy preserving solutions that disclose the symmetric friendship in an asymmetric way.
3. Third, the proposed misinformation influence attacks is designed to carefully select which users to query, which can significantly reduce the total amount of query effort.

Advantages of Proposed System:

- The system provides the flexibility for individual users to determine the number of friends, say k, to display in response to friend queries.
- Particularly focus on the design of misinformation influence attacks against users' friendship privacy in OSNs.

SYSTEM DESIGN



Hardware Requirements:

- System : RYZEN 5000 series
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating System : Windows
- Coding Language : Java
- Type of Application : Web application (J2EE)
- Coding Concepts : (JSP, Servlet)
- Front End : HTML, CSS, JAVASCRIPT
- Back End : MySQL

INPUT AND OUTPUT DESIGN

INPUT DESIGN:

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations. This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design. Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases. Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

OUTPUT DESIGN:

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects

allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only. The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

RESULTS

Fig 1: Home Page.

Fig 2: Server Login

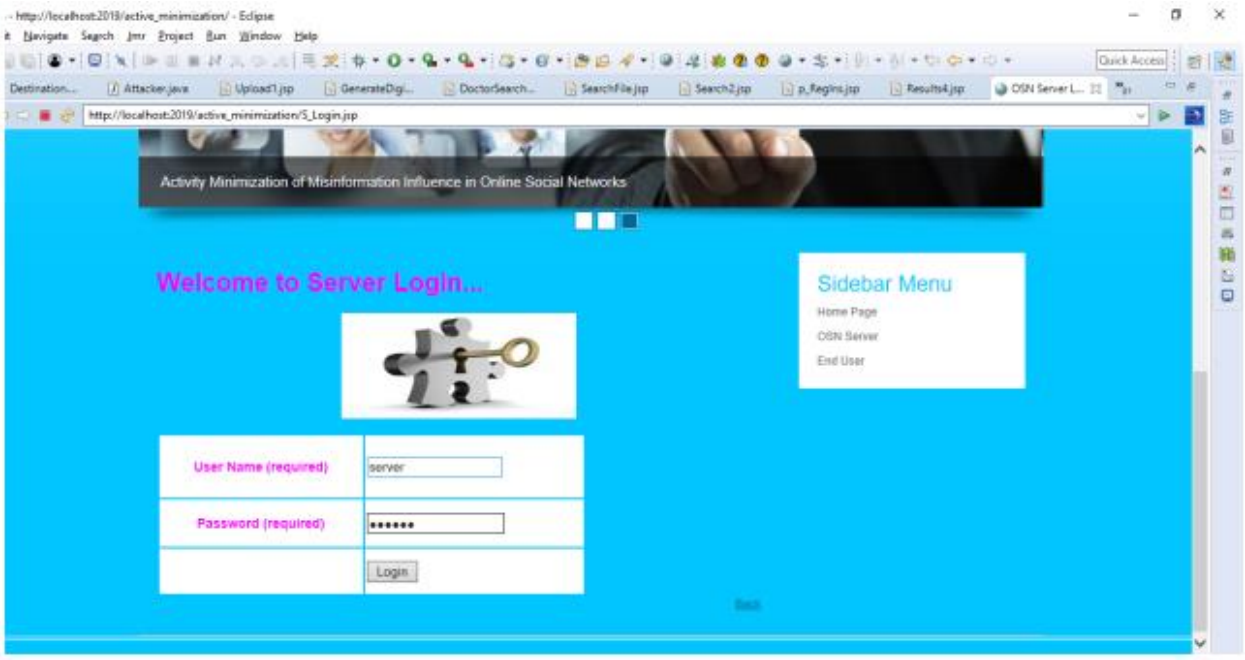


Fig 3: OSN Server Menu

Fig 4: Users Details

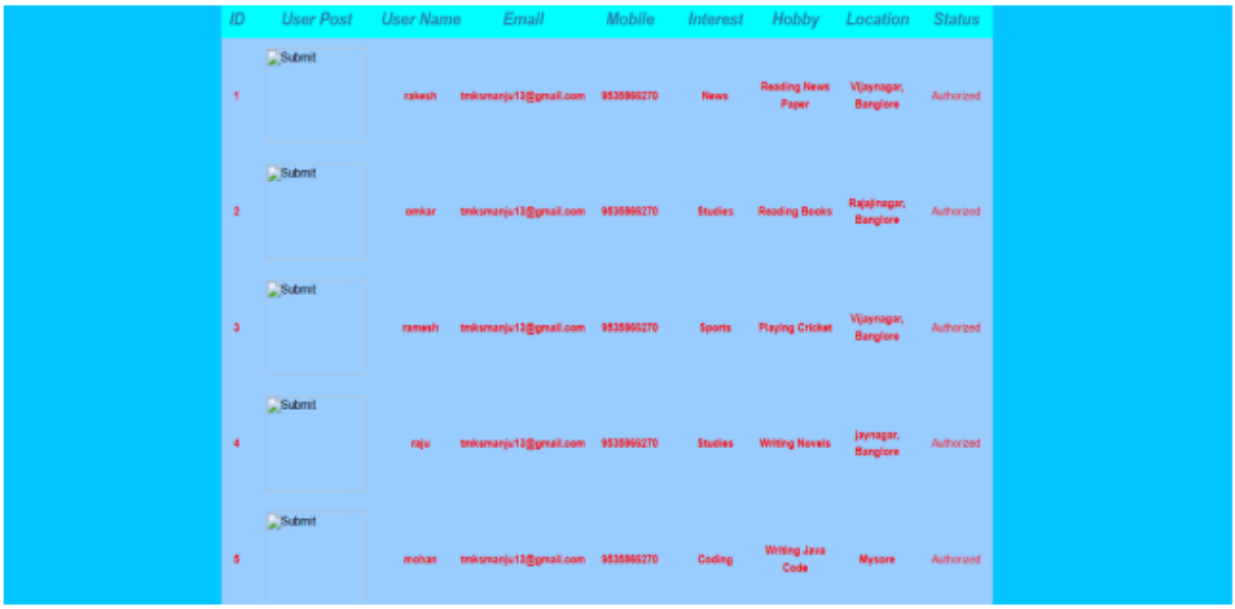
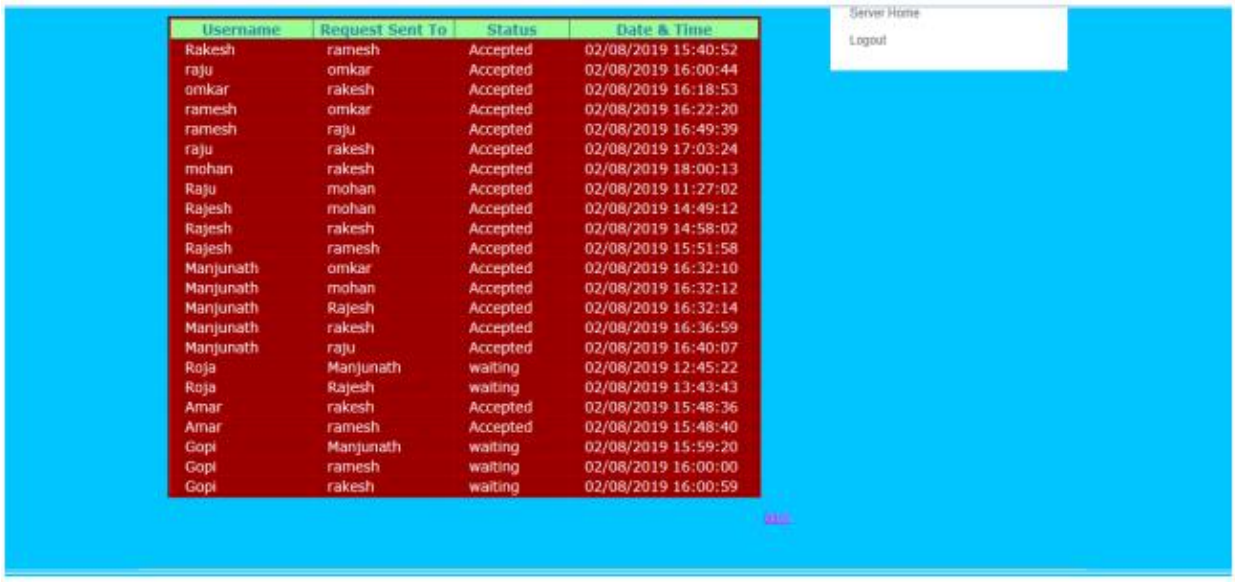


Fig 5: All Requests & Response Details



Username	Request Sent To	Status	Date & Time
Rakesh	ramesh	Accepted	02/08/2019 15:40:52
raju	omkar	Accepted	02/08/2019 16:00:44
omkar	rakesh	Accepted	02/08/2019 16:18:53
ramesh	omkar	Accepted	02/08/2019 16:22:20
ramesh	raju	Accepted	02/08/2019 16:49:39
raju	rakesh	Accepted	02/08/2019 17:03:24
mohan	rakesh	Accepted	02/08/2019 18:00:13
Raju	mohan	Accepted	02/08/2019 11:27:02
Rajesh	mohan	Accepted	02/08/2019 14:49:12
Rajesh	rakesh	Accepted	02/08/2019 14:58:02
Rajesh	ramesh	Accepted	02/08/2019 15:51:58
Manjunath	omkar	Accepted	02/08/2019 16:32:10
Manjunath	mohan	Accepted	02/08/2019 16:32:12
Manjunath	Rajesh	Accepted	02/08/2019 16:32:14
Manjunath	rakesh	Accepted	02/08/2019 16:36:59
Manjunath	raju	Accepted	02/08/2019 16:40:07
Roja	Manjunath	waiting	02/08/2019 12:45:22
Roja	Rajesh	waiting	02/08/2019 13:43:43
Amar	rakesh	Accepted	02/08/2019 15:48:36
Amar	ramesh	Accepted	02/08/2019 15:48:40
Gopi	Manjunath	waiting	02/08/2019 15:59:20
Gopi	ramesh	waiting	02/08/2019 16:00:00
Gopi	rakesh	waiting	02/08/2019 16:00:59

Fig 6: Users Posted Posts Details

Fig 7: User Login Page

Fig 8: User Profile Matching Details

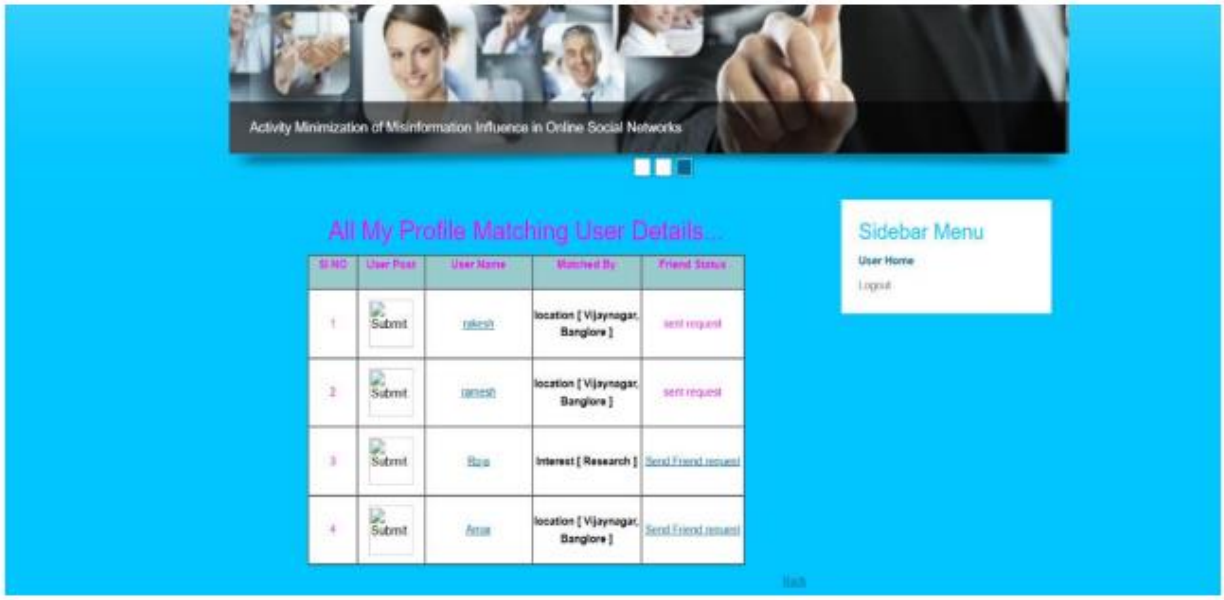


Fig 9: All Posts Ranks

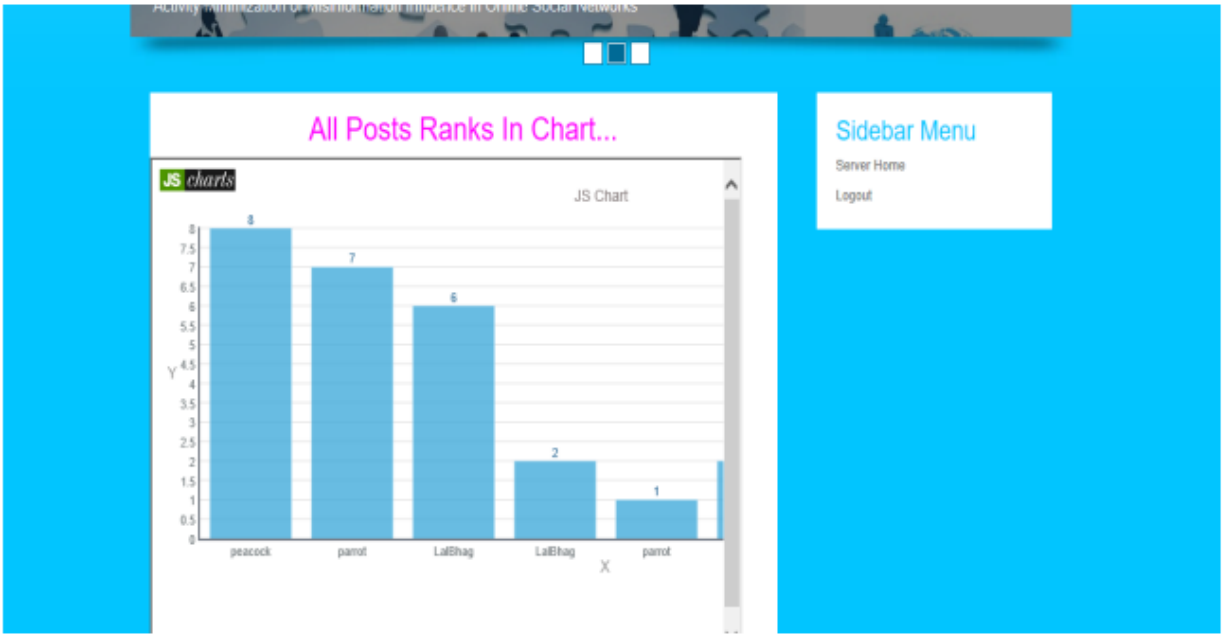
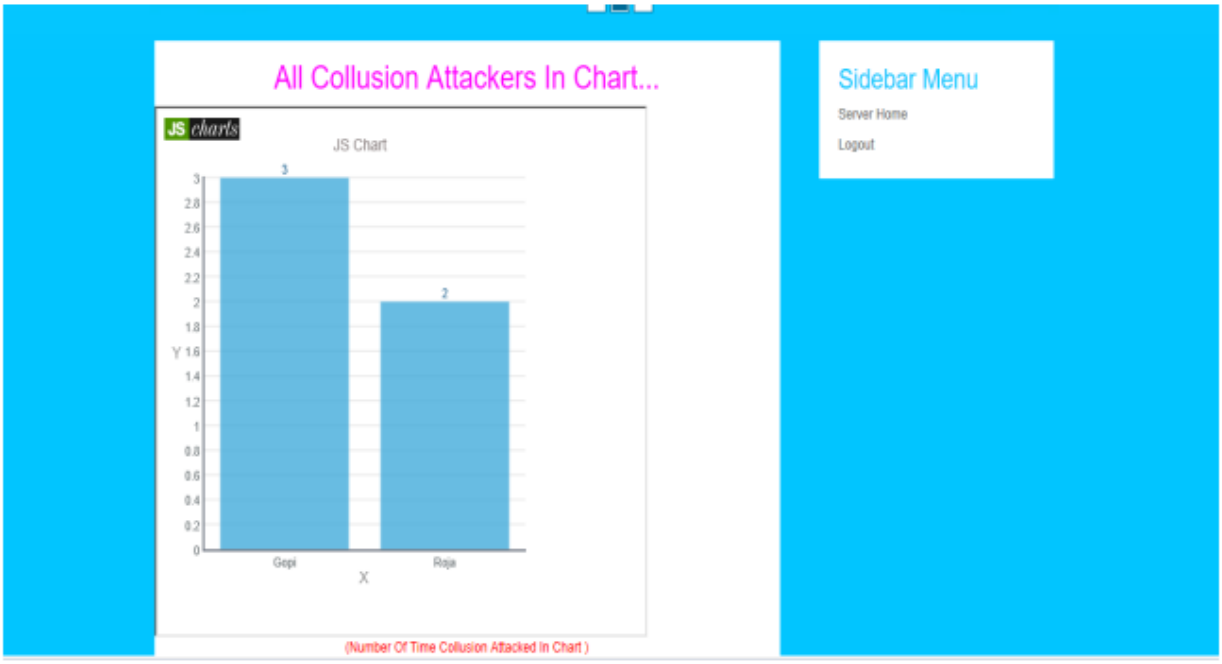


Fig 10: All Collusion Attackers



CONCLUSION & FUTURE ENHANCEMENT

Conclusion:

In this article, we study a new problem called the AMMI problem, which blocks a node set from the OSNs to minimize the TAMIN. In the IC model, we first construct a node criterion LF, which converts the minimized objective function into a maximized objective function. Then, a simple counterexample is used to show that the transformed objective function is neither submodular nor supermodular. Second, an HGA based on loss influence LF is proposed to select the set of nodes to block. Finally, we conducted extensive experiments on three real-world networks to evaluate the performance of HGA. By analyzing

and discussing the experimental results, our proposed method is superior to existing greedy or heuristic algorithms. We believe that the current research focus on misinformation control is how to quickly and accurately find a way to spread misinformation and control its spread before a large-scale spread. For future research, we study more efficient methods to solve nonsubmodular problems, such as the AMMI problem, and study the problem of minimizing the interaction of misinformation on different network structures, such as dynamic networks and time-varying networks.

Future Enhancement:

Enhancing the minimization of misinformation influence in online social networks necessitates a multifaceted approach encompassing technological advancements, user education, policy interventions, and collaborative efforts among stakeholders. Future enhancements could involve the development of advanced AI and machine learning algorithms for real-time detection and flagging of misinformation, along with user empowerment tools such as browser extensions and mobile apps to verify source credibility. Collaborative fact-checking platforms and regulatory measures could be implemented to hold social media platforms accountable and promote transparency. Community engagement and awareness campaigns, coupled with ethical considerations and human-cantered design principles, are essential for fostering a culture of media literacy and responsible online behaviour. By integrating these strategies, we can strive towards building more resilient online ecosystems that mitigate the influence of misinformation and promote the dissemination of accurate information.

BIBLIOGRAPHY

1. E. Morozov, “Swine flu: Twitter’s power to misinform,” Foreign Policy, 2009.
2. R. Yan, Y. Li, W. Wu, D. Li, and Y. Wang, “Rumor blocking through online link deletion on social networks,” ACM Trans. Knowl. Discovery from Data, vol. 13, no. 2, pp. 1–26, Jun. 2019.
3. L. Fan, Z. Lu, W. Wu, B. Thuraisingham, H. Ma, and Y. Bi, “Least cost rumor blocking in social networks,” presented at the IEEE 33rd Int. Conf. Distrib. Comput. Syst., Jul. 2013
4. L. Wu, F. Morstatter, X. Hu, and H. Liu, Big Data in Complex and Social Networks. Boca Raton, FL, USA: CRC Press, 2016, pp. 125–152.
5. H. Zhang, H. Zhang, X. Li, and M. T. Thai, “Limiting the spread of misinformation while effectively raising awareness in social networks,” in Computational Social Networks. Cham, Switzerland: Springer, 2015, pp. 35–47.
6. D. Ferraioli, D. Ferraioli, D. Ferraioli, and D. Ferraioli, “Contrasting the spread of misinformation in online social networks,” in Proc. Conf. Auton. Agents Multiagent Syst., 2017, pp. 1323–1331.
7. T. Chen, W. Liu, Q. Fang, J. Guo, and D.-Z. Du, “Minimizing misinformation profit in social networks,” IEEE Trans. Comput. Social Syst., vol. 6, no. 6, pp. 1206–1218, Dec. 2019.
8. J. Leskovec, L. Backstrom, and J. Kleinberg, “Meme-tracking and the dynamics of the news cycle,” in Proc. 15th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2009, pp. 497–506.
9. H. W. Hethcote, “The mathematics of infectious diseases,” SIAM Rev., vol. 42, no. 4, pp. 599–653, 2000.
10. J. Medlock and A. P. Galvani, “Optimizing influenza vaccine distribution,” Science, vol. 325, no. 5948, pp. 1705–1708, Sep. 2009.
11. K. Kawachi, M. Seki, H. Yoshida, Y. Otake, K. Warashina, and H. Ueda, “A rumor transmission model with various contact interactions,” J. Theor. Biol., vol. 253, no. 1, pp. 55–60, Jul. 2008.
12. P. Basaras, D. Katsaros, and L. Tassiulas, “Dynamically blocking contagions in complex networks by cutting vital connections,” in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2015, pp. 1170–1175.
13. W. Li et al., “The rumor diffusion process with emerging independent spreaders in complex networks,” Phys. A, Stat. Mech. Appl., vol. 397, pp. 121–128, Mar. 2014.
14. Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, “Cost-efficient strategies for restraining rumor spreading in mobile social networks,” IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2789–2800, Mar. 2017.
15. F. Jin, E. Dougherty, P. Saraf, Y. Cao, and N. Ramakrishnan, “Epidemiological modeling of news and rumors on Twitter,” in Proc. 7th Workshop Social Netw. Mining Anal. SNAKDD, 2013, pp. 1–9.
16. X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, “A novel approach for

inhibiting misinformation propagation in human mobile opportunistic networks," Peer-toPeer Netw. Appl., vol. 10, no. 2, pp. 377–394, Mar. 2017.
17. S. Wang, X. Zhao, Y. Chen, Z. Li, K. Zhang, and J. Xia, "Negative influence minimizing by blocking nodes in social networks," in Proc. Workshops 27th AAAI Conf. Artif. Intell., 2013, pp. 134–136.
18. M. Kimura, K. Saito, and H. Motoda, "Minimizing the spread of contamination by blocking links in a network," presented at the Proc. 23rd Nat. Conf.Artif. Intell, vol. 2, Chicago, IL, USA, 2008, pp. 1175–1180.
19. C. Budak, D. Agrawal, and A. El Abbadi, "Limiting the spread of misinformation in social networks," in Proc. 20th Int. Conf. World Wide Web WWW, 2011, pp. 665–674.
20. Y. Wang, G. Cong, G. Song, and K. Xie, "Community-based greedy algorithm for mining top-K influential nodes in mobile social networks," presented at the Proc. 16th ACM SIGKDD Int. Conf. Know. Discovery Data Mining, Washington, DC, USA, Jul. 2010.
21. X. He, G. Song, W. Chen, and Q. Jiang, "Influence blocking maximization in social networks under the competitive linear threshold model," in Proc. SIAM Int. Conf. Data Mining. Philadelphia, PA, USA: SIAM, 2012, pp. 463–474.