

DETECTING AND CHARACTERIZING EXTREMIST REVIEWER GROUPS IN ONLINE PRODUCTRE VIEWS

Project under the guidance of: K.Sivakumar (Asst.Professor), Computer Science and Engineering Department, VNITSW, Guntur, AndhraPradesh, India. T.Madhavi, T.Cherishma, G.Hima Bindu, B.Deepika IV B.Tech, Department Of Computer Science and Engineering, Vignan's Nirula Institute of Technology & Science For Women, PedaPalakaluru, Guntur-522009, AndhraPradesh, India.

1. ABSTRACT

Opinion spam in the form of reviews is common in online marketplaces. People are frequently employed to write highly good or bad reviews for specific brands in order to promote or hinder them. This is frequently carried out in groups. Although some earlier studies have attempted to identify and analyze such opinion spam groups, nothing has been done to identify individuals that target a brand as whole rather than individual goods. In this post, we manually labeled a collection of 923 possible reviewer groups using data from Amazon's product review site. We believe that the nature of reviewer groups is determined by eight characteristics unique to each (group, brand) pair. To classify prospective groups as extremist entities, we design a feature-based supervised model. Consistency in ratings, review sentiment, confirmed purchases, review dates, and helpful votes earned on reviews are examples of these behaviors. Surprisingly, we notice that a large number of verified reviews express strong feelings, which, with further research, leads to strategies to get around Amazon's existing systems for preventing unauthorized incentives.

2. INTRODUCTION

In today's online marketplace-dominated world, review portals and websites play a critical role in a buyer's decision to make their next purchase. "It's a win-win situation: the more reviews there are, the more people are willing to buy. The greater the number of individuals who purchase something, the more reviews there will be. "The more purchases you make, the higher your search ranking and the more sales you get," says Alice, the owner of Elizabeth Mott, an online cosmetics firm. Without a doubt, some people will create evaluations that aren't entirely true in order to sway the majority of purchasers' decisions in their favor. Individual reviewers may write such reviews out of frustration or delight, they do not have a significant impact on the general view of a product, but they do assist other customers by sharing their experiences. A more compelling scenario is when numerous individuals establish a complicated network, and as a result of the sheer volume of reviews, they have a significant impact on the overall sentiment of the product. Opinion spam reviews aren't the only thing that has this kind of power.

This is common opinion spam, and every review website should be aware of it and take proper precautions to identify and/or prevent it. This is a classic case of collective fraud, in which numerous users form a business network and collaborate to target and influence a certain product. This is a lesser-known phenomenon, and most groups use specific strategies to keep their collaboration hidden. Using a comprehensive and extensive analytic technique, these traits can be used to better classify them. To combat opinion spam, Amazon India has implemented a new policy that limits the number of reviews a product can receive in a single day, as stated.

We suggest that certain organizations target brands in general and write severe reviews across several products for a specific target brand in order to remain effective. This is a more advanced kind of opinion spamming, which involves creating very good or bad evaluations for a brand in general in order to promote or demote them in the internet marketplace's cutthroat competition. Although studies have been undertaken to identify such organizations that attempt to influence a product, the subject of brand-based opinion spamming remains mostly unknown. Our annotated data contains an example of such extremist groups. The products from four distinct brands are represented by four rows. Four columns reflect four different reviewers who are all

members of the same group, according to our annotation. The review information is shown by each box. As can be seen from the extreme scores, similar comments, and nearly the same date, reviewers are extremely enthusiastic about these products/brands. It's evident that this set of reviewer had strong feelings about the brands they were reviewing, both in terms of ratings and substance.

3. LITERATURE SURVEY

We divide the existing literature into two parts: general studies on e-commerce services and detection of fake reviews.

A. E-Commerce Reviews in General: There have been numerous researches on mining internet reviews and categorizing them based on user's sentiment. Review have also been used extensively in the development and enhancement of recommendation systems, as well as the extraction of product features. Another study found that product reviews are useful in clarifying the recommendations made by a recommendation system. Reviews also play a significant role in sustaining a brand's online reputation, according to various marketing research.

B. Studies on Fake Reviews

- **Studies on Reviews:** Jindal and Liupioneered the detection of fraudulent reviews. They discussed the issue of opinion spam and looked at three types of online reviews: untruthful opinions, seller/brand only reviews (no product involved), and non-reviews that used near-duplicate content as a phonic review signal. Other research into the detection of review-level spam looked at text linguistic factors, handwritten rules, and a mix of review and reviewer features.
- **Studies on Reviewers:** Rating behavior and trust scores based on relationship graph among reviewers, reviews, and stores are used in studies to detect reviewer fraud. Other research used strategies such as spikes of popularity and Bayesian methodologies to identify fraud reviewers based on their behavioral imprints. Wang et al., for example, pioneered the use of a review graph to identify spammers.
- **Studies on Reviewer Groups:** Individual fraud reviewers have a more negative and subtle influence than groups of fraud reviewers. Instead of individual reviews, the problem of manual labeling was handled by considering a group of reviewers. Labeling a group of reviewers is easier than labeling individual reviews, according to Mukherjee et al. Other notable research that use metadata to classify different entities in e-commerce platforms include Land, which classifies products, reviews, and users all at once.

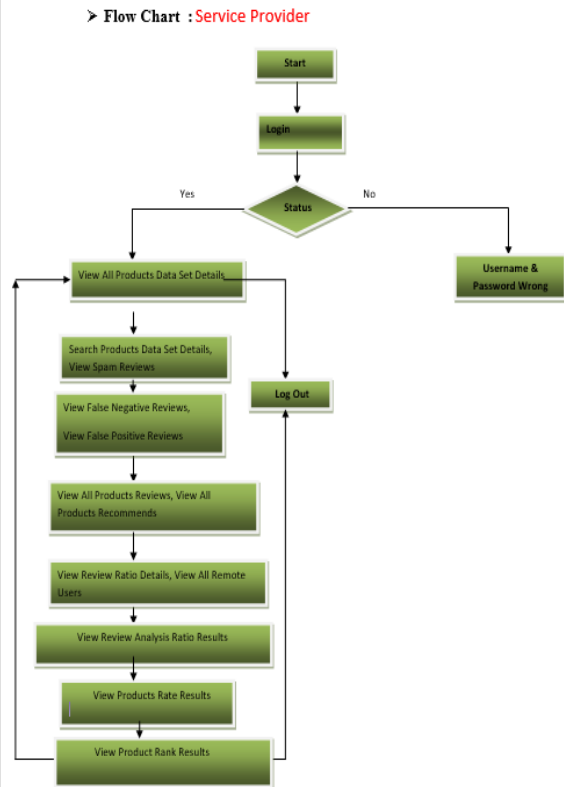
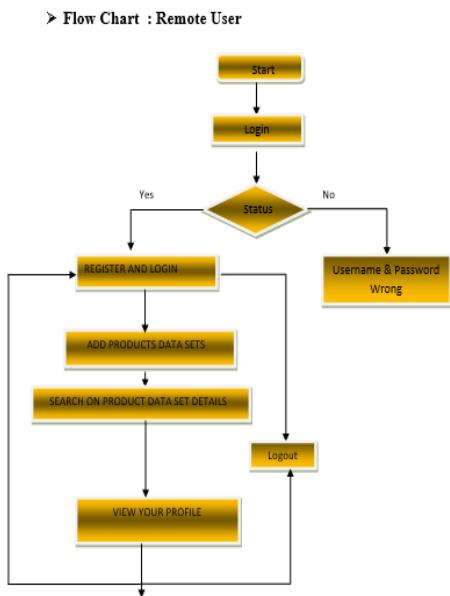
4. PROPOSED MODEL:

This paper identifies and investigates the behavioral characteristics of radical reviewer groups. We created a feature-based classifier based on the brand-specific activities of reviewer groups on the Amazon India market place to identify extremist organizations.

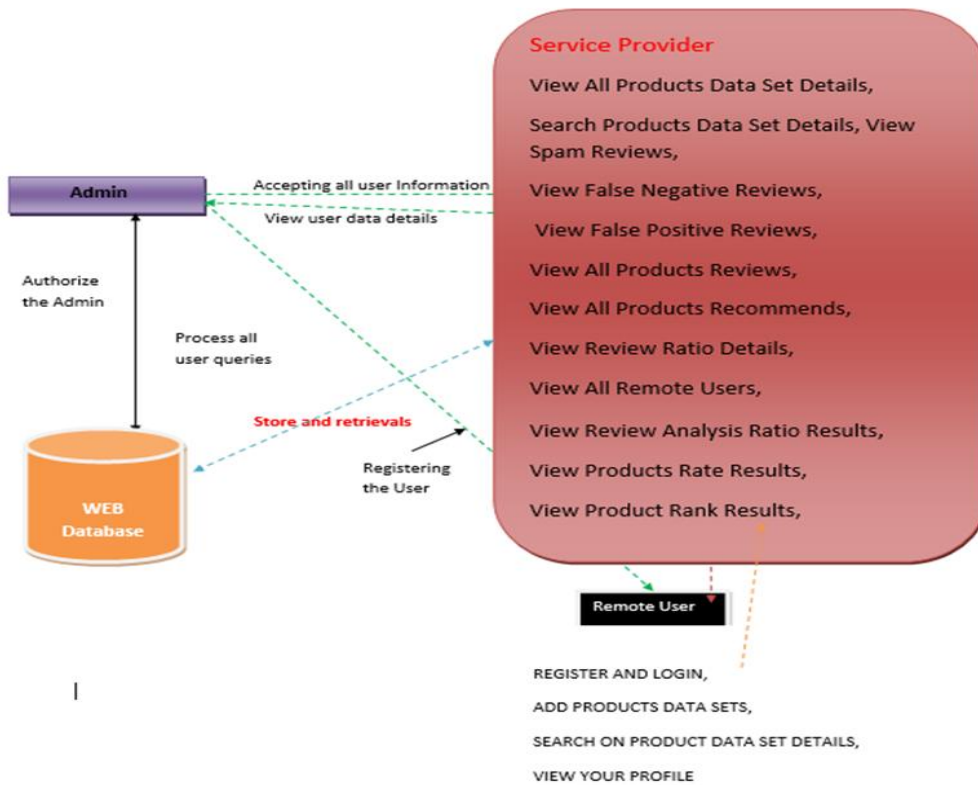
We next examine our methods further to uncover the behaviors that best represent such activities, as well as compare and analyze the general trend of these groups in relation to their behaviors, such as:

- A manually labelled data set of 923 reviewer groups that are classified into "extremist" and "moderate" categories.
- The innovative problem of identifying brand-level extremism is described and studied for the first time.
- Detailed characterization of extremist reviewer groups.
- Design supervised approach to detect extremist reviewer group.

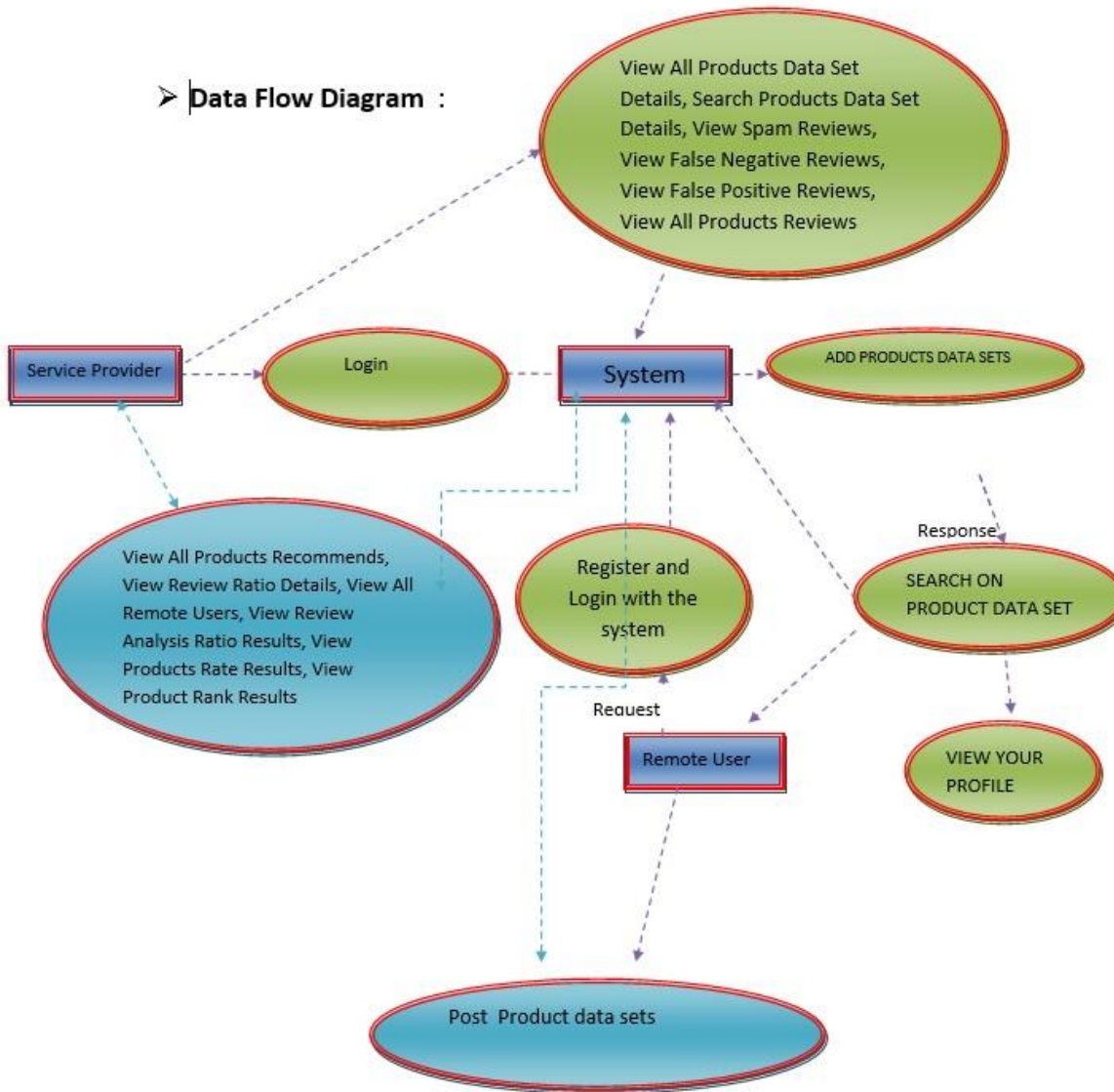
Flow Chart



Architecture Diagram



➤ **Data Flow Diagram :**



5. EXPERIMENTAL RESULTS

Detecting and Characterizing Extremist Reviewer Groups in Online Product Reviews

Behaviour, electronic commerce, machine intelligence, machine learning, reviews, social computing, web mining.

LOGIN USING YOUR ACCOUNT:

sign_in

LOGIN USING YOUR ACCOUNT:

SERVICE PROVIDER

REGISTER

Detecting and Characterizing Extremist Reviewer Groups in Online Product Reviews

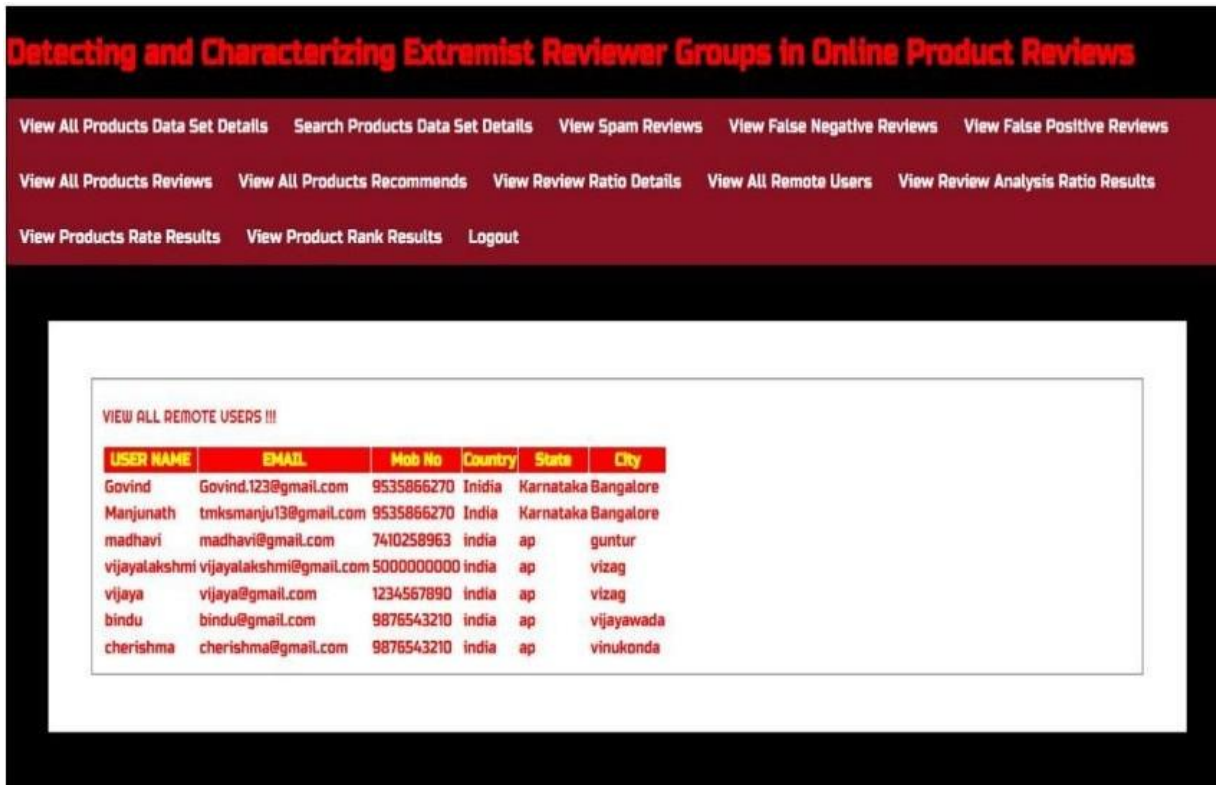
[View All Products Data Set Details](#) [Search Products Data Set Details](#) [View Spam Reviews](#) [View False Negative Reviews](#) [View False Positive Reviews](#)

[View All Products Reviews](#) [View All Products Recommends](#) [View Review Ratio Details](#) [View All Remote Users](#) [View Review Analysis Ratio Results](#)

[View Products Rate Results](#) [View Product Rank Results](#) [Logout](#)

VIEW ALL EXTREMIST FALSE NEGATIVE REVIEWER DATA SET DETAILS III

Product Category	Sub Category	Product Name	Model	Brand	Price	Description	Review	Extremist Reviewer	Review Date	Group Name
Electronics	TV	Samsung TV	2020	Samsung	55000	Connectivity,2 HDMI ports to connect set top box,Blu Ray players,gaming console,1 USB ports to connect hard drives and other USB devices	This is very good tv and can purchase all people	Gopi	28/06/2020	Music
						Hp Laptops are	This is an			



6. CONCLUSION

We covered nun known kind of opinion spam in this essay, in which spammers attack brands as a whole, writing harsh reviews in order to affect public perception of the brand. These organizations are frequently apart of a sophisticated business web capable of influencing the overall popularity and reputation of a number

of brands on review sites. This paper is the first step in establishing a link between brand-level group activity and extremist min reviews, which reveals crucial market place data.

7. FUTURE ENHANCEMENTS

These insights will aid in the development of a better recommendation based on online views. Extremist groups were discovered by observing their actions as a group based on multiple attributes, using a supervised learning technique based on a ground truth of manually annotated labels, and a set of potential spam groups was extracted using FIM. The accuracy of several classification algorithms was then examined as we categorized extreme and moderate organizations. We examined the behavior of extremist groups in detail after classifying them to learn more about the phenomena and the overall trends in how these groups target these brands. We have also released the codes and annotated dataset for further studies.

REFERENCES

1. A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in Proc. 21st Int. Conf. World Wide Web (WWW), 2012, pp. 191–200.
2. Y. Lu, L. Zhang, Y. Xiao, and Y. Li, "Simultaneously detecting fake reviews and review spammers using factor graph model," in Proc. 5th Annu. ACM Web Sci. Conf. (WebSci), 2013, pp. 225–233.
3. S. Rayana and L. Akoglu, "Collective opinion spam detection: Bridging review networks and metadata," in Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD), 2015, pp. 985–994.
4. S. Dhawan, S. C. R. Gangireddy, S. Kumar, and T. Chakraborty, "Spotting collective behavior of online frauds in customer reviews," 2019, arXiv:1905.13649.
5. K. Dave, S. Lawrence, and D. M. Pennock, "Mining the peanut gallery: Opinion extraction and semantic classification of product reviews," in Proc. 12th Int. Conf. World Wide Web (WWW), 2003, pp. 519–528.
6. B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment Classification using machine learning techniques," in Proc. Conf. Empirical Methods Natural Lang. Process., 2002, pp. 79–86.
7. K. Mouthami, K. N. Devi, and V. M. Bhaskaran, "Sentiment analysis and classification based on textual reviews," in Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES), Feb. 2013, pp. 271–276. Q. Ye, Zhang, and R. Law, "Sentiment classification of online reviews to travel destinations by supervised machine learning approaches," *Expert Syst. Appl.*, vol. 36, no. 3, pp. 6527–6535, Apr. 2009.
8. M. Chelliah and S. Sarkar, "Product recommendations enhanced with reviews," in Proc. 11th ACM Conf. Recommender Syst., Aug. 2017, pp. 398–399.
9. [9] L. Chen and F. Wang, "Preference-based clustering reviews and for augmenting ecommerce recommendation," *Knowl.-Based Syst.*, vol. 50, pp. 44–59, Sep. 2013. 87
10. J. Feuerbach, B. Loepp, C.-M. Barbu, and J. Ziegler, "Enhancing an interactive recommendation system with the review-based information filtering," in Proc. IntRS @ Rec Sys, 2017, pp. 10–55.
11. A. Almahairi, K. Kastner, K. Cho, and A. Courville, "Learning distributed representations from reviews for collaborative filtering," 2018, arXiv:1806.06875.
12. [12] A.-M. Popescu and O. Etzioni, "Extracting product features and opinions from reviews," in Proc. HLT, 2005, pp. 339–346.
13. B. Liu, M. Hu, and J. Cheng, "Opinion observer: Analyzing and comparing opinions on the web," in Proc. 14th Int. Conf. World Wide Web (WWW), 2005, pp. 342–351.
14. M. Hu and B. Lin, "Mining opinion features in customer reviews," in Proc. AAAI, 2004, pp. 755–760.
15. Kanumalli, S. S., Chinta, A., Chandra Murthy, P. S. R. (2019). Isolation of wormhole attackers in IOV using WPWP packet. *Revue d'Intelligence Artificielle*, Vol. 33, No. 1, pp. 9-13. <https://doi.org/10.18280/ria.330102>
16. Narayana, Vejjendla Lakshman, et al. "Secure Data Uploading and Accessing Sensitive Data Using Time Level Locked Encryption to Provide an Efficient Cloud Framework." *Ingénierie des*

- Systèmes d'Information 25.4 (2020).
17. Kotamraju, Siva Kumar, et al. "Implementation patterns of secured internet of things environment using advanced blockchain technologies." *Materials Today: Proceedings* (2021).
 18. Krishna, Komanduri Venkata Sessa Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using CNN and Firefly Optimization." *Traitement du Signal* 38.1 (2021).
 19. Satya Sandeep Kanumalli, Anuradha Ch and Patanala Sri Rama Chandra Murty, "Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach" *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(1), 2020. <http://dx.doi.org/10.14569/IJACSA.2020.0110157>
 20. CHALLA, RAMAIAH, et al. "Advanced Patient's Medication Monitoring System with Arduino UNO and NODEMCU." 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2020.
 21. Kanumalli, Satya Sandeep, Anuradha Ch, and Patanala Sri Rama Chandra Murty. "Advances in Modelling and Analysis B." *Journal homepage: http://iieta.org/Journals/AMA/AMA_B* 61.1 (2018): 5-8.
 22. Venkatramulu, S., et al. "Implementation of Grafana as open source visualization and query processing platform for data scientists and researchers." *Materials Today: Proceedings* (2021).
 23. Sandeep, Kanumalli Satya, Anuradha Chintu, and Patanala Murty. "Isolation of Wormhole Attackers in IOV Using WPWP Packet." *Rev. d'Intelligence Artific.* 33.1 (2019): 9-13.
 24. Gopi, Arepalli Peda, et al. "Classification of tweets data based on polarity using improved RBF kernel of SVM." *International Journal of Information Technology* (2020): 1-16.
 25. Narayana, Vejjendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." *Rev. d'Intelligence Artific.* 33.1 (2019): 45-48.
 26. Arepalli, Peda Gopi, et al. "Certified Node Frequency in Social Network Using Parallel Diffusion Methods." *Ingénierie des Systèmes d'Information* 24.1 (2019).
 27. Narayana, Vejjendla Lakshman, Arepalli Peda Gopi, and R. S. M. Patibandla. "An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology." *Blockchain Applications in IoT Ecosystem*. Springer, Cham, 2021. 239-256.
 28. Kotamraju, Siva Kumar, et al. "Implementation patterns of secured internet of things environment using advanced blockchain technologies." *Materials Today: Proceedings* (2021).
 29. Bharathi, C. R., et al. "A Node Authentication Model in Wireless Sensor Networks With Locked Cluster Generation." *Design Methodologies and Tools for 5G Network Development and Application*. IGI Global, 2021. 236-250.
 30. Vejjendla, Lakshman Narayana, Alapati Naresh, and Peda Gopi Arepalli. "Traffic Analysis Using IoT for Improving Secured Communication." *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory*. IGI Global, 2021. 106-116.
 31. Narayana, Vejjendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology."
 32. Yamparala, Rajesh, and Balamurugan Perumal. "EFFICIENT MALICIOUS NODE IDENTIFICATION METHOD FOR IMPROVING PACKET DELIVERY RATE IN MOBILE AD HOC NETWORKS WITH SECURED ROUTE." *Journal of Critical Reviews* 7.7 (2020): 1011-1017.
 33. Devi, S. Pramela, et al. "Likelihood based Node Fitness Evaluation Method for Data Authentication in MANET." *International Journal of Advanced Science and Technology* 29.3 (2020): 5835-5842.
 34. Yamparala, Rajesh, and Balamurugan Perumal. "Secure Data Transmission with Effective Routing Method Using Group Key Management Techniques-A Survey Secure Data Transmission with Effective Routing Method Using Group Key Management Techniques-A"