Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 4, 2020

Review Article

DISCOVERING AND EXPANSION THE IRREGULAR MANNERS OF USERS IN ONLINE SOCIAL NETWORKS USING DATA MINING TECHNIQUES

S. Sadhasivam[1], Dr.P. Valarmathie[2], Dr.K. Dinakaran[3]

[1]Assistant Professor, Department of Computer Science and Engineering, KSR College of Engineering, Namakkal, Tamilnadu, India.
sivam.sadha@gmail.com
[2]Professor, Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamil nadu, India.
csevalar@gmail.com
[3]Professor, Department of Information Technology, Saveetha Engineering College, Chennai, Tamil nadu, India.
kdinacse@gmail.com

Received: 05.12.2019 ***Revised: 16.01.2020*** ***Accepted: 19.02.2020***

Abstract
The anomaly detection in social media using data mining concept is an evergreen topic in present situation due to the hacking of user information from various hand held devices. These anomaly activities are also known as malicious activities which are spread over the social media through different social media tools. These creates false information in among the various age groups and its threatens the media in all over world. This paper takes a detailed survey on Detecting anomalous behavior of user in online Social networks using data mining techniques.

Keywords: Social Media, Attacks, Abnormal, Behavior, Users.

http://dx.doi.org/10.31838/jcr.07.04.62

INTRODUCTION

The anomaly detection in social media using data mining concept is an evergreen topic in present situation due to the hacking of user information from various hand held devices. These anomaly activities are also known as malicious activities which are spread over the social media through different social media tools. These creates false information in among the various age groups and its threatens the media in all over world. These malicious patterns or activities should be detected for improving the entire network strategies in social media. These also create mal functions in various routine activities based on the entire learning platform as illustrated in Meier et al. (2017). These will be eliminated using various data mining approaches in present form as depicted in Sirivianos et al. 2014.

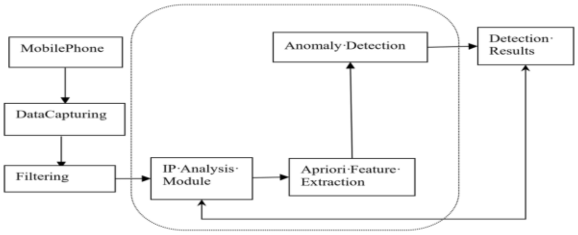

Figure 1: Anomaly Detection Model

Figure 1 shows the anomaly detection model. Recently there has been a rapid increase in interest regarding social network analysis in the data mining community. The basic motivation is the demand to exploit knowledge from large amounts of data collected, pertaining to social behavior of users in online environments (Soliman et al. 2016). This structured learning platform will effectively improves the learning behavior of the modern media in social networks. This will improve the reliability among the certain area of the networks using various data mining techniques. Data mining based techniques are proving to be useful for analysis of social network data, especially for large datasets that cannot be handled by traditional methods.

SURVEY ON ANOMALOUS BEHAVIOR OF USER IN ONLINE SOCIAL NETWORKS

Qi et al. (2010) proposed Group Anomaly Detection (GAD) methods for detecting the anomaly behavior of the users in social networks. The authors used inference and learning algorithms for predicting the misbehavior users in social media. The pair wise and point wise algorithms were used in this paper for determining the anomalous behaviors and activities of the users in social network system. The standard model was developed by analyzing various attributes in social media using data mining techniques. The authors checked their dataset in both real time data set and synthetic dataset. Figure 2 shows the Group Anomaly Detection model for determining the unusual activities or behaviors of users in social networks.

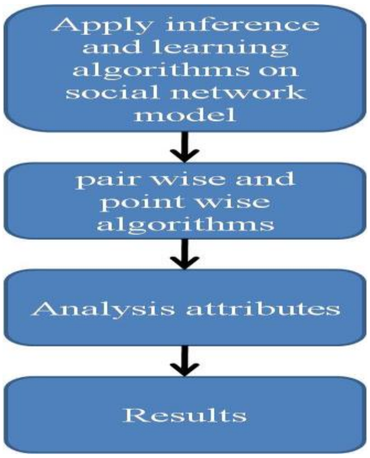
Apply inference and learning algorithms on social network model
pair wise and point wise algorithms
Analysis attributes
Results

Figure 2: Group Anomaly Detection Model

Srivastava et al. (2008) developed a linear regression model or algorithm for analyzing the behavior or performance of users in social networks. The authors used various data mining techniques for retrieving the particular data from the set of available data from the mined data set. The authors applied viral marketing technique on the collected information's for selecting the best data from the available set of data.

Muhammad Al-Qurishi et al. (2018) developed a methodology or framework for identifying the malicious activities of every user in social media like face book and twitter. The authors used prediction mathematical model for analyzing the behavior or performance of every user in social media for detecting these kinds of certain behavior activities. The proposed framework consists of the following modules as stated below.

- Social service manager
- Data acquisition layer
- Storage management layer
- Analysis representation layer

The social service manager received requests from various nodes as desktop computers, laptops or mobile devices. All these requests were collected and maintained by the data acquisition layer, which was the second layer of the proposed method. The sensed and measured data were collected and stored in storage management layer which was the next to the data acquisition layer. The final required output was produced in analysis representation layer which was the final layer of the proposed method. The author used Principal Component Analysis (PCA) method for selecting the best patterns in the collected information.

Figure 3 shows the proposed social behavior analysis method using data mining techniques.

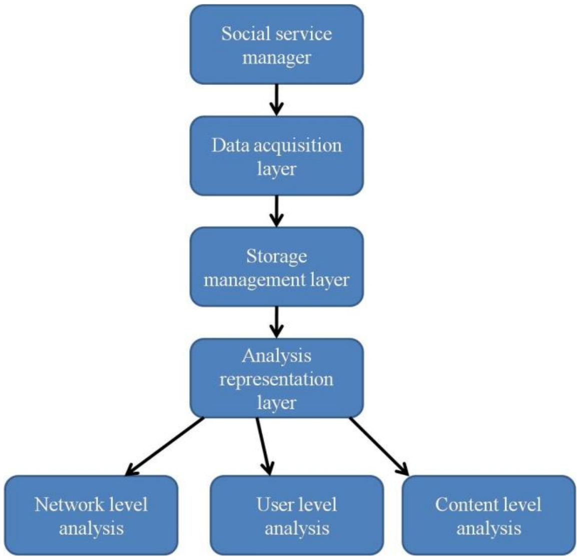

Figure 3: Proposed Social Behavior Analysis Method

Lin et al. (2012) used different patterns for receiving the user requests from various nodes in social media networks. The different social media were connected by different social networks which were further maintained by unique node architecture. The authors analyzed the performance of every user in social networks using different data mining techniques.

Tyshchuk et al. (2018) predicted the behavior of the users in social media with respect to different contributions in various social media activities.

The following procedures were used for observing the behavior of each user in social network models.

- Determine the warning messages of each user which were received during their content analysis in social networks.
- Confirm the additional information requests for each and every user in social activities.
- Take the required action on each user request.

Figure 4 shows the context analysis of each and every user in social models.

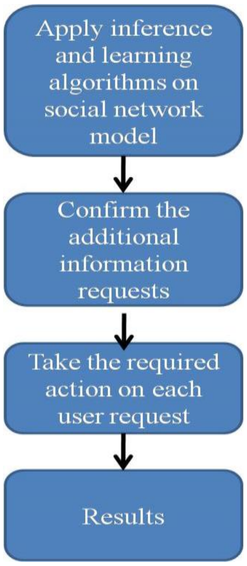
Apply inference and learning algorithms on social network model
Confirm the additional information requests
Take the required action on each user request
Results

Figure 4: Context Analysis

Laleh et al. (2018) analyzed the Anomalous Behaviors of every user in social media or networks in order to improve the user security in social Medias. The proposed method has risk assessment phase and group identification phase. In case of risk assessment phase, user behavior diverges were analyzed which classified each user activities as either normal or abnormal. The normal behavior and abnormal behavior were addressed in this phase for determining the performance of the users in social networks. The number of friends, activity level and percentage of public profile of each user were analyzed in this work through this phase. Probabilistic-based clustering was used in this work for determining the abnormal activities of every user in social media networks.Figure 5 shows the Assessment phases in social media.

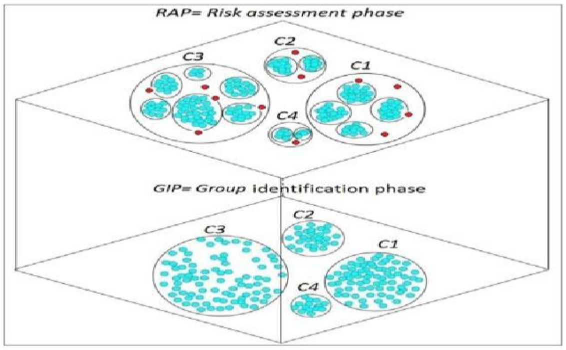

Figure 5: Assessment Phases in Social Media

Srishty Jindala et al. (2018) predicted various social media feeds for analyzing the behavior of users in social media networks. Iterative Clustering algorithm was used in this work for determining the behavior of each user in social networks.

COMPARISON AND DISCUSSION

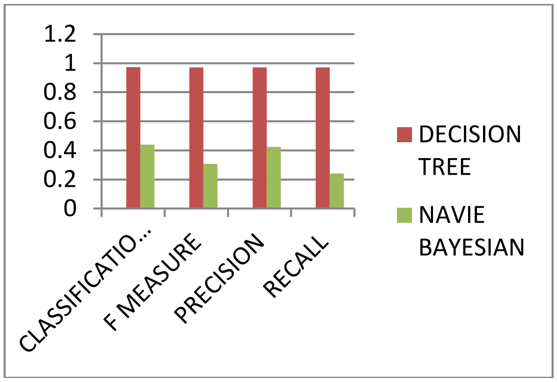

Figure 6: Comparison of Data Mining Techniques

The decision tree and Naive Bayesian techniques are data mining techniques that are compared in figure 6. Therefore, the decision tree algorithm is much better than naive Bayesian. This study has conducted a comparison between two classification algorithms namely; Decision Tree *C*4.5 and Naïve Bayesian on Squid, using Orange tool. The presented study illustrated that Decision Tree algorithms had 97% accuracy, 97% precision and 97% recall. On the other hand, Naïve Bayesian indicated 43% accuracy, 30% precision and 42% recall. By comparing the three evaluateparametersforthetwoalgorithmsitisconcludedthatDecisionTreehashighestperformance than Naïve Bayesian over the dataset using manual and automatic folding to adjust the required bandwidth inside the network.

CONCLUSIONS

In this paper, various conventional methods for analyzing the anomaly behavior of the users in social media networks were analyzed. The pair wise and point wise algorithms were analyzed in this paper for determining the anomalous behaviors and activities of the users in social network system. The standard model was developed by analyzing various attributes in social media using data mining techniques.

REFERENCES

1. Qi(Rose) Yu, Xinran He and Yan Liu, “GLAD: Group Anomaly Detection in Social Media Analysis” ACM Transactions on Knowledge Discovery from Data, Vol. 9, No. 4, Article 39, Publication date: March 2010.
2. J. Srivastava, "Data mining for social network analysis," *2008 IEEE International Conference on Intelligence and Security Informatics*, Taipei, 2008.
3. Muhammad Al-Qurishi, Shamim Hossain, Majed Alrubaian, SkMd Mizanur Rahman, “Leveraging Analysis of User Behavior to Identify Malicious Activities in Large-Scale Social Networks”, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 14, NO. 2, FEBRUARY 2018.
4. J. Lin, Z. Li, D. Wang, K. Salamatian, and G. Xie, “Analysis and comparison of interaction patterns in online social network and social media,” in Proceedings of International Conference on Computer Communications and Networks (ICCCN), August 2012.
5. Y. Tyshchuk and W. A. Wallace, "Modeling Human Behavior on Social Media in Response to Significant Events," in *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 444-457, June 2018.
6. N. Laleh, B. Carminati and E. Ferrari, "Risk Assessment in Social Networks Based on User Anomalous Behaviors," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 295-308, 1 March-April 2018.
7. Srishty Jindala, Kamlesh Sharma, “Intend to analyze Social Media feeds to detect behavioral trends of individuals to proactively act against Social Threats”, Procedia Computer Science, Volume 132, 2018, Pages 218-225.
8. F. Meier, J. Aigner, and D. Elsweiler, “Using sessions from clickstream data analysis to uncover different types of twitter behaviour,” in *Everything Changes, Everything Stays the Same? Understanding Information Spaces Proc. 15th Int. Symp. Inf. Sci. (ISI 2017)*, pp. 237–250, 2017.
9. T. Shakiba, S. Zarifzadeh, and V. Derhami, “Spam query detection using stream clustering,” *World Wide Web*, New York, NY, USA: Springer- Verlag, 2017, pp. 1–16.
10. T. Silawan and C. Aswakul, “Sybilvote: Formulas to quantify the success probability of sybil attack in online social network voting,” *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1553–1556, Jul. 2017.
11. M. Sirivianos, K. Kim, J. W. Gan, and X. Yang, “Leveraging social feedback to verify online identity claims,” *ACM Trans. Web*, vol. 8, no. 2, 2014, Art. no. 9.
12. A. Soliman and S. Girdzijauskas, “Dlsas: Distributed large-scale anti-spam framework for decentralized online social networks,” in *Proc. IEEE 2nd Int. Conf. Collaboration Internet Comput.*, 2016,
13. Penumetsa, S.C., Hoque, M.Z., Giugliano, G.Reversible myocardial dysfunction following intraocular bevacizumab administration(2013) Journal of Cardiovascular Disease Research, 4 (1), pp. 58-60.
DOI: 10.1016/j.jcdr.2013.02.017