IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Detection of Anomaly Actions on Social Networks using Machine Learning

Mayur Jain[1*], PrashanthA[2],Prabhudev B K[3], Sagar Reddy N J[4], Mangala C N[5]

[1,2,3,4,5]Department of Computer Science, East West Institute of Technology, Bengaluru, India

DOI: https://doi.org/10.26438/ijcse/v7si15.116121 | Available online at: www.ijcseonline.org

***Abstract*—**Social media is no doubt the richest source of human generated data. The user's options, feedbacks and critiques provided by social network users reflect attitudes and sentiments of certain topics, products, or services. Every day, large quantity of messages is created, stored, commented, and shared by people on social media websites, such as Twitter, Instagram, Quora and Facebook. This in general acts as valuable data for researchers and practitioners in different application domains, such as data analytics, marketing, to inform decision-making. Extracting valuable social signals from the huge crowd's messages is challenging, due to the dynamic crowd behaviors. These are the anomalies caused by a user because of his/her variable behavior towards different sources. Due to such risk parameters, it is always a great practice to have a mechanism to monitor each online social network user. This paper provides a way in which anomaly analysis can be implemented in social media such as Facebook. This work hence acts as a risk analyzer for the administrator of the Face book services so that they can formulate strategies to overcome the same.

***Keywords*-**Anomaly detection,Social network,SVM,Data Analytics

I. INTRODUCTION

Over the recent years, the surge of social media, such as Facebook and twitter, has significantly advanced the way that people publish, acquire, and share news and information. Every day, millions of data gets created, commented on, and disseminated by over one billion active social media users [10]. Such publicly available data as well as their respective patterns among people acts as great asset for researchers and practitioners in a variety of fields, such as behavioural science and marketing, to make data-oriented decisions. While there is quite a large amount of information available on social media, not every posting is considered equally valuable. The first challenging question is: which data is more beneficiary? To be efficient, analysts aim to study such data completely in order to find anomalies.

Anomalies are the irregularbehaviour of the user which results in suspicious activity causing threats to the information being shared and other regular network users. With the growth of online social interaction sites, userbehaviour tracking and anomaly detection are two of the major areas of research. The main goal of detecting anomalies is to identify improper usage of social media services [17]. A lot of research has been carried out to build a generalized method for anomaly detection. A number of methods are proposed for detecting them under specific conditions on different domains.

Over the past few years, detection of the anomalies has been taken as a serious research which required efficient approaches for improved identification. However, the approaches proposed so far are valid for networks under certain pre-defined parameters which mostly involves the level of information exchange between the source and the users.

One of the popular Online Social Network is Facebook which provides platform where user can keep in touch with family, friends and share the information among them. Facebook is also used for commercial purposes. Despite of drastic increase in OSN usage – Facebook, for instance, has now 1 billion daily users, 1.3 billion mobile users, 1.55 billion monthly active users; which has led to lot of security and privacy concerns.

Anomaly detection is based on the idea that the behavioural characteristics of a normal user can be distinguished from behaviour of abnormal user [1].

In this paper, we describe a new method for anomaly detection in social media posts. The basis for this method is a series of patents filed in [4] [5] and [6]. The rest of this paper is organized as follows. Section II discusses about the related works. Section III presents the proposed methodology of fine-grained sentiment analysis. Section IV provides the system architecture for proposed method using real world anomaly buzzwords, in Section V, we have provided the overview of algorithm used, Section VI provides the results and lastly in Section VII we conclude this study along with all the references.

II. RELATED WORK

The analysis of user's behaviour in online social networks to find anomalies can be carried out in different ways. Over the

past few years, different kinds of anomalies have been identified. The solutions for these anomalies focus on the categorization of the anomaly and then provide appropriate solutions which can resolve the problem.

Rule-based Anomaly Detection
Predefining the rules which can help in identification of anomalies.[16] considered the anomalies inthe weighted graphs and developed an algorithm called Oddball algorithm for finding the affected nodes. The authors of [16] utilized the rule-basedapproach to detect the anomalies in graph. The aboveapproaches are capable of identifying a particular kind of anomaly in a restricted environment. These approaches fail to identify node behaviour in online social networks as these rely only on the connections between the nodes, which can be manipulated very easily.

Compromised Account-based Anomaly Detection
Another main aspect of the anomalies in the social networksis the compromised accounts, this is examined in [6] [3]. The authors developed an approach under the name COMPA, which can identify almostall the compromised accounts in any of the social networking sites. The authors analysed and tested this approach on a huge data set comprising approximately 1.4 billion Twittermessages which were publicly available.

Interaction-based Anomaly Detection
The Point of interaction can be one more solution for identifyinganomalies. This kind of approach utilizes the concept of anomaly scores.[12] proposed change-point detection technique which made use of the Sequentially Discounting Normalized Maximum Likelihood (SDNML). The authors utilized the anomaly scores obtained from these experiments to identify the link anomalies.

Statistical Anomaly Detection
Statistics can be one more solution to the problem of anomaly detection. Using the concept of statistics,[15] proposed an efficient system for anomaly detection in the social networks, the work uses the Bayesian analysis approach. A two-phase approach is used by the authors of [15] for the anomaly detection which reduces the number of groups of potentially anomalous nodes. These solutions rely much on the collected data, which can be used only in the case of learned anomalies.

The works presented in this section clearly showsthat almost all of the existing approaches have been actingas generic solutions in the detection of the anomalies and have not considered for live anomaly detection. Thus, efficient approaches are required which can not only identify the threat level caused by those anomalies but also act wisely in resolving those actions.

The machine-learning method uses known properties derived from the training data to classify new information. For thetext data, it derives the relationship between features of the text segments. There is a wide variety of machine-learning based methods, such as the Naive Bayes (NB) classifier, Maximum Entropy classifier and support vector machine (SVM). The Naïve Bayes classifier is a probabilistic classifier that assumes the statistical independence of each of the feature [10] [13]. Max Ent is one more probabilistic classifier that uses a multinomial logistic regression model [11]. It is closely related to the Naive Bayes classifier, but has some kind of dissimilarities such as it uses search-based optimization to find weights for the features that maximizes the likelihood of the training data.Whereas SVM is quite different it is a non-probabilistic classifier that works by constructing a decision surface [14] [18]. The principle of the SVM algorithm is to find a decision surface, named hyperplane that will optimally splits the training set. Then, the algorithm finds thehyperplane in this space with thelargest margin, separatingthe data into different groups. This approach can achieve a good classification accuracy when compared to simple lexicon-based approaches and hence, it was widely used[20] [7].

The first major limitation is that the training data needs tobe large enough to allow sufficient representation of full target domains. In the real-world social media context, it is hard to determine the effective size for a training dataset. This makes learning-based approaches too costly and impractical to be applied to set of problems.

To overcome the limitations as well as to tackle the challengesmentioned above, this study proposes a new anomaly detection method which enhances the current methods available for anomaly detection, through vectors acting live on social media. The working of the proposed method is demonstrated using a live model of social network.

III. METHODOLOGY

Our proposed system demonstrates how anomaly can be detected in live on social media such as Facebook. The proposed system creates a social network hosted on a cloud service. The social network acts as a replica to actual Facebook site. The users can register on the social network and can login with login credentials anytime. The users are greeted with home page and are provided with an option to share his/her opinions through posts. As soon as the user posts, the text is stored and compared with predefined feature vectors created using anomaly buzz words, the text are dimensionally reduced and concluded as either anomaly affected or not. In case of mixed posts, the Gradient Based SVM is applied on the text with the help of feature vectors and anomaly is detected, as shown in Figure 1.

Depending upon result of this anomaly detection module a report is generated which contains information about users and number of the time they have voided the rules. This information is provided graphically to the admin using data analytics. Depending upon report generated appropriate action are taken (sending warning mail/removing the user)

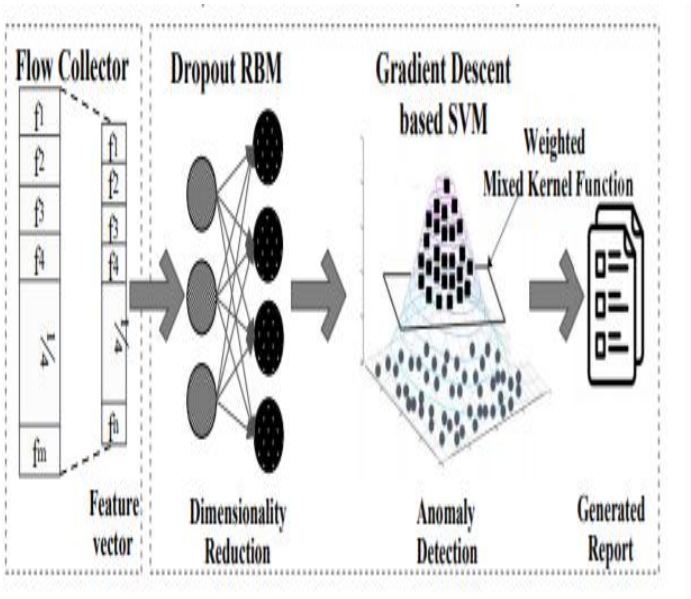

Figure 1: Anomaly detection module

IV. SYSTEM ARCHITECTURE

User first logins to the social network cloud with fresh registration or login credentials. The user then enters a text messages, and these text messages are stored in database. From the database, all the messages are extracted and the classification of the messages is done, that is messages are classified into Anomaly posts and normal posts. The classification of the posts is done using SVM. For the input messages anomaly identification rules are applied to determine the category of the words in the messages. Neurons are trained using the training dataset. Finally result of the messages is predicted that is whether the entered posts are anomaly affected or not.

The system keeps a count of number of times a user tweets an anomaly text. After 5 anomaly tweets the system warns the user through email and after 10 anomaly tweets the user will be removed and notified the same through email, the admin of the social network has full control to remove anomaly tweets any time. The admin is also provided with data analytics about all the users and their number of anomaly actions.

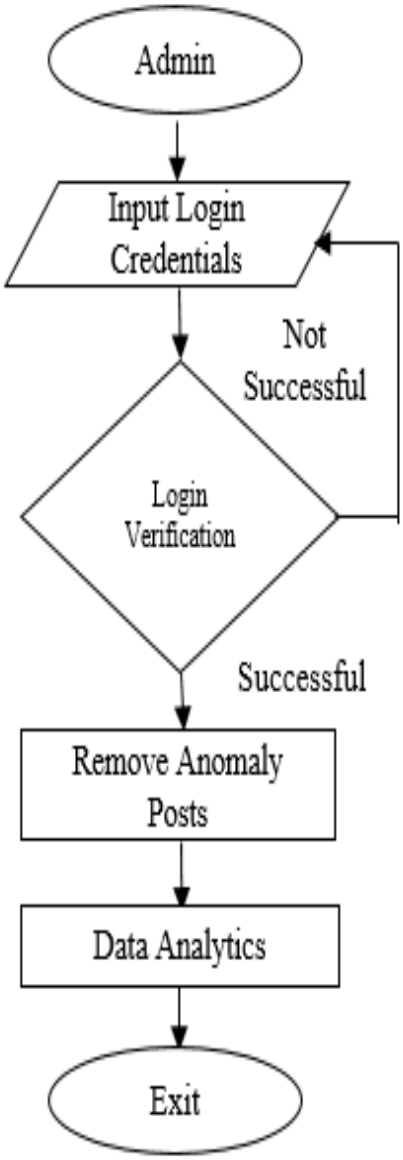

Figure 2: An Overview Architecture for admin actions

The system architecture for admin is as shown in Figure 2 and system architecture of proposed model for user is as shown in Figure 3. The system also allows users to categorize available tweets and view them through notepad. The users are provided with options of categorizing tweets and also an option to remove their anomaly tweets personally.

The system architecture shows the exact part at which the anomaly detection module is applied. The anomaly detection module is designed to handle both direct and mixed kind of tweets.

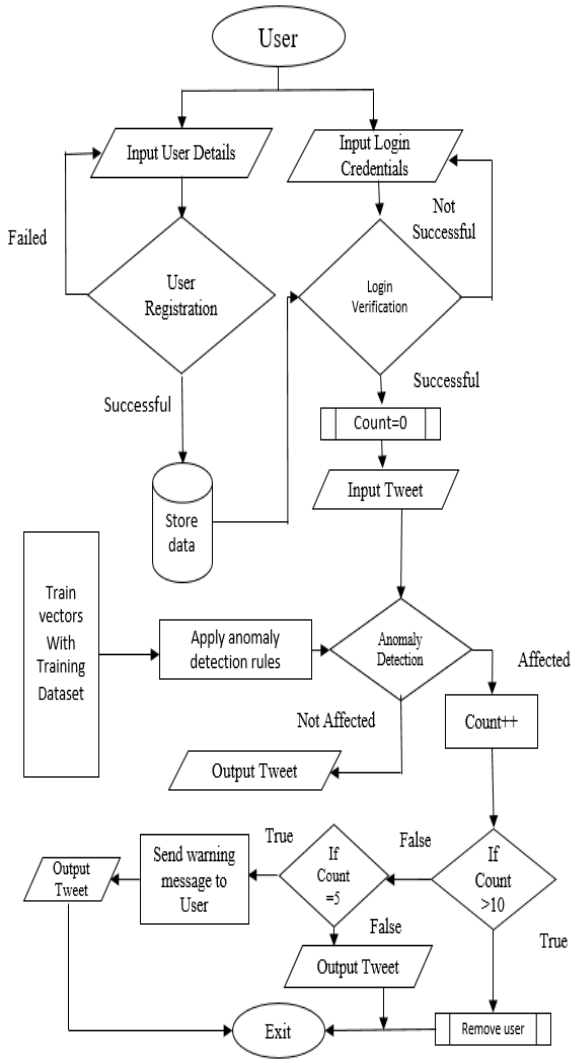

Figure 3: An Overview Architecture for Anomaly Detection.

V. ALGORITHM

The Anomaly check on the text can be determined using support vector machines. The anomaly in the text is distinguished in two ways as direct anomaly and mixed anomaly. When a person enters a comment or post in social media it is compared with vectors created using training data.

The proposed algorithm creates vectors (Hidden and visible) with the training data provided. The target class contains testing data in the form of posts. The training objective is created for the vectors created. The contents of the target class are made to pass through this objective function. As a result the vectors trained will check for the buzzwords in the testing data set to classify the testing posts as anomaly posts or not. In case of mixed posts the anomaly is identified using +, - properties of the trained vectors. In case of direct posts the anomaly is found by passing trained vectors and the test data into a objective function created for anomaly detection. The algorithm with input and output is mentioned below as stepwise

Algorithm: Anomaly text classification using support vector machine

Input: Training dataset with anomaly buzz words
Output: classification of testing text to be affected by anomaly or not
1: Load training dataset
2: Sample training vector from training dataset
3: Initialize weights W and bias a and b
4: Set m visible units (v)
5: Set n hidden units (h)
6: Compute conditional probability P for all v
7: Compute conditional probability P for all h using dropout
8: Initialize target class c = {c1, c2, · · ·, ct}
9: Set training objective
10: To deal with the computational problem, compute gradient of log P (ct, vt), i.e., ∂ log P (ct, vt)/$\partial\theta$
11: Repeat the procedure G times to classify all target class members
12: Return classified texts

VI. RESULT AND DISSCUSION

This algorithm helps in differentiating the text from the normal and anomaly text, which in turn will help in keeping the social network free from anomaly tweets. As said,this algorithm plays a major role in categorizing the text. The test text goes into the classification algorithm, according to the algorithm the result of the process is defined. The action on anomaly users are takes based on the value of the count variable. The result can be either be any of the 3 actions shown in Table 1. Figure 4 shows design of data analytics option provided to admin.

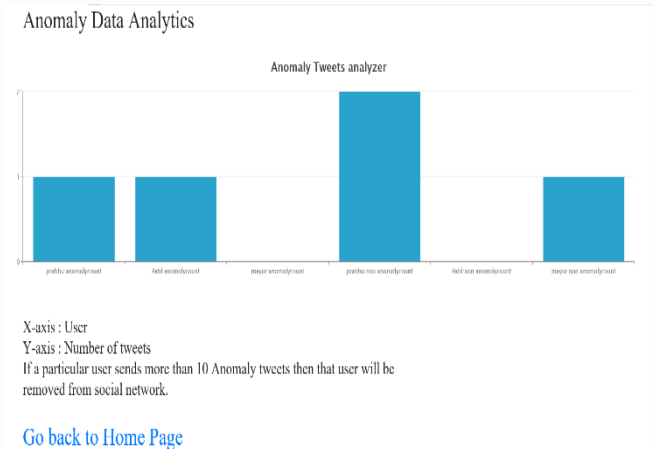

Figure4: overview of data analytics

Table 1:Action Table

Value of count variable	Action to be performed
count< 5	No action
Count=5	Send warning mail
Count>10	Remove user

VII. CONCLUSION AND FUTURE WORKS

In this paper, a vector-based anomaly detection model is proposed that accounts for efficient detection of anomalies in online social networks. The proposed model uses support vector machine and detect anomaly action as soon as performed (Live). Study results indicated that SVM based anomaly detection algorithm is efficient in identifying anomaly actions and the visualization is useful for analysts to discover insights and comprehend the model. The proposed approach uses simple algorithm even for identifying complex anomalies and mixed posts.

In the future, we will further investigate anomaly detection models for Twitter conversational threads and improve the current algorithm to allow a faster analysis. In addition to anomaly detection, it is interesting to integrate other content features (e.g., topics and semantic information) to the current system. Results suggest that the proposed model proves to be efficient and more accurate in comparison with the existing approaches over various parameters namely, anomaly filtering rate, accuracy in anomaly detection, convergence value, and approach failures.

ACKNOWLEDGMENT

Firstly, we express our sincere thanks to our guide Mrs. Mangala C N, Assoc. Professor, Department of CSE, EWIT for her guidance and support. We also like to thank Dr. Arun Biradar, Head, Department of computer science and engineering for his moral support. We express our sincere gratitude to our principal Dr. K Chennakeshavalu for his constant support and encouragement, we also thank all the faculties of East West Institute of Technology for their co-operation and support.

REFERENCES

[1] M Swarna sudha ,K Arun Priya,"Data mining approach for anomaly detection in social network analysis",2018,ICICCT conference 2018

[2] Z. Wang and Y. Parth, "Extreme Learning Machine for Multi-class Sentiment Classification of Tweets," Proc. ELM-2015, Springer Int. Publ. 2016, vol. 1, pp. 1–11, 2016.

[3] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," IEEE Transactions on Dependable andSecureComputing,vol.14,no.4,pp.447 – 460,2015.

[4] R. Yu, X. He, and Y. Liu, "Glad: group anomaly detection in social media analysis," ACM Transactions on Knowledge Discovery from Data, vol. 10, no. 2, pp. 18–22, 2015.

[5] Z. Wang, J. C. Tong, and D. Chan, "Issues of social data analytics with a new method for sentiment analysis of social media data," in 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, 2014, pp. 899–904.

[6]M.Egele,G. Stringhini, "Compa: Detecting compromised accounts on social networks," in NDSS, 2013,

[7] E. Haddi, X. Liu, and Y. Shi, "The role of text pre-processing in sentiment analysis," Procedia Computer Science, vol. 17, pp. 26-32, Jan.2013.

[8] P. Gonçalves and M. Araújo, "Comparing and combining sentiment analysis methods," Proc. first ACM Conf. Online Soc. networks. ACM, pp. 27–38, 2013.

[9] B. Yuan, Y. Liu, and H. Li, "Sentiment classification in Chinese microblogs:Lexicon-based and learning-based approaches," Int. Proc. Econ. Dev. Res., vol. 68, pp. 1–6, 2013

[10] J. Ortigosa-Hernández, J. D. Rodríguez, L. Alzate, M. Lucania, I. Inza, "Approaching sentiment analysis by using semisupervised learning of multi-dimensional classifiers," Neurocomputing, vol. 92, pp. 98-115, Sep. 2012.

[11] H. Ji, H. Deng, and J. Han, "Uncertainty reduction for knowledge discovery and information extraction on the World Wide Web," Proceedings of the IEEE, vol. 100, no. 9, pp. 2658-2674, Sep. 2012.

[12] T. Takahashi, R. Tomioka, and K. Yamanishi, "Discovering emerging topics in social streams via link anomaly detection,"2011 IEEE 11th International Conference on Data Mining, pp. 1230–1235, 2011.

[13] X. Glorot, A. Bordes, and Y. Bengio, "Domain adaptation for largescalesentiment classification: A deep learning approach," Proceedings of the 28th International Conference on Machine Learning

[14] B. Gokaraju, S. S. Durbha, R. L. King, S. Member, and N. H. Younan,"A machine learning based spatio-temporal data mining approach for
detection of harmful algal blooms in the Gulf of Mexico," IEEE Journal, vol.4, pp. 710-720, 2011.

[15] N. A. Heard, D. J. Weston, K. Platanioti, D. J. Hand, et al.,"Bayesian anomaly detection methods for social networks," ANNS, vol. 4, pp. 645–662, 2010.

[16] L. Akoglu, M. McGlohon, and C. Faloutsos, "Oddball: Spottinganomalies in weighted graphs," in Pacific-Asia Conference on KnowledgeDiscovery and Data Mining, pp. 410–421, 2010.

[17] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in 2010 IEEE Symposium on Security and Privacy, pp. 305–316, May 2010.

[18] T. Wilson, J. Wiebe, "Recognizing contextual polarity: An exploration of features for phrase-level sentiment analysis," ACL, vol. 35, no. 3, 2009.

[19] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: Theory and applications," Neurocomputing, vol. 70, no. 1–3, pp. 489– 501,Dec. 2006.

[20] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? sentiment classificationusing machine learning techniques," Proc. ACL-02 Conf. Empir. methods Nat. Lang. Process. Assoc. Comput. Linguist., vol. 10, pp. 79–86, 2002.

Authors Profile

[1] Mr. Mayur Jain is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Machine Learning, Big Data and Deep Learning.

[2] Mr. Prashanth A is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Machine Learning and Image processing.

[3] Mr. Prabhudev B K is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Big Data, Machine Learning and Image processing.

[4] Mr. Sagar Reddy N J is pursuing his 8 semester B.E in Computer Science & Engineering at East West Institute of Technology, Bengaluru, India. His area of interest includes Machine Learning and Image Processing.

[5] Mrs. Mangala C N received the B.E degree in Computer Science and Engineering from NCET, Bengaluru, VTU in2006 and got M.Tech degree in Computer Science from RVCE, Bengaluru, India. She is currently working as Associate Professor in the Department of CSE, EWIT, and pursuing PhD in DSCE, Bengaluru, India. Her area of interest includes Image Processing, Network Security, Data Mining and Big Data.

