

Recognize Fraud Accounts on Social Platform Using SVM and Neural Networks

Thepalle Reddeppa¹, Dr. J. Srinivasan²

¹PG Scholar, Department of Computer Application, Madanapalle Institute of Technology & Science, India

²Assistant Professor, Department of Computer Application, Madanapalle Institute of Technology & Science, India

ABSTRACT

Article Info

Publication Issue :

Volume 8, Issue 4

July-August-2022

Page Number : 256-259

Article History

Accepted: 10 August 2022

Published: 28 August 2022

The present generation, online social networks (OSNs) have become increasingly popular, people's social lives has become more associated with these sites. They use OSNs to keep in touch with each other's, share news, organize events, and even run their own e-business. The rabid growth of OSNs and the massive amount of personal data of its subscribers have attracted attackers, and imposters to steal personal data, share false news, and spread malicious activities. On the other hand researchers have started to investigate efficient techniques to detect abnormal activities and fake accounts relying on accounts features, and classification algorithms. However, some of the account's exploited features have negative contribution in the final results or have no impact, also using standalone classification algorithms does not always reach satisfied results. In this paper, a new algorithm, SVIn M-NN, is proposed to provide efficient detection for fake Instagram accounts, four feature selection and dimension reduction techniques were applied.

Keywords : Support Vector machine (SVM) and Neural network

I. INTRODUCTION

Online social network's(OSNs), such as Face book , Twitter, LinkedIn, Google+ have become increasingly popular over last few years .People use OSNs to keep in touch with each other, share news, organize events, and even run their own e-business. For the period between 2014 and 2018 around 2.53 million U.S. dollars have been spent on sponsoring political ads on Face book by non-profits. The open nature of OSNs

and the massive amount of personal data for its subscribers have made them vulnerable to Sybil attacks. In 2012, Face book noticed an abuse on their platform including publishing false news, hate speech, sensational and polarizing, and some others. In researchers have made a study to predict, analyze and explain customer's loyalty towards a social media-based online brand community, by identifying the most effective cognitive features that predict their customer's attitude.

II. LITERATURE REVIEW

SURVEY OF SUPPORT VECTOR MACHINE

R. Burbidge et. al., [31] have shown that the support vector machine (SVM) classification algorithm, proves its potential for structure–activity relationship analysis. In a benchmark test, they compared SVM with various machine learning techniques currently used in this field. Giorgio Valentini [32] have proposed classification methods, based on non-linear SVM with polynomial and Gaussian kernels, and output coding (OC), ensembles of learning machines to separate normal from malignant tissues, A training method to increase the efficiency of SVM has been presented by Yiqiang Zhan [34] for fast classification without system degradation. Yuchun Tang et. al., [35] have developed an innovative learning model called granular support vector machines for data classification problems by building just two information granules in the top-down way. Shutao Li et. al., [33] have applied SVMs by taking DWFT as input for classifying texture, using translation-invariant texture features. They used a fusion scheme based on simple voting among multiple SVMs, each with a different setting of the kernel parameter, Shu-Xin Du et. al., [38] have developed a Weighted support vector machines for classification where penalty of misclassification for each training sample is different. Kemal Polat [41] has developed a medical decision making system based on Least Square Support Vector Machine (LSSVM) which was applied on the task of diagnosing breast cancer and the most accurate learning methods was evaluated. Fabien Lauer et. al., [44] have proposed different formulations of the optimization problem along with support vector machines (SVMs) for classification task. They have exposed the utility of concerns on the incorporation of prior knowledge into SVMs in their review of the literature Urmil B. Parikh et. al., [47] have proposed a new SVM based fault classification algorithm for a series compensated transmission line , which uses samples of three phase currents as well as

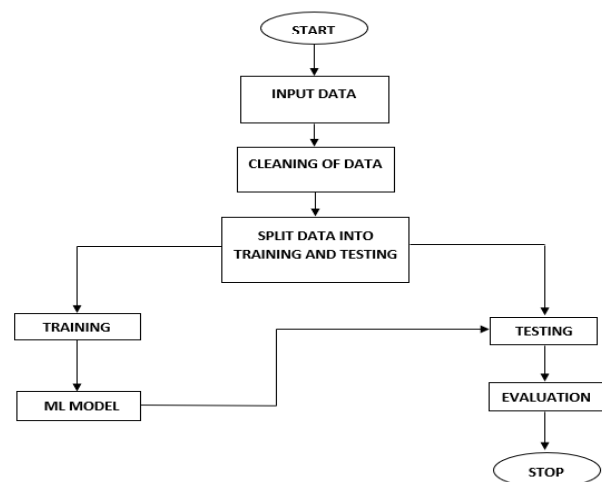
the zero sequence current as input features to the SVMs for identification of the faulted phase(s) Nahla Barakat et. al., [53] have reviewed on a historical perspective for the SVM area of research and conceptually groups and analyzes the various techniques. In particular, they have proposed two alternative groupings; E.A. Zanaty [60] have constructed SVMs and computed its accuracy in data classification.

III. PROPOSED SYSTEM

We propose this application that can be considered a useful system since it helps to reduce the limitations obtained from traditional and other existing methods. The objective of this study to develop fast and reliable method which detects sentiment accurately. To design this system is we used a powerful algorithm in a based Python environment.

ADVANTAGES:

Accuracy is good. Low complexity. Highly efficient. No need of skilled persons



IV. EXISTING METHOD

The increasing growth of machine learning, computer techniques divided into traditional methods and machine learning methods. This section describes the related works of sentimental analysis is detected and how machine learning methods are better than

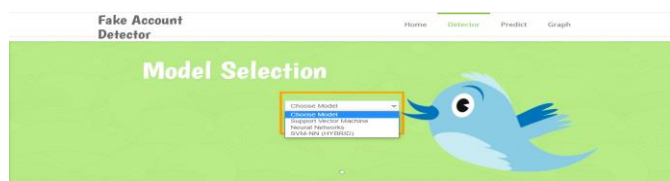
traditional methods. The existing method in this project have a certain flow and also normal sentimental analysis is used for development. But it requires large memory and result is not accurate.

DISADVANTAGES:

Low Accuracy .High complexity .Highly inefficient. Requires skilled persons

V. RESULT

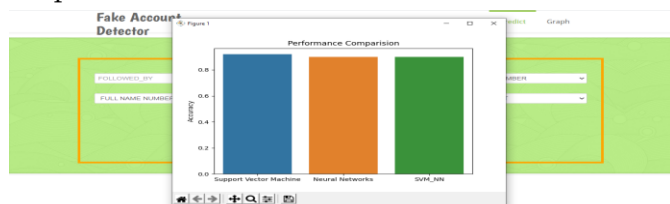
Model Selection:



OUTPUT:



Graph



VI. CONCLUSIONS AND FUTURE SCOPE

After proper analysis and comparison, it was found that Support Vector Machine reported the maximum accuracy .The accuracies for prediction could be further improved .Size of dataset changes in future (presently a constraint).Class Distribution of the target variable gets balanced. The ability to identify fake accounts in this application in the future. We

intend to investigate prediction approach with the revised data set and employ the most accurate and relevant machine learning algorithms for detection.

VII. REFERENCES

- [1]. (2018) Political advertising spending on Face book between 2014 and 2018. Internet draft. [Online]. Available: <https://www.statista.com/statistics/891327/political-advertising-spending-face-book-by-sponsor-category/>
- [2]. J. R. Douceur, "The Sybil attack," in International workshop on peer-to-peer systems. Springer, 2002, pp. 251–260.
- [3]. (2012) Cbc.facebook shares drop on news of fake accounts. Internet draft. [Online]. Available: <http://www.cbc.ca/news/technology/facebook-shares-drop-on-news-of-fake-accounts-1.1177067>
- [4]. R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216, 2016.
- [5]. L. M. Potgieter and R. Naidoo, "Factors explaining user loyalty in a social media-based brand community," South African Journal of Information Management, vol. 19, no. 1, pp. 1–9, 2017.
- [6]. (2018) Quarterly earning reports. Internet draft. [Online]. Available: <https://investor.fb.com/home/default.aspx>
- [7]. (2018) Statista.twitter: number of monthly active users 2010-2018. Internet draft. [Online]. Available: <https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/>
- [8]. Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake accounts by predicting their victims," in Proceedings of the

8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015, pp. 81–89.

- [9]. (2018) Facebook publishes enforcement numbers for the first time. Internet draft. [Online]. Available: <https://newsroom.fb.com/news/2018/05/enforcement-numbers/>
- [10]. (2013) Banque populaire dis-moi combien damis tu as sur facebook, je te dirai si ta banque va raccorder un prt. Internet draft. [Online]. Available: <http://bigbrowser.blog.lemonde.fr/2013/09/19/popularitedis-moi-combien-damis-tu-as-sur-facebook-je-te-dirai-si-ta-banqueva-taccorder-un-pret/>
- [11]. S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 New Security Paradigms Workshop. ACM, 2010, pp. 61–72.
- [12]. S. Fong, Y. Zhuang, and J. He, "Not every friend on a social network can be trusted: Classifying imposters using decision trees," in Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012, pp. 58–63.
- [13]. K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: an analysis of twitter spam," in Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, 2011, pp. 243–258.
- [14]. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th annual computer security applications conference. ACM, 2011, pp. 93–102.
- [15]. J. Ratkiewicz, M. Conover, M. Meiss, B. Goncalves, S. Patil, A. Flammini, and F. Menczer, "Truthy: mapping the spread of astroturf in microblog streams," in Proceedings

of the 20th international conference companion on World wide web. ACM, 2011, pp. 249–252.

Cite this article as :

Thepalle Reddeppa, Dr. J. Srinivasan, "Recognize Fraud Accounts on Social Platform Using SVM and Neural Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 4, pp. 256-259, July-August 2022.

Journal URL : <https://ijsrcseit.com/CSEIT228444>