Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018)
IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3

MACHINE LEARNING BASED TWITTER SPAM ACCOUNT DETECTION: A REVIEW

Shivangi Gheewala
M.E. Student, Department of Computer Engineering,
Sarvajanik College of Engineering and Technology,
Surat, India.
shivangigheewala08@gmail.com

Rakesh Patel
Assistant Professor, Department of Computer Engineering,
Sarvajanik College of Engineering and Technology,
Surat, India.
rakesh.patelco@scet.ac.in

Abstract*—Online social networks (OSNs) are emerging communication medium for people to establish and manage social relationships. In OSNs, regularly billions of users are involved in social interaction, content and opinion dissemination, networking, recommendations, scouting, alerting, and social campaigns. The popularization of OSNs open up a new perspectives and challenges to the study of social networks, being of interest to many fields. Social network is a place where social activities, business oriented activities, entertainment, and information are exchanged. It establish a worldwide connectivity environment where communities of people share their interests and activities, or who are interested in interests and activities of others Although social network has given immense benefits to people at the same time harming people with various mischievous activities that take place on social platforms. This causes significant economic loss to our society and even threaten the national security. All the social networks Facebook, Twitter, LinkedIn, etc. are highly susceptible to malware activities. Twitter is one of the biggest microblogging networking platform, it has more than half a billion tweets are posted every day in average by millions of users on Twitter. Such a versatility and wide spread of use, Twitter easily get intruded with malicious activities. Malicious activities includes malware intrusion, spam distribution, social attacks, etc. Spammers use social engineering attack strategy to send spam tweets, spam URLs, etc. This made twitter an ideal arena for proliferation of anomalous spam accounts. The impact stimulates researchers to develop a model that analyze, detects and recovers from defamatory actions in twitter. Twitter network is inundated with tens of millions of fake spam profiles which may jeopardize the normal user's security and privacy. To improve real users safety and identification of spam profiles become key parts of the research.

Keywords*—social networks, micro-blogging twitter, spam profile, classification, spam drift, early detection, machine learning, spammer's evasion and spam URLs.

I. INTRODUCTION

The term Online Social Network has emerged from different interdisciplinary fields. Field of social, psychology, sociology, statistics and graph theory represent social network structure that consist of set of individuals or organizations with various interactions or relationships among them [1]. Online Social Networks are deemed to be most sought after social tool used by masses over the world [2] to share common interest and to communicate with each other. Social sites started with six degrees.com in 1997 [3] but could not survive much and disappeared very soon but new sites Myspace, Twitter, Facebook, LinkedIn, etc. became successful. All over the world millions of users involved with these social networks. The popularity of social sites is shown in Fig. 1. Dependency of people visiting social sites for seeking relevant news and to build social and professional relations is increasing.

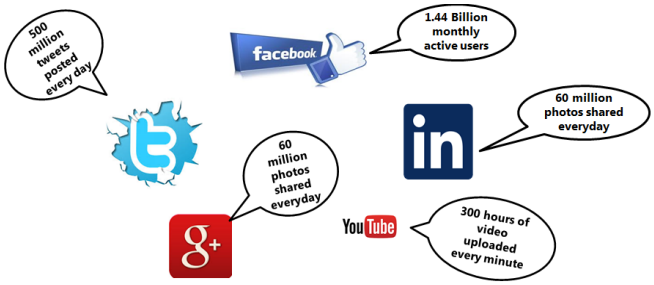

Fig. 1. Popular Social Sites

It is true that though OSN have become useful platform for multiple users at that same time it exploits users by spreading misinformation, spam links, unsolicited messages, creation of fake accounts, etc. Intruders, phishers, spammers, scammer's crop the social networks all the time and forcefully corrupt the OSNs with spamming activities. Such activities on social networks not only degrades the OSN reputation but also disturbs the genuine users can also be called as non-spammers. Twitter is viewed as one of the most prevalent and sought after online website utilized for microblogging [2]. Twitter attracts users by providing free microblogging services. Microblogging services includes broadcasting or discovering 140 characters messages, follow other users, enabling posting of videos, images, etc. Every month over 42 million of new accounts are created in Twitter [36]. Twitter as most prominent OSN is continuously under attack by spammers. Spammer is a person that perform scamming activities over the internet and tries to corrupt the social networks.

Various work have been done on spam detection in Twitter. Initially research started with building spam filter model to filter spam coming from different URL links. However, spammer change their way and take a visit from another URL before he get trapped under spam filter model. The failure of spam filtering model encourage researchers to find another way of detecting spam. Researchers have look

for a way of adopting (ML) Machine Learning concept in spam detection. Machine Learning is a rising field of computer science. Machine learning gives any application model the ability to learn and make prediction. With machine learning algorithms classification, clustering, regression, visualization, data processing and feature selection tasks can be carried out. Spam Detection framework is a binary classification problem. A framework that classifies Twitter account as spam or non-spam. To make binary classification in spam detection, researches have moved their contrivance towards machine learning technique. A machine learning spam account detection model commonly comprises of two phases mentioned below:

- Training phase: It is a first phase in which detection model is trained using classified labelled samples.
- Testing phase: It is follow up of training phase. Unlabeled samples are tested and generate the results by classifying each sample into spam or non-spam class.

Since many years machine learning is overruling in various study related to online social network spam or spammer or spam account detection. Researchers have used different strategies in modelling spam detection system with embracement of machine learning concept. While researchers are working to detect spam, spammers are trying to avoid being detected [42]. Researchers are still struggling in achieving 100% accurate detection system that guarantees to make twitter a complete spam free platform. But problem is that spammer still look for a way [4] to evade researcher's method by generating new evasion tactics. Researchers also observed among all social networks Twitter network is more prone to spammers invasions. Day by day creation of spam accounts on Twitter increases. Looking to the undesirable scenario, various study focuses on developing machine learning based an efficient model that detects spam accounts in Twitter. Detection system not only classify the account as spam or non-spam but also enhance the privacy and provide security for non-spam users in Twitter.

The paper is structured as follows: Section II gives an overview of previous related work on spam detection in Twitter, in Section III a brief explanation of Twitter spam account detection based on machine learning approach. Section IV is an analysis of different machine learning techniques for spam profile detection. Section V reveals the motivation behind a review study Section VI presents the closure of study in the form of conclusion. Finally paper gives an end with list of references.

II. RELATED WORK

Detection of spam accounts in Twitter involves detection of twitter spam, spammers or spam URLS, spam content, spam tweets, etc. Consequently security companies as well as Twitter itself are combating spammers to make Twitter as spam free platform [4]. In early work a security company Trend Micro uses a blacklisting service called (WRT) Web Reputation Technology system to filter spam URLs for users who have its products installed [31]. Twitter has also implemented blacklist filtering as a component called Bot Maker in their detection system [32]. Researcher's show that more than 90 percent spammers may visit with new spam link before it is blocked by blacklists [33]. This traditional blacklist technology got failed to protect victims from spam accounts due to time lagging [34]. Even heuristic rules have been used to filter Twitter spam [4]. In order to address limitation of traditional work, researchers have come up with new methodology termed as machine learning spam detection.

Currently number of research studies apply machine learning algorithms for detection of Twitter spamming accounts. Machine learning techniques categorized spam detection into detection based on syntax analysis and detection based on feature analysis shown in Fig. 2.

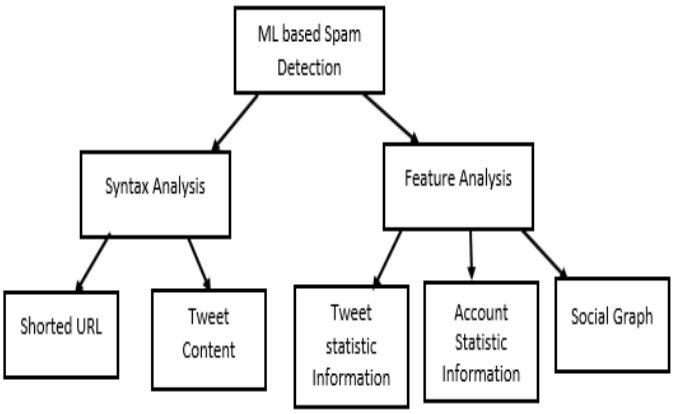

Fig. 1. Machine Learning based Spam Detection Techniques [37]

Feature analysis based spam detection make the use of Twitter statistical features for spam account detection. There are different types of statistical features ingested into machine learning model for binary classification. Twitter features are shown in Fig. 3. Statistical features include type one and type two features. Type one feature is account or content based features such as account number, number of URLs in tweet, number of characters in tweet, profile picture, number of followers and followings, etc. Benevenuto et al. have considered user and content based features and proposed non-linear (SVM) Support Vector machine classifier to distinguish spammers and non-spammers [36]. A. H. Wang has applied Bayesian classification algorithm and considered content based features to distinguish suspicious behaviors from normal users. Type one feature can be easily fabricated by spammers. Feature fabrication relates posting more tweets, purchasing more followers, etc. To avoid feature fabrication researchers have implemented spam detection work with more robust second type of feature i.e., graph based features. Some graph based features are Local clustering coefficient, Betweenness centrality, Bidirectional Link's ratio, etc. In graph based method, social network is modelled as graph and this graph is used to identify spam account in Twitter. A graph is normally represented as G = (V, E) where V is a set of vertices denotes individual user who has created account in Twitter. E is a set of edges represent connection or relation between two accounts. Social graph can be categorized into static, dynamic labelled or unlabeled [35]. Static graph neglects time while

individual nodes make interaction on network. Dynamic network consider the time that changes with the changes in pattern of interactions. In labelled graph, considers node attributes say name, age, number of tweets, etc. along with nodes and edges. While in unlabeled graph node attributes are not considered. C. Yang et al. make the comprehensive and empirical analysis of spammer's tactics. Further extracted and analyzed robustness of 24 detection features. Then applied these 24 features on machine learning classifier such as Random Forest, Decision Tree, BayesNet and Decorate to detect spammers [25]. Some of the limitation with graph based method is that it is very difficult and cumbersome approach to model social network into graph. Graph based feature extraction is expensive and time consuming. A wrongly modeled graph may lead to an inappropriate detection.

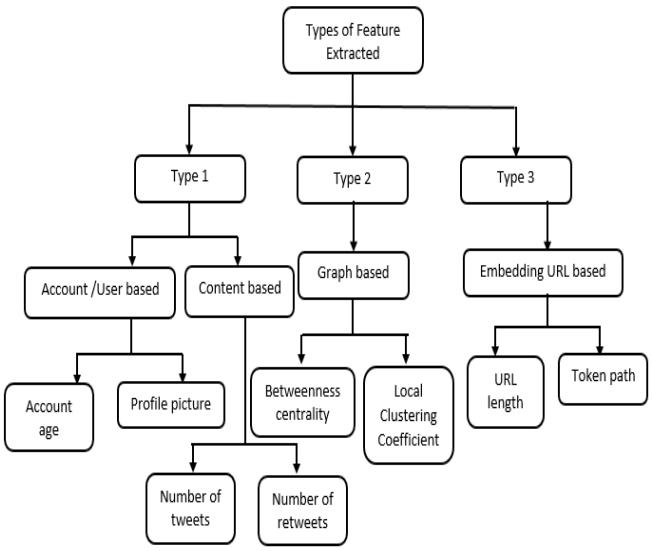

Fig. 3. Types of Twitter Features

During the period of spam detection, it is been observed most of the time spammer spread spam using URL links. Thus third type of feature is embedded URLs based features shown in Fig. 3. This type of feature comes under syntax analysis. Syntax analysis based spam detection make the use of Twitter non-statistical features for classification. Detection of Twitter spam accounts using syntax analysis is very limited. There are some works focusing on inspecting shortened URLs inside tweets. It analyze tweets at character or word level [37]. Shortened URLs can be generated by inputting short links embedding inside long URLs by spammers to hide their malicious URLs [37].While it is possible to send spam without embedding URLs on Twitter, majority of spam contains URLs [4]. URL based features include URL redirect chain length, query parameters of URL, relative number different initial URLs, etc. S. Lee and J. Kim proposed a new suspicious URL detection system for Twitter. Firstly investigated correlations of URL chains extracted from twitter tweets. Used LIBLINEAR library to implement LR based algorithms. It supports the real time detection concept and classifier detects suspicious URLs accurately and efficiently [40]. URL based features also showed their discriminative power when used for classifying spam [4]. Not all features are useful for analysis. Based on impact of features on spam detection model, features are selected.

III. TWITTER SPAM ACCOUNT DETECTION USING MACHINE LEARNING

Concept of machine learning is adapted while building spam account detection model. Machine learning framework mainly consist of two phases i.e., training and testing phases. A basic working of Twitter spam account detection system is shown in Fig. 4.

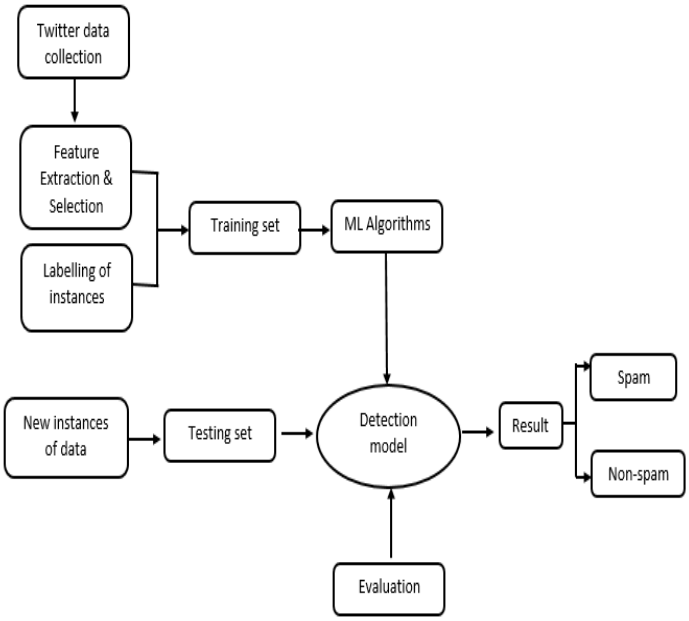

Fig. 4. A framework of Machine Learning based Spam Account Detection

A detailed explanation of above flowchart is given below:

- Initiate with gathering Twitter data. Either crawl the Twitter streaming API to collect the data or use publically available data for research purpose.
- Then next step is extraction of features from dataset. Various type of features mentioned in Fig. 3. can be used in spam account detection. Not all features are useful. Some of the features are selected from the list of extracted features. Features that shows more effectiveness in yielding correct result are selected for spam account detection.
- Then small set of samples are labelled for training purpose with class spam or non-spam. Labelling is done either manually or using spam filtering services. Spam filtering services allow those instances who is spam free hence label instances as non-spam and block those instances who is spam effective hence label instances as spam.
- Machine Learning based detection models are trained with labeled samples and then tested to identify class of particular data instance.

- Finally detection models are evaluated with evaluation parameters like accuracy, detection rate, true positive, false negative, recall, precision, f-measures, etc.

Within the field of data analytics, machine learning is a method used to devise complex models and algorithms that lend themselves to prediction. Accuracy of prediction depends on performance of detection model. In spam account detection system, detection model is nothing but a classifier or assemble of classifiers. These classifiers are built using data mining algorithms say SVM (Support Vector Machine), Decision tree based algorithms, Boosting algorithms, Bayesian algorithms, Neural network based algorithms, Clustering algorithms, etc. Performance of detection model in turn depends upon proper selection of features, number of labelled instances and stability of data mining algorithms. From past research work, detection model is built using clustering, classification or combined algorithms as shown in Fig. 5. for Twitter spam detection. Here presenting a brief summary of different strategies used to develop spam or spam account detection model.

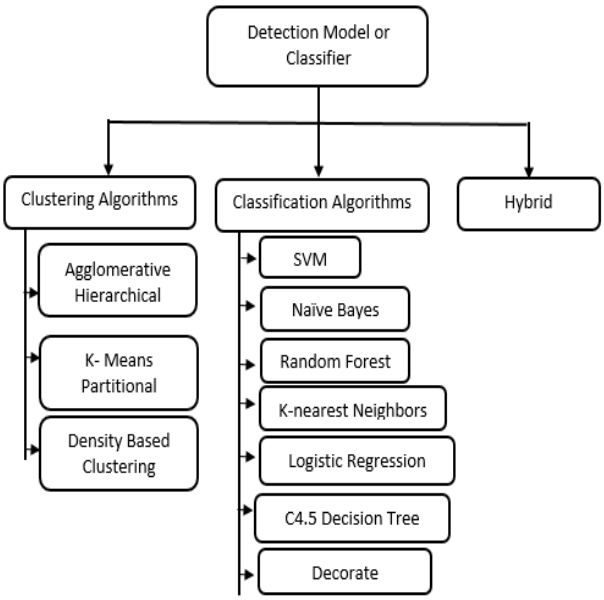

Fig. 5. Data Mining Algorithms for Spam detection model

IV. EXISTING MACHINE LEARNING BASED LITERATURE SURVEY

In various direction work has been done in detecting spam and spam profiles in Twitter or other social networks. Contribution in each spam detection research follow same manner as mentioned in following statements. Either create their own dataset or used publically available dataset for spam or non- spam classification [10]. Each paper gives a deep analysis on different kind of extraction of features. Proper selection of features creates a great impact on detection model and increase the performance of detection model. A deep analysis on proper picking up of classifier that fits the detection criteria and yield higher throughput. Table 1 shows various past research on spam detection in social networks especially in Twitter network.

Table I. Analysis on diffternt methods for Spam Profile Detection

No.	Title/ Author/ Publication	Category	Feature Extracted	Classifier	Result
1	Detecting Spam Tweets in Twitter Using a Data Stream Clustering Algorithm [7] **Authors**: N. Eshraqi, M. Jalali and M. H. Moattar **Publication** IEEE, 2015.	Clustering	Graph based, content based and time based	Den stream algorithm	Cluster data are centralized around the core and dispersion is low thus cluster process has been done with high quality result into minimum value of FPR and 89% of spam detection.
2	Detecting spammers on twitter [36] **Authors:** F. Benevenuto , G. Magno, T. Rodrigues and V. Almeida **Publication** Colla-boration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS), 2010.	Classi-fication	User and content based	Non-linear SVM classifier	Result shows about 70% of spammers and 96% of non-spammers classified correctly.
3	A Hybrid Approach for Spam Detection for Twitter [10] **Authors:** M. Mateen, M. Aleem, M. A. Iqbal and M. A. Islam **Publication** *IEEE*, 2017.	Classi-fication	content based, user based as well as graph based features	J48, Decorate and Naïve Bayes	Detection rate of hybrid technique is much higher than other previously existing techniques.
4	Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers [25] **Authors:** C. Yang, R. Harkreader	Classi-fication	Profile based, Content based, Graph based, Neighbor based, Timing based and Auto-mation	RF, Decision tree, Naïve Bayes and Decorate	On lowering false positive ratio, the detection rate is found to be significantly higher than existing work using new robust features.

	and G. Gu. **Publication** IEEE, 2013.		based		
5	Don't Follow Me Spam Detection in Twitter [38] **Authors:** A. H. Wang **Publication** IEEE, 2010.	Classi-fication	Graph based and content based	Bayesian classi-fication	Compared the result of Bayesian algorithm with SVM, neural network, decision tree and KNN. Result shows spam detection system achieved 89% precision.
6	Click Traffic Analysis of Short URL Spam on Twitter [41] **Authors:** D. Wang, B. N. Shamkant, L. Liu, D. Irani, A. Tamersoy and C. Pu **Publication** IEEE, 2013.	Classi-fication	Short URLs	Random Forest, Decision Table, Random Tree, K*, SMO, Simple Logistic, and Decision Tree	Random Tree algorithm achieved the best performance with an accuracy of 90.81% and an F1measure value of 0.913.
7	Statistical Features-Based Real-Time Detection of Drifted Twitter Spam [4] **Authors:** C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou and G. Min. **Publication** IEEE Transactions, April 2017.	Classification	Account and content based statistical features	Random Forest	Lfun can effectively detect Twitter spam by reducing the impact of "Spam Drift" issue.
8	Detecting malicious Tweets in Trending Topics using Clustering and Classification [6] **Authors**: S. J. Soman and S. Murugappan **Publication** IEEE, 2014	Hybrid	Profile based, activity based, location based and text/content based	Fuzzy k-means clustering algorithm and Extreme Learning Machine (ELM). Classifier	Proposed ELM classification method provides better spam detection rate with significant accuracy than Support Vector Machine spam detection result.

V. MOTIVATION

Due to ease of sharing information, to gain sync with regular updates of current trend and to attain socio relationship in Twitter, daily billions of users remain active. Such popularity of twitter have become a target for spammers. Differentiating spam accounts from non-spam accounts is day by day getting difficult, as spammers behave intelligently and are very well aware of detection techniques. This helps spammers to easily evade available detection schemes. Detecting such spam accounts has become essential in order not to degrade value of Twitter network and to keep network secure and private from malicious users. The longer time a spam activity exists, the more chance it can be exposure to victims [4]. Thus it is very important to detect and report spam activity in turn spamming accounts to victims as early as possible. This motivates to propose an efficient method that detects spam accounts in early time.

VI. CONCLUSION

The continuous increase in the volume of social network data has contributed to the growth in spamming accounts. Due to openness, the ability to influence featured taglines, inflate profiles has made Twitter an attractive platform to marketers and deceivers who commonly employ spam accounts to achieve their goals. To reduce the effect of spam accounts on real user, spammer evasion tactics are to be analysed and effort is required to develop a productive system that detects spam accounts on Twitter and prevent real users from getting attacked by spammers. A profound survey has been carried out in this paper. Each study have utilized different types of Twitter features, different types of classifiers and different roadway in spam detection. It has been observed machine learning based classifiers yields good results. But some of the issues like class imbalance, spam drift problem, feature fabrication, etc. for spam detection have lowered the result. Lowering the overall performance of the detection system. Thus nowadays research has started to work on solving the above mentioned issues in order to achieve satisfactory results.

REFERENCES

[1] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan and S. A. Razak, "Malicious accounts: Dark of the social networks", *Elsevier*, 2017, pp. 41-67.

[2] A. Gupta and R. Kaushal, "Improving Spam Detection in Online Social Networks", *IEEE,* 2015.

[3] M. Verma, Divya, S. Sofat, "Techniques to Detect Spammers in Twitter – A Survey", *International Journal of Computer Applications,* January 2014, Vol. 85, No. 10, pp. 27-32.

[4] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou and G. Min, "Statistical Features- Based Real- Time Detection of Drifted Twitter Spam", *IEEE Transactions*, April 2017, pp.914-925.

[5] W. Hua and Y. Zhang, "Threshold and Associative Based Classification for Social Spam Profile Detection on Twitter", *9th International Conference on Semantics, Knowledge and Grids,* 2013, pp. 113-120.

[6] S. J. Soman and S. Murugappan, "Detecting Malicious Tweets in Trending Topics using Clustering and Classification", *IEEE*, 2014.

[7] N. Eshraqi, M. Jalali and M. H. Moattar, "Detecting Spam Tweets in Twitter Using a Data Stream Clustering Algorithm", *IEEE*, 2015, pp. 347-351.

[8] A. Almaatouq, E. Shmueli, M. Nouh, A. Alabdulkareem, V. K. Singh, M. Alsaleh, A. Alarifi, A. Alfaris, A. S. Pentland, "It is looks like a

spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts", *Springer*, 2016, pp. 475-491.

[9] C. Meda, E. Ragusa, C. Gianologio, R. Zunino, A. Ottaviano, E. Scillia and R. Surlinelli, "Spam Detection of Twitter Traffic: A Framework based on Random Forests and non-uniform feature sampling", *IEEE*, 2016, pp. 811-817.

[10] M. Mateen, M. Aleem, M. A. Iqbal and M. A. Islam, "A Hybrid Approach for Spam Detection for Twitter", *IEEE*, 2017, pp. 466-471.

[11] A. Zoubi, J. Alqatawna and H. Faris, "Spam Profile Detection in Social Networks Based on Public Features", *IEEE*, 2017, pp. 130-135.

[12] D. Ramalingam and V. Chinnaiah, "Fake profile detection techniques in large-scale online social networks: A comprehensive review", *ELSEVIER*, 2017, pp. 1-13.

[13] Dr. M. Nandhini and Bikram Bikash Das, "An Assessment and Methodology for Fraud Detection in Online Social Network", *IEEE,* 2016, pp. 104-108.

[14] M. Torky, A. Meligy and H. Ibrahim, "Recognizing Fake Identities In Online Social Networks Based on a Finite Automaton Approach", *IEEE*, 2016, pp. 1-7.

[15] B. Mutlu, M. Mutlu, K. Oztoprak and E. Dogdu, "Identifying Trolls and Determining Terror Awareness Level in Social Networks Using a Scalable Framework", *IEEE*, 2016, pp. 1792-1798.

[16] I. David, O. S. Siordia and D. Moctezuma, "Features combination for the detection of malicious Twitter accounts", *IEEE*, 2016.

[17] Dr. M. Nandhini and B. B. Das, "Profile Similarity Technique for Detection of Duplicate Profiles in Online Social Network", *International Journal of Computer Science and Information Technology*, 2016, Vol. 7, No. 2, pp. 507-512.

[18] C. Xiao, D. M. Freeman and T. Hwa, "Detecting Clusters of Fake Accounts in Online Social Networks", *ACM*, 2015, pp. 91-101.

[19] S. Cresci, R. D. Pietro, M. Petrochhi, A. Spognardi and M. Tesconi, "Fame for sale: Efficient detection of fake Twitter followers", *Elsevier*, 2015, pp. 56-71.

[20] P. Garcia, J. Puerta, C. Gomez, I. Santoz and P. Bringas, "Supervised Machine Learning for the Detection of Troll Profiles in Twitter Social Network", *Springer,* 2014, pp. 419-428.

[21] M. Fire, D. Kagan and A. Elyashar, "Friend or Foe? Fake profile identification in online social networks", *Springer*, May 2014, pp. 1-23.

[22] S. Lee and J. Kim, "Early filtering of ephemeral malicious accounts on Twitter", *Elsevier*, 2014, pp. 48-57.

[23] S. Kiruthiga, P. Sujatha and A. Kannan, "Detecting Cloning attack in Social Networks Using Classification and Clustering Techniques", *IEEE*, 2014.

[24] M. Alsaleh, A. Alarifi, A. Salman, M. AlFayez and A. Almuhaysin, "TSD: Detecting Sybil Accounts in Twitter", *IEEE*, 2014, pp. 463-469.

[25] C. Yang, R. Harkreader and G. Gu, "Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers", *IEEE*, 2013, pp. 1280-1293.

[26] K. Gani, H. Hacid and R. Skraba, "Towards Multiple Identity Detection in Social Networks", *ACM,* April 2012, pp. 503-504.

[27] M. Conti, R. Poovendran and M. Secchiero, "FakeBook: Detecting Fake Profiles in On-Line Social Networks", *IEEE*, 2012, pp. 1071-1078.

[28] J. Jiang, Z. Shan, W. Sha, X. Wang and Y. Dai, "Detecting and Validating Sybil Groups in the Wild", *IEEE*, 2012, pp. 127-132.

[29] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Zhao and Y. Dai, "Uncovering Social Network Sybils in the Wild", *ACM*, November 2011.

[30] B. Viswanath, A. Post, K. Gummadi and A. Mislove, "An Analysis of Social Network-Based Sybil Defenses", *ACM*, 2010, pp. 363-374.

[31] J. Oliver, P. Pajeras, C. Ke, C. Chen and Y. Xiang, "An in-depth analysis of abuse on twitter", *Trend Micro, Irving, Tx, USA, Tech. Rep.*, September 2014.

[32] R. Jeyaraman, "Fighting Spam with Botmaker, Twitter", 2015.

[33] K. Thomas, C. Grier, D. Song and V. Paxson, "Suspended accounts in retrospect: An analysis of twitter spam" in *Proc. ACM SIGCOMM Conf. Internet Meas. Cof*., 2011, pp. 243-258.

[34] C. Grier, K. Thomas, V. Paxson and M. Zhang, "@spam: The underground on 140 characters or less", in *Proc. 17th ACM Conference*, 2010, pp. 27-37.

[35] D. Savage, X. Zhang, X. Yu, P. Chou and Q. Wang, "Anomaly detection in Online Social Networks", *Social Network. 39*, pp. 62-70.

[36] F. Benevenuto, G. Magno, T. Rodrigues and V. Almeida, "Detecting spammers on twitter", *Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS),* 2010.

[37] W. Tingmin, W. Sheng, Liu. Shigang, J. Zhang, Yang Xiang, M. Alrubaian and M. M. Hassan, "Detecting spam activities in twitter based on deep learning technique", *High performance and security in cloud computing: Editorial: High Performance and Security in Cloud Computing*, 2017, pp. 1-11.

[38] A. H. Wang, "Don't Follow Me Spam Detection in Twitter", *IEEE*, 2010.

[39] S. Liu, J. Zhang and Y. Xiang, "Statistical Detection of Online Drifting Spam", *ACM*, 2016, pp. 1-10.

[40] S. Lee and J. Kim, "Warning Bird: A near Real-Time Detection System for suspicious URLs in twitter stream", *IEEE Transactions*, 2013, pp. 183-195.

[41] D. Wang, B. N. Shamkant, L. Liu, D. Irani, A. Tamersoy and C. Pu, "Click Traffic Analysis of Short URL Spam on Twitter", *IEEE*, 2013, pp. 250-259.

[42] C. Chen, J. Zhang, Y. Xiang and W. Zhou, "Asymmetric Self-Learning for Tackling Twitter Spam Drift", *IEEE*, 2015, pp. 208-213.

[43] C. Meda, F. Bisio, P. Gastaldo and R. Zunino, "A Machine Learning Approach for Twitter Spammers Detection", *IEEE*, 2014.

[44] E. I. Setiawan, C. P. Susanto, S. Sumpeno and M. H. Purnomo, "Preliminary Study of Spam Profile Detection for Social Media using Markov Clustering: Case Study on Javanese People", *IEEE*, 2016.