Spam Detection in Social Media Networking Sites using Ensemble Methodology with Cross Validation

K Subba Reddy, E. Srinivasa Reddy

Abstract— Social media networking sites are more popular over Internet. The Internet users spend more amount of time on social media sites like Twitter, Facebook, Instagram and LinkedIn etc. The social media networking users share their ideas, opinions, information and make new friends. Social networking sites provide large amount of valuable information to the users. This large amount of information in social media attracts spammers to misuse information. These spammers create fake accounts and spread irrelevant information to the genuine users. The spam message information may be advertisements, malicious links to disturb the natural users. This spam data in social media is a very serious problem. Spam detection in social media networking sites is critical process. To extract spam messages in social media various spam detection methodologies are developed by researchers. In this paper we proposed an ensemble methodology for identification spam on Twitter social media network. In this methodology we used Decision tree induction algorithm, Naïve bayes algorithm and KNN algorithm to construct a model. As part of this approach, we compare the classification results of any two classification algorithms, if both classifiers predict the same result, then we finalize the class of tweet under investigation. If the predicted classes of both classification algorithms differ, then we use the prediction of third algorithm as the final class label of tweet. To measure the performance of our model we used precision, recall and F measure.

Keywords: Social media, Twitter, Naïve bayes, Decision Tree, KNN algorithm.

I. INTRODUCTION

In recent day's social media networking sites such as Facebook, Twitter have been gaining more popularity. Twitter is one of most familiar, popular and largest networking site compare to other social Medias. These social media networks attract million users and they are becoming an important medium of communication [1]. Social media sites are basically Internet based tools for sharing and discussing ideas and views. In social networking sites users can share photos, images, videos and establish communication between users [2]. Twitter is largest and popular networking site, that has been allows users to post latest news and messages. The size of the posted message is 280 characters, such messages are called tweets.

To give feedback and reviews on products, these sites can act as best platform for users. 0.13% of messages advertised on Twitter are clicked, whenever media users click on these links they accessed into spam data [3]. Twitter allows the users to follow their favorite scientists, business people and other familiar persons.

Revised Manuscript Received on February 10, 2020.
K Subba Reddy, Research Scholar, Anucet, ANU, Guntur, AP, India.
Dr. E. Srinivasa Reddy, Dean, Anucet, ANU, Guntur, AP, India

Generally a user can create own account in Twitter network openly without any restrictions, simply providing personnel details. Due to this open accessing policy into Twitter network many users misuse the network activities. Huge user base Twitter network has made main target for cybercriminals and social bots. The social bots can act as normal users to get trust in a network. Once users get faith on these bots and then these bots are used for malicious activities [4]. Spammers can mislead the normal users using retweets, hash tags and url links. Spam is biggest problem in social media sites like Twitter, Facebook etc. various researchers shows that 3% of tweets are spam messages. The spammers can capture the trending news and can create fake accounts to access genuine users and lead them. Some of the social media challenges are finding suspicious contents, messages posted by users and study the behavior of users and characteristics in social media [5].

To handle attacks from spammers Twitter provides different ways to report the spam. A user can report the spam by clicking a link in their home page. The network user given reports are analyzed by Twitter and the spam accounts are being suspended. Twitter network puts its efforts in efficient manner to disclose the malicious tweets and suspicious accounts. At filtering malicious tweets and suspicious accounts, some of the genuine user accounts are filtered out by Twitter. So we need some of efficient methods to automatically detect spam messages and spammer accounts. In meanwhile these advanced methodologies are not affect the legitimate user tweets.

In this work we proposed a methodology to detect spam messages. In this work we used Twitter data set. The collected data set is processed to obtain normal set of data. The features extracted were content based and user based features. With these features we construct a model using Decision tree classifier, Naïve bayes classifier, and KNN classifier. In section 2, presents some spam detection methodologies done by various researchers, section 3 describes our proposed methodology to detect spam. In section 4 and 5 we describe experimental results and future work.

II. RELATED WORK

The spam detection issue in social networking sites is very critical task. The researchers are very much interested to do their research work on these spam detection areas. Many researchers have concentrated to find efficient methods to identify spam. This section summarizes the major contribution of various researchers on spam detection in various social networking sites. Benjamin Markines et. al [6] describes a spam message detection approach with supervised learning algorithms.

With these algorithms the spam detection model is constructed using six different features such as TagSpam, TagBlur, DomFp, Numads, Plagiarism, ValidLinks. Kyumin Lee et. al [7] proposed a spam message detection approach using honeypots and SVM machine learning algorithm. Xin Jin et. al [8] used GAD clustering algorithm to detect spammers in social networking sites. This methodology deal with scalability and real time spam detection challenges in social media networking sites. Xueying et. al [9] describes a spam data detection procedure to classify the social media networks dataset messages into spam messages and ham messages using ELM algorithm. This classification methodology is developed using various features available with original data messages such as messages containing URL's and life time of account. Hongyu et. al [10] proposed a model to filter the spam messages over social networking sites. Faraz Ahmed et. al [11] proposed a classification model to classify the spam profiles in online social networks with Markov clustering. In this method a weighted graph is used. From this weighted graph find active friends, page likes and shared URLs features. Cheng Cao et. al [12] describes a methodology to classify the data into spam or ham messages using behavioral analysis of the users. To analyze the behavior of network users use click based features and post based features. Saini Jacob Soman et. al [13] describes an approach to detect malicious tweets in social networking sites with user based features, location based features, content based features and text based features. With these extracted features a classification model is developed by SVM classifier and ELM classifier algorithms. Proposed ELM based spam detection methodology performs better spam detection rate compare to SVM classifier. Kaiyu Wang et. al [14] proposed a methodology to detect spam messages with combining of network features and textual features. With these features a spam detection model is constructed by SVM machine learning algorithm. The overall accuracy of model is increased up to 29%. Fabricio Benevenuto et. al [15]describes a model to classify user profiles into spammers or non spammers based on content based features and user based features. To construct a classification model they have used support vector machine learning algorithm. Sajid Yousuf Bhat et. al [16] describes a methodology to detect spam users in social networking sites by ensemble learning methods. To train these ensemble learning algorithms facebook data set is used. In this proposed methodology network structure based features are used to construct a model. Hailu Xu et. al [17] are described different features to detect spam in various social network sites such as facebook, Twitter. Arushi Gupta et. al [18] propose a mechanism to detect spammers in Twitter social media network. In this approach they used tweet level features, user level features, URL's, spam word features. They have used combined approach to develop a model with Naive Bayes classifier, clustering and decision trees. Xianghan Zheng et. al [19] describes a methodology to detect spammers in social networking sites. They have used content based features and user based features using SVM machine learning algorithm to construct a spammer detection model. Zahra Mashayekhi et. al [20] analyzed content based features and non content based features to detect spam messages in E-mail data. They have combined decision tree algorithm and Neural Network algorithm to develop a classification model. They have implemented this model on Lingaspam data set. Anjali Sharma et. al [21] analyzed various spam detection techniques methodologies to detect spam. They have studied different origin based spam detection methodologies such as Blacklists filters, white lists filters, Realtime Blackhole list filters and content based spam detection techniques such as Rule based filters, Bayesian filters, Support vector machines and Artificial Neural Network algorithms. Saumya Goyal et. al [22]describes a model to classify the spam messages in Twitter social media network. They have used decision tree induction classification algorithm and KNN classification algorithm to construct a classification model. Chen Lin et. al [23] describes a spam detection procedure with Extreme Machine Learning (ELM) algorithm. They have used content based features, user based features and social interactivity features to construct classification model. Prabhjot Kaur et. al [24] describes a survey on various spam detection techniques. They have done the survey on various user based spam detection techniques, content based spam detection techniques, hybrid based techniques and relation based techniques. Bhagyashri Toke et. al [25] describes a spam detection approach to detect spam messages in Facebook dataset. They have used combined approach of Naive bayes classification algorithm and Rule based classification algorithm. Bhagyasri Toke et. al [26] studied an integrated approach to detect spam data in social networking sites. Ala M et. al [27] describes a spam detection approach to detect spam messages in social networking sites. In this methodology they have used various features like content features, user based features. They have used various feature extraction methods such as information gain, relief methods. Malik Mateen et. al [28] describes spam detection approach to detect spam messages in Twitter data. Sachin Kamley et. al [31] analysed various machine learning techniques such as Decision tree, Neural Network, Support Vector Machines, Genetic algorithms and Bayesian Networks for performance forecasting of Share Market. Sharvil Shah et. al. [32] studied various classifier algorithms for sentimental analysis in Twitter data. In our proposed approach we used content based features, user based features.

III. PROPOSED METHODOLOGY

The framework of our spam detection methodology is shown in Fig.1. In our proposed methodology we used different steps to detect spam in Twitter data. The previous spam detection analysts used various spam detection methodologies. Each approach uses its own data set and features for classification of data. Various spam detection approaches used different kind of features like user based features, content based features, network based features and location based features etc [19] [28]. Initially we train and test the classifiers individually with individual features on Twitter dataset. Next we train and test the ensemble approach on individual features and combination of user based and content based features. Later we did the same experiments on Twitter data set with cross validation approach. Ensemble cross validation approach has outperformed compare to other performed approaches

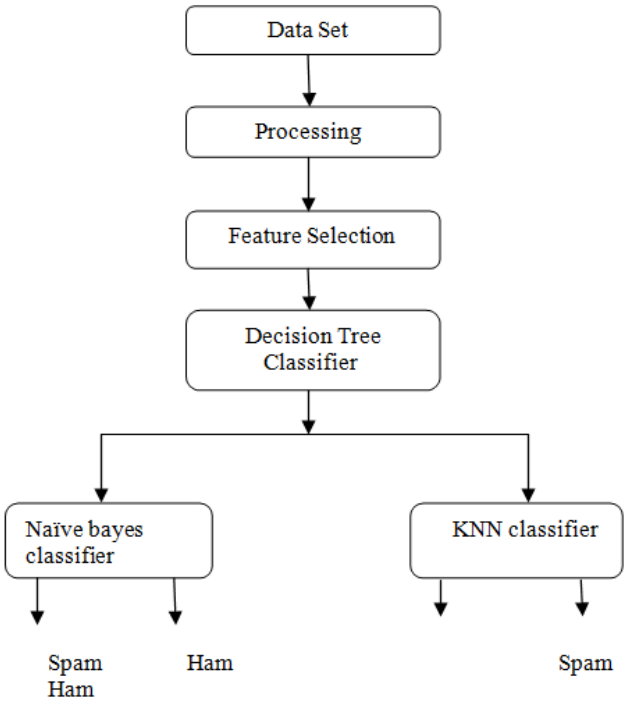

Fig.1 Spam Detection Frame work.

A. Dataset

Our research is conducted based on users perspective and content perspective. We get all the tweets from normal users instead of crawling public tweets. We randomly pickup 25 normal users from our Twitter and crawl tweets of the publishers they follow. We totally collected 2500 tweets.

B. Labeling tweets

Once the Twitter data was gathered, the next task was to develop a collection of tweets labeled into spam and ham groups. These categories could be used to train and test our classifier. Out of 2500 tweets, 2000 tweets are considered as ham tweets and remaining 500 tweets are considered as spam tweets.

C. Feature selection

In the proposed spam detection method 11 features are identified. The feature set is classified into two categories namely user based features and content based features

User Based Features: User based features are used to describe the behavior of users in twitter. These features are based on user relationships and properties of user accounts in twitter dataset. Generally in social media networks users can develop their own social networks with other users. In social network one user follows other users and allows other users to follow him. Spammers want to follow many profiles to spread misinformation to them, so they try to follow large number of users to spread misinformation. Generally we consider, the number of users following is more than number of users following him, such user account is considered as spam account. Here we are using different user based features to construct a model. User features are related to user accounts and the features are extracted from user accounts. The various user based features used in our approach are:

a) Number of Followers: This feature specifies the number of other users in network follow your account tweets. Generally followers define the popularity of someone profile. Generally spammers have less popularity and have less number of followers.

b) Number of Following: This feature specifies the number of other user accounts you follow. In twitter if you follow someone means you will see their tweets in your timeline. Twitter network knows to whom you follow and who is following you.

c) Age of Account: This feature specifies when the account has been created.

d) Follower to Following Ratio: This is the ratio of followers to following ratio in network for any user account. Generally ff ratio is less for normal users and this ratio is high for spammers.

$$FF\ Ratio = \frac{\text{Number of following}}{\text{Number of followers}}$$

e) Reputation: This is the ratio between number of followers to sum of following and followers

$$Reputation = \frac{\text{Followers}}{\text{Followers} + \text{Following}}$$

Content Based Features: These features are related to tweets posted by user. Generally normal users can't post duplicate content but spammers post lot of duplicate tweets. Content based features are based on messages that users write. The content based features are important to detect spam messages. Spammers are malicious users, who spread large amount of misinformation to the network users. The misinformation contains advertisements about their product and malicious links. The various content based features are used in our approach are:

a) Number of Tweets: Total number of tweets posted by user after creating his account.

b) Hashtag Ratio: This is the ratio between the tweets containing hashtags to total tweets posted and those tweets containing unique hashtag.

$$hashtag\ ratio = \frac{\text{Duplicate Hashtag}}{\text{Unique Hashtags X Tweet count}}$$

c) URL's Ratio: This is the ratio between duplicate URL's to number of distinct URL's in tweets and sum of tweets.

$$Total\ URLs = \frac{\text{Hash duplicate URLs}}{\text{Hash Unique URLs X Tweet count}}$$

d) Mentions Ratio: Twitter account users are identified by @username. @username can be written anywhere in the tweet. Spammers misuse this feature to send spam messages to the genuine users in network. Generally the user messages contain large number of mention and reply tags then user is consider as spam user.

$$@Tweets = \frac{\text{Tweets Containing@}}{\text{Total Number of Tweets}}$$

e) Tweet Frequency: Generally the tweet frequency of spammers is greater than genuine twitter user.

f) Spam words: we use specific spam words and count their occurrence in tweets of users.

The spammers use this spam words and spread misinformation to the users.

D. Ensemble approach:

Ensemble classifiers are used to group machine learning instances to improve the results of a classification model. The idea is based on the assumption that combination of multiple classifiers may be able to produce an overall classifier which is more accurate than any of the individual classifier.

In our proposed approach we use supervised machine learning algorithms. These algorithms are first trained on the labeled data set to develop classification models. These models are applied on unlabelled data to predict which data as spam data and which data as non spam data. In our proposed approach we ensemble decision tree induction algorithm, Naive Bayes classification algorithm and KNN Classifier to improve spam detection accuracy. In our methodology first decision tree classifier classifies the dataset as spam or non spam. To improve the classification accuracy of spam detection, categorized spam records of decision tree is given as input to the Naive bayes classifier and KNN classifier. Naive bayes classifier and KNN classifier further classify the messages into spam or non spam. In this way categorized non spam messages of decision tree are also given as input to the Naive bayes algorithm and KNN classifier to classify the any misclassified messages. As part of this approach, we compare the classification results of any two classification algorithms, if both classifiers predict the same result, then we finalize the class of tweet under investigation. If the predicted classes of both classification algorithms differ, then we use the prediction of third algorithm as the final class label of tweet.

E. Decision Tree Induction:

The decision tree is one of the known classification algorithms used in machine learning to guide the decision making process [30]. Many researchers used [20], [33] this classification algorithm to detect spam messages. The decision tree has three types of nodes. The root node has no incoming edges and zero or more outgoing edges. An internal node has exactly one incoming edge and two or more outgoing edges. The leaf or terminal node has exactly one incoming edge and no outgoing edges. Decision tree induction algorithms must provide a method for expressing an attribute test condition for different types of attributes like binary, nominal, ordinal and continuous attributes. There are many measures that can be used to determine the best way to split the records. These measures are defined in terms of the class distribution the records before and after splitting. The measures developed for selecting the best split are often based on the degree of impurity of the child nodes.

F. Naive Bayes Classifier:

This is one of the best machine learning algorithms for spam classification [17], [28]. To classify the message as a spam or non spam can be generalized by probability theory. The spam messages contain the specific words. The relationship between the attribute set and class variable within dataset is non-deterministic. To resolve this problem Bayes theorem introduces a statistical principle for combining prior knowledge of the classes with new evidence gathered from given data. Let X and Y be a pair of random variables. The joint probability, P (X=x, Y=y), gives the probability that variable X will take on the value x and variable Y will take on the value y. The conditional probability is the probability that a random variable will take on a particular value given that the outcome of another random variable is known. The conditional probability p (X=x| Y=y), gives the probability that the variable Y will take on value y, given that the variable X is observed to have the value x. Based on joint and conditional probabilities.

Bayes theorem, $P(Y|X) = \frac{P(X|Y)P(Y)}{P(X)}$

Y is the event that a given tweet belongs to a given class. X is the d dimensional feature vector corresponding to the tweet. The Naive bayes model makes the independence assumption that the attributes are all independent.

G. KNN Classifier:

This is very popular algorithm for classification of data. This algorithm is used for categorize dataset samples based on nearest training samples. To classify the test tweet, KNN algorithm identifies, k closest samples that are similar to test sample. The k nearest neighbors is identified by similarities of data sample. The data sample similarities are computed with some set of similarity measures. Euclidean distance measure is one of familiar similarity computing approach. The distance between two data samples can be found using Euclidean distance formula.

$D(X,Y)=\sqrt{\sum_{i=1}^{D}(Xi - Yi)^2}$

After k nearest neighbors is found, various strategies are used to predict the class label of the test tweet. A fixed k value is used for all classes in these methods. In this approach we used k=4.

IV. EXPERIMENTS AND RESULT

The main aim of this paper is to evaluate the performance of the ensemble classifiers for spam detection in social media networking sites. In order to detect spam in social media networks, user based and content based features are proposed and these features are extracted from social media networks. We compare the performance of classifiers including decision tree, Naïve bayes and KNN and their ensemble variants with cross validation and without cross validation.

The classification experiments are performed individually on each classifier. To do the experiments 80% of twitter dataset is randomly selected for training purpose and remaining 20% dataset is selected for testing the classifiers.

To evaluate the overall process of methodology we used a set of measures called precision, recall and F measure. The confusion matrix for spam detection system is:

Table 1: Confusion Matrix

		Predicted class	
		Spam	Ham
Actual class	Spam	S	T
	Ham	U	V

Where S represents the number of spam messages that were correctly classified, T represents the number of spam messages that were incorrectly classified as ham, U represents the number of ham messages that were incorrectly classified as spam and V represents the number of ham messages

that were correctly classified.
The proposed methodology is evaluated using three metrics, called, precision, recall and F measure.
The performance metrics are:

$$Precision = \frac{S}{S+U}$$

$$\text{Recall} = \frac{S}{S+T}$$

$$\text{F Measure} = \frac{2 * \text{Precision} * \text{Recall}}{Precision + Recall}$$

Initially all the classifiers are individually trained and tested with user based features. In next all the classifiers are individually trained and tested with content based features. Later all the classifiers are individually trained and tested using user based features and content based features. Table 2 presents performance of classifiers using user based features, table 3 describes performance of classifiers using content based features and table 5 presents performance of classifiers using user based and content based features.

Table 2: Performance of individual classifiers using only user based features

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.95	0.96	0.954
KNN	0.93	0.92	0.924
Naïve Bayes	0.95	0.956	0.952

The decision tree classifier has highest precision, recall and F measure compared to KNN classifier and Naïve bayes classifier

Table 3: Performance of individual classifiers using only content based features

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.92	0.92	0.92
KNN	0.91	0.912	0.91
Naïve Bayes	0.90	0.75	0.818

The decision tree classifier has highest precision, recall and F measure compared to KNN classifier and Naïve bayes classifier and Naïve bayes classifier has lowest recall and F measure compared to decision tree and KNN classifier.

Table 4: Performance of individual classifiers using user based features and content based features

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.95	0.96	0.954
KNN	0.91	0.92	0.914
Naïve Bayes	0.90	0.85	0.874

The decision tree classifier has highest precision, recall and F measure compared to KNN classifier and Naïve bayes classifier and Naïve bayes classifier has lowest recall and F measure compared to decision tree and KNN classifier.

In next phase of experiments our proposed model is trained and tested using user based features. After that the proposed model is also trained and tested using only content based features. Finally our model is trained and tested by user based and content based features. In tables 5, 6,7 presents performance of proposed model using only user based , content based and combination of user based and content based features.

Table 5: Performance of Proposed model using only user based features

	Precision	Recall	F measure
Classification model	0.96	0.967	0.963

The performance of proposed ensemble model using only user based features has highest precision, recall and F measure compared to Decision tree, naïve bayes and KNN classifiers.

Table 6: Performance of proposed model using only content based features

	Precision	Recall	F measure
Classification model	0.956	0.962	0.958

The performance of proposed ensemble model using only content based features has highest precision, recall and F measure compared to Decision tree, naïve bayes and KNN classifiers.

Table 7: Performance of proposed model using user based and content based features

	Precision	Recall	F measure
Classification model	0.965	0.968	0.966

The performance of proposed ensemble model using user based and content based features has highest precision, recall and F measure compared to Decision tree, naïve bayes and KNN classifiers.

In next level of our approach, we did classifications experiments using 10 fold cross validation. In every test, the original dataset is partitioned into 10 sub samples. Out of 10 subsamples nine are used as training data and the remaining one is used for testing the classifier. The process is then repeated 10 times, with each of the 10 sub samples used exactly once as the test data, thus producing 10 results. The average of the result is considered as final result. Table 8 presents the performance comparison of classifiers using user based features with cross validation approach. In this Naïve bayes approach has highest precision, recall and f measure compared to other classifiers. Tables 9,10 presents performance comparison of classifiers using content based features and combination of content based and user based features.

Table 8: Performance of individual classifiers using only user based features with cross validation

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.958	0.965	0.961
KNN	0.93	0.935	0.932
Naïve Bayes	0.961	0.967	0.963

Table 9: Performance of individual classifiers using only content based features with cross validation

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.92	0.925	0.922
KNN	0.915	0.921	0.917
Naïve Bayes	0.91	0.88	0.894

Table 10: Performance of individual classifiers using user based and content based features with cross validation

Classifier(individual)	Precision	Recall	F Measure
Decision tree	0.965	0.97	0.967
KNN	0.93	0.94	0.934
Naïve Bayes	0.92	0.85	0.883

Tables 11, 12, 13 presents the performance of our proposed model with only user based features, content based features and combination of user based and content based features. The proposed model with user and content based features has highest performance in terms of precision, recall and f measure.

Table 11: Performance of proposed model using only user based features with cross validation

	Precision	Recall	F Measure
Classification model	0.961	0.965	0.962

Table 12: Performance of proposed model using only content based features with cross validation

	Precision	Recall	F Measure
Classification model	0.925	0.923	0.923

Table 13: Performance of proposed model using user based and content based features with cross validation

	Precision	Recall	F Measure
Classification model	0.968	0.97	0.968

A. Comparison Analysis

This section describes a comparative analysis of the proposed method with other existing works for detecting spam messages. Table 14 presents the performance comparison of proposed method with other classification methods in terms of precision, recall and F measure. Table 15 presents the performance comparison of proposed method with or without cross validation.

Table 14: Comparison of proposed model with existing works

	Precision	Recall	F measure
Decision tree	0.965	0.97	0.967
KNN	0.93	0.94	0.934
Naïve Bayes	0.92	0.85	0.883
Proposed model	0.972	0.97	0.968

Table 15: Comparison of proposed models performance

	Precision	Recall	F measure
Proposed model without cross validation	0.965	0.968	0.966
Proposed model with cross validation	0.972	0.97	0.968

Table 15 describes comparison between proposed model with cross validation and without cross validation. In two methodologies user based features and content based features are used. The proposed model with cross validation approach has outperforms compared to without cross validation.

In this section we presents a comparative analysis of the proposed method with one of the methods for detecting spam messages proposed by X.Zhang et al. in [34]. The approach presented in [34] is implemented and evaluated on Twitter dataset. Fig 2 presents the performance comparison of proposed methodology with X.Zhang et al. method in terms of precision, recall and F measure. It can be observed from the figure that the proposed approach outperforms X.Zhang et al. method.

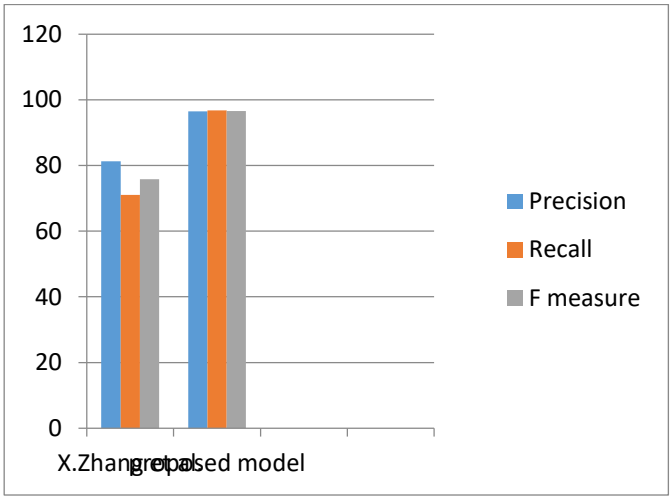

Fig 2: Comparison of results

V.CONCLUSION

In this paper, we have introduced an ensemble based spam detection methodology for social networks. This methodology considers user based features and content based features and apply them into Decision tree algorithm, Naïve bayes algorithm and KNN algorithm for spam detection. These algorithms are implemented individually without cross validation and with cross validation.

The ensemble approach is also implemented without cross validation and with cross validation. We have shown that our proposed solution is feasible and is much better classification result than other existing methodologies. One issue of our proposed approach is it takes more amount of time for model training. The feature extraction in our proposed solution is based on manual selection. The feature extraction process in our approach might be low adaptive and costive.

REFERENCES

1. Facebook" https://en.wikipedia.org/wiki/Facebook#Impact
2. "Twitter" https://en.wikipedia.org/wiki/Twitter#Statistics
3. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: The underground on 140 characters or less," in proc. ACM conf. Computer communication security, 2010, pp. 27-37.
4. Y Boshmaf, I.Muslukhov, K Beznoson, and M. Ripeanu, " design and analysis of social botnet," computer networks, vol. 57, no. 2, pp. 556578, 2013.
5. Arora, Harsha, Govinda Murali Upadhyay, "A framework for the detection of Suspicious Discussion on online forum using integrated approach of support vector machine and particle Swarm Optimization", international Journal of Advanced research in computer science, 2017.
6. Benjamin Markines, Ciro Cattuto and Filippo Menczer, "Social Spam Detection," Airweb'09 spain, ACM 978-160558-438-6
7. Kyumin Lee, James Caverlee and Steve Webb, "Uncovering Social Spammers: Social honeypots + Machine learning, SIGIR, july-10, Switzerland, ACM 978-1-60558-896-4/10/07
8. .Xin Jin, Cindy Xide Lin, Jiebo Luo and Jiawei Han, "SocialSpamGuard: A Data mining based Spam Detection System for Social Media Networks," 37th international conference on very large data bases, Washington, 215 8097/11/08, 2011.
9. Xueying Zhang and Xianghan Zheng, "A Novel Method for Spammer Detection in Social Networks," IEEE, 2015.
10. Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia and Alok Choudhary, "Towards Online Spam Filtering in Social Networks," cucis.ece.northwestern.edu/publications/pdf/GaoChe12.pdf
11. Faraz Ahmed and Muhammad Abulaish, "An MCL-Based Approach for Spam Profile Detection in Online Social Networks," IEEE, DOI 10.1109/Trustcom.2012.83, 2015.
12. Cheng Cao and James Caverlee, "Detecting Spam URLs in Social Media via Behavioral Analysis,"springer, ECIR 2015, LNCS 9022, pp. 703-714, 2015.
13. Saini Jacob Soman and Dr. S. Murugappan, "Detecting Malicious Tweets in Trending Topics using Clustering and Classification," International Conference on Recent Trends in Information Technology, IEEE, 2014.
14. Kaiyu Wang, Yumei Wang, Hongqiao Li, Yilin Xiong and Xinyu Zhang, "A New Approach for Detecting Spam Microblogs Based on Text and Users Social Network Features," National college Innovation program, Beijing University, china
15. Fabricio Benevenuto, Gabriel Magno, Tiago Rodrigues and Virgilio Almedia, "Detecting Spammers on Twitter," CEAS 2010-seventh annual collaboration, electronic messaging, anti-abuse and spam conference july-2010.
16. Sajid Yousuf Bhat, Muhammad Abulaish, Abdulrahman A. Mirza, "Spammer Classification using Ensemble Methods over Structural Social Network Features," IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent agent Technologies, 2014, DOI 10.1109/WI_IAT.2014.133
17. Hailu Xu, Weiqinh Sun, ahmad Javid, "Efficient Spam Detection across Online Social Networks," IEEE-2015
18. [18]. Arushi Gupta, Rishabh Kaushal, "Improving Spam Detection in Online Social Networks," IEEE-2015
19. Xianghan zheng, Zhipeng Zeng, Zheyi Chen, Yuanlong Yu,Chunming Rong, "Detecting Spammers on Social Networks," Elsevier, NeuroComputing 159 ,27-34, 2015.
20. Zahra Mashayekhi, Ali HarounAbadi, "A Hybrid Approach for Detection Based on Decision tree Algorithm and Neural Network," International Journal of Mechatronics, Electrical and Computer Technology, 2017
21. Anjali Sharma, Manisha, Dr.Manisha, Dr.Rekha Jain, "A Survey on Spam Detection Techniques," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, issue 12, December 2014.
22. Saumya Goyal, R.K.sharma, Shabnam Parveen, "Spam Detection using KNN and Decision Tree Mechanism in Social Network," Fourth International Conference on Parallel, Distributed and Grid Computing(PDGC), IEEE, 2016.
23. Chen Liu, Genying Wang, "Analysis and Detection of Spam accounts in Social Networks," 2nd IEEE International Conference on Computer and Communications, IEEE, 2016.
24. Prabhjot Kaur, Anubha Singhal, Jasleen Kaur, "Spam Detection on Twitter: A Survey," IEEE, 2016.
25. Bhagyashri Toke, Dinesh Puri, "Spam Detection in Online Social Networks using Integrated Approach,'' International Journal of Innovating Research in computer nd communication Engineering, vol. 4, issue 12,
26. Bhagyashri Toke, Dinesh Puri, "Review on Spam Detection in OSN using Integrated Approach," International Research Journal of Engineering and Technology, Volume:3, Issue:5,May-2016.
27. Ala M. AI-Zoubi, Ja far Alqatawna, Hossam Faris, "Spam Profile Detection in Social Networks Based on Public Features," 8th International Conference on Information and Communication Systems, IEEE, 2017.
28. Malik Mateen, Mahammad Aleem, Mihammad Azhar Iqbal, Muhammad Arshad Islam, "A Hybrid Approach for Spam Detection for Twitter," proceedings of 2017 14th International Bhurban Conference on Applied Sciences & Technology, IEEE, 2017.
29. Aziah Khamis, Yan Xu, and Azah Mohamed, "Comparative Study in Determining Features Extraction for Islanding Detection using Data Mining Technique: Correlation and Coefficient Analysis," International Journal of Electrical and Computer Engineering (IJECE) Vol. 7, No. 3, pp. 1112 – 1124 ISSN: 2088-8708, June 2017
30. Alhamza Munther, Rozmie Razif, Mosleh AbuAlhaj, Mohammed Anbar, Shahrul Nizam, "A Preliminary Performance Evaluation of K-means, KNN and EM Unsupervised Machine Learning Methods for Network Flow Classification", International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 2, pp. 778~784 ISSN: 2088-8708, April 2016.
31. Sachin Kamley, Shailesh Jaloree, R. S. Thakur, "Performance Forecasting of Share Market using Machine Learning Techniques: A Review," International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 6, pp. 3196~3204 ISSN: 2088-8708, December 2016, DOI: 10.11591/ijece.v6i6.13323
32. Sharvil Shah*, K Kumar**, Ra. K. Saravanaguru**, "Sentimental Analysis of Twitter Data Using Classifier Algorithms," International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 1, pp. 357~366 ISSN: 2088-8708, February 2016, DOI: 10.11591/ijece.v6i1.8982
33. Saumya Goyal, R.K.sharma, Shabnam Parveen, "Spam Detection using KNN and Decision Tree Mechanism in Social Network," Fourth International Conference on Parallel, Distributed and Grid Computing(PDGC), IEEE, 2016.
34. Xianchao Zhang, Haijun Bai, Wenxin Liang, " A Social Spam Detection Framework via Semi Supervised Learning," Springer international publishing, PAKDD 2016 workshops, pp.214-26,2016

AUTHORS PROFILE

Mr K Subba Reddy, is PhD student in Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, India. He has published papers in international conferences and journals. His area of interest is Big Data, Data mining and machine learning. He may be contacted at: kurapatisr80@gmail.com

Dr E Srinivasa Reddy, PhD., is currently serving as principal in University College of Engineering and Technology and also serving as Head of Department in Computer Science and Engineering, Acharya Nagarjuna University, Guntur, India. He has more than 24 years teaching experience. He is guiding PhD to 8 scholars and 15 has completed his PhD. Dissertations and contributed 45 articles in conferences and 120 papers in Research Journals. His area of interest is Image Processing and Data mining. He may be contacted at: esreddy67@gmail.com