# Feature Extraction Techniques in Microblogging Social Networks

T. Venkata Rathnam<sup>1</sup>, Divya Jyothi. N<sup>2</sup> <sup>1, 2</sup> Assistant Professor <sup>1, 2</sup> AITS-Tirupati, JNTUA University <sup>1</sup> isit.rathnam@gmail.com <sup>2</sup> nara.divyajyothi@gmail.com

Abstract - In recent years, the role of online social networking in our everyday lives has expanded quickly. At present, it is not only utilized for social communication, but also a vital stage for trading data and news. Micro-blogging websites such as Twitter, associates with a billions of users around the globe allows to spread these kind of valid and unique information i.e. news. Twitter has, in any case, not exclusively been utilized for the spread of legitimate news, yet in addition tricky and fake news. Detection of fake news in these blogs has recently pulled in a growing interest from the overall public and research scientists as the misinformation circulation has been increases particularly in the social blogging sites. Initially the ratio of these fake news is a bit low, but is growing continuously at an alarming rate in the recent years. This trend has created much interest from the academia to politics and many other industries throughout the world. The result of these fake news or spams are showing much influence from educational, financial and politics and it becomes a challenging issue for the researchers to avoid or prevent the fake news by detecting the origin of these fake news. Numerous data science communities are also focused on it and reacted by taking some actions against these issues, such as Kaggle "Fake News Challenge", Facebook and Twitter deployed AI to filter the fake posts or tweets from the user channels. In this paper, we described about the challenges in fake news detection along with recent machine learning techniques developed for this purpose. Extracting the features from the social blogs especially the top most microblogging website i.e. twitter and the types of the features used to detect the fake news are also presented in our paper. Additionally, we also presented the various types of spam detection methods.

**Keywords**—fake news, spam detection, tweet based spam detection methods, supervised and unsupervised learning methods.

## I. INTRODUCTION

Detection of fake information is a hot topic especially concerning news industry and also in societal aspects with the intension of evaluating the exactness of digital form of information. Over social network sites the false information will reach the society easily and attains real impacts in shortly to mass people. Society related issues raised by the people have able to tell which is fake and authentic. Anderson [1] mentioned that youth are very much aware about technology than their parents but to confirm whether that information is fake or real the youth seem like they confused and 44% people were confirmed it when research done by Common Sense Media. In the same statistics report it was represented as 31% of children who were having the age between 10-18 years are sharing at least a story and then they realize that it was fake one.

This leads to raise a completely new dimension related to the digital awareness which will have the capability in accessing and managing the technology. Along with the societal challenges, there is considerable and modest situation occurring in media concerns, the public circle and also journalism industry that needs debate and examination figuring out two important aspects [2]. The former one depends on a fact that the news publishers lost their control on news publishing to internet users by using some algorithms which are obscure and not even predictable. Besides, the new comers to the news market have created their presence by grabbing those technologies. The later depends on increasing the power of social media companies like Google, Apple, Facebook and Amazon attained a control over what was publishing to whom and how the publishing news is?

From the earlier context, to make online data as reliable is challenging but digital information is spread by many parties included in supporting to present data and in sharing the data among people in Internet, browsers and social networking sites. The concept of spreading of fake news has become more prevalent that Media and Sport Committee is now investigating the problems of users who are impacted with such fake information [4]. As disclosed by Conroy [3] detection of fake news can be defined as expecting the chances of specific news publications are intended to mislead the users. In this paper, we discussed the problem with the spreading of fake news in present technical aspects and also

discussed its emerging scope accordingly. Twitter is one of the leading social media sites which make users to text or post information up to 140 characters over a network known as "Tweet". In Twitter anyone can share their opinions, ideas and so on [5]. As per Twitter, it has approximately 320 million users are actively doing nearly 500 million tweets i.e., 350,000 tweets per minute in everyday [6]. Twitter displays the list which includes the topics which are mostly discussed in a specific time and it is called as "Trending Topics (TT)". This enables users to be aware about many trendy topics that are posting in Twitter. If user wants to mention the Tweet's topic he can use "#" character which is known as "Hashtag" so that one can easily track the topic on their interest. Twitter instantly reflects valuable events in real-time.

The structure of Twitter allows real time search systems and mining real time tweets to know what's happening in world in less time [7]. Sentiment analysing services are able to conclude the topics posted in Twitter [8]. Those services become successful when there is proper filtering of Spam from legal users. Customers prefers Twitter to know the people's perception regarding buying the products. In the same manner, companies uses Twitter to evaluate user satisfaction levels about their products [9]. This paper majorly contributes are summarized here. Twitter features which are utilized in spam detection by discussing their effectiveness, a detailed review regarding techniques of spam detection in Twitter are discussed along with its advantages and disadvantages as well, recent features of a Twitter that are not being used under spam detection methods those are used in spam detection are presented, Twitter features which are outdated that usually used by the spam detection methods in the study are also presented. According to authors [11], the framework of Twitter spam detection is show in Figure 1.

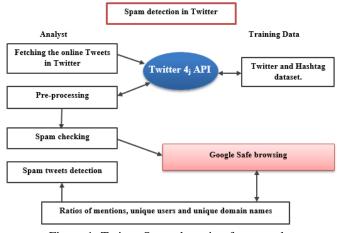


Figure 1: Twitter Spam detection framework.

#### ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)

#### II. ROLE OF MACHINE LEARNING

Machine Learning (ML) retrieves information from huge data repositories and performs prediction. In this the machines are capable of learning by the data which is trained and those machines are developed so as to use some algorithms by which it is able to make its self-decisions and yields the output to user. It is said to be the sub part of AI (Artificial Intelligence). Currently ML is used for critical data classification and also for decision making. In short, ML is the generation of paradigms which allows learning and decision making by the system itself. It is engaged with certain computing tasks where the design and coding of algorithms are not practical. Some of the instances of applications like filtering Spams .OCR (Optical Character Recognition), web browsers, Computer Vision and so on [12].

Machine learning is one of the research domains which usually concentrate on conceptual aspects, performance and the algorithms including the learning system properties. This ML domain constituted from various types of domains like AI (Artificial Intelligence), information and optimization theoretical aspects, statistics and some other fields of Science, Engineering and Mathematics. The implementation of machine learning is done on extensively and covered almost every scientific related fields which brought greater influence over science and societal aspects. The paradigm of ML used on multiple diversified issues such as recommender systems, mining the data and Informatics, self-control systems. In general, the machine learning domain is categorized into three sub fields. Those are Supervised Learning, Unsupervised Learning and Reinforcement Learning.

Supervised learning needs trained data that is labelled. It contains inputs and required outputs. But for Unsupervised learning there will be no need of having labelled data to train instead it requires inputs but no required outcomes. Reinforcement learning needs feedback which is obtained by interactions from outer world. In order to deal with the data tasks there proposed many application services and techniques [13]. It is done based on the above stated three learning algorithms. For instance, Google implements ML paradigms to obtain huge data from Internet to Google translator, image search engine and so on. Another important method here is that Outlier detection, which is one of primary issues related to data mining. Outlier is a type of pattern that differs from other patterns in a data set. This method is almost related research domain of data mining. The outliers those come early are treated as noisy information [14]. The outlier detection is very useful in some situations such as fraud finding on credit cards,

identifying intrusions in computer and illegal access and so on.

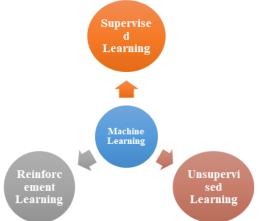


Figure 2: Types of Machine Learning techniques

# **III.** LEARNING METHODS

**Supervised machine learning** is specialized for algorithms generation which can yield general structures and concept through externally provided instances and forecast the upcoming instances. The intension of supervised learning is to classify the data from existing data. It examines and works with the training information and with that analysis it attempts to finalize a function which is utilized in mapping the recent instances. The leaning paradigm is able to perform conception through training information for further situations in future with best.

# 3.1 Naïve Bayes Classifier

Naïve Bayes classifiers comprises of labelled datasets, with those we tried to train the information i.e., examine the available probability of various class labels of the system. But before this we try to evaluate the posterior probability where we just tried to examine the fresh data probability to which it is required to derive a class label through the objects that are nearer to it. After evaluating both we attempt to integrate those in end.

# **3.2 Decision Trees**

The purpose of Decision trees is do classification by decision making. Here a tree is generated and comprises of multiple branches and those branches results various class labels. If this label compromises the class property then that label is allocated to that input variable.

# **3.3 K-NN Nearest neighbors**

The algorithm of K-NN nearest neighbor comprises of predefined class labels which are used to train the system.

# ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)

Later as one more input raises and is checked with its K nearest neighbors. The k value chooses to be odd for more time since in some cases the even one's has same distribution of class. Hence it is not easy to decide a class with dissimilar labels.

In **unsupervised learning**, there will no availability of labelled or training information but there will be some unordered information and we gave an attempt to cluster those depending on data. If this data is showing some similarities then the clustering is done by behavior and also similarities. That is to say we are trying to convert unlabeled data to labelled data. The best example of unsupervised learning is K means.

# 3.4 K-Means

The algorithm of K-means works like clustering. We integrated the unordered information into groups/clusters. These will have same criteria and same behavior as well. In k-means paradigm it is needed to have some k-centroids. K-centroid is group of classes which are essential to partition the information in and later we tried to partition the unlabeled information to their nearer centroid labels. We also estimated the belonging distance and update the position of centroid and just repeat the same step again till that centroid reach its destination.

In **Reinforcement Learning**, we must be aware of the term reinforcement. It means the outcome of strengthen behavior so that it is able to do better than before. Learning on that basis is called as Reinforcement learning. Some of the examples of Reinforcement learning are Markov decision process, Monte-Carlo approximation problem and so on.

# **3.5 Markov Decision Process**

In the process of Markova decision model, some of the considerations are to be taken into sight such as a state which we are in, action that is going to perform and a state that results when that action performs. Markov in the Markova decision model represents only current details which is not regarding with past things. Another factor must be taken into sight is reward.

# **3.6 MONTELCARLO** Approximation

It is the process of things approximation by using samples and an expectation is that many of the things relates to machine learning, hence the approximation of expectation results Monte Carlo approximation. This depends on odd experiment to get numerical outputs.

# IV. RELATED WORK

The data reliability can be defined with different words like trustworthiness, credibility, fairness, accuracy and so on. Many machine learning methods are used during research to evaluate the reliability of a Tweet message. Fake news enables the people to believe those easily with their false beliefs. Whenever someone post some message in Twitter it rapidly reaches to mass people. No matter what whether the published information is genuine or fake but people will believe those and it leads to confusion to know which is real and which is not. It is hard to classify. Anyways the fake news publishing will greatly influences the people's lives and also their safety. Many research processes uses sentiment analysis and classification of emotions to find the fake information but it relies on the language in which that message is posted.

The data reliability can be defined with different words like trustworthiness, credibility, fairness, accuracy and so on. Many machine learning methods are used during research to evaluate the reliability of a Tweet message. Fake news enables the people to believe those easily with their false beliefs. Whenever someone post some message in Twitter it rapidly reaches to mass people. No matter what whether the published information is genuine or fake but people will believe those and it leads to confusion to know which is real and which is not. It is hard to classify. Anyways the fake news publishing will greatly influences the people's lives and also their safety. Many research processes uses sentiment analysis and classification of emotions to find the fake information but it relies on the language in which that message is posted.

There exists considerable concept for research is Machine Learning techniques to detect deception, most of those concentrated in doing classification of online reviews and posts which are publicly available. In particular these methods are useful in grouping with highly complicated methods of analysis. Specifically, Deep Syntax analysis including Probabilistic Context Free Grammars (PCFG) is shown to be particularly valuable in combination with n-gram methods. Under this section, we presented Twitter features and how it deals with the spams.

#### 4.1 Features of Twitter

Twitter allows accounts to "Follow" other accounts which one can put interest on. In contrary, the interaction between the users in Twitter is bi-directional instead of one way communication. A user can hit a "like" otherwise he can "Retweet (RT)" the same tweet to his followers. In the

#### ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)

following figure, we can see how the interaction will be between the users in Twitter. Every user can login to Twitter with unique username and he can post the tweets by referring some other Twitter user with a special character "@" called as a "mention" in the Twitter. Users can instantly get notify whenever somebody hits like or do retweets or mention.

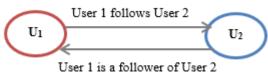


Figure 3: Relationship between users in Twitter

One more Twitter feature is to allow users in creating a public/private lists based on their interest and can group other users who are with the similar interests [15-17]. In the same way, there is a possibility to manage those lists by including or removing the users in them and it is only done by the user who is an owner. The lists which are subscribed by the users are classified as "subscribe to" whereas the lists in which the user added by that owner are classified as "member of" and is shown in Figure 4.

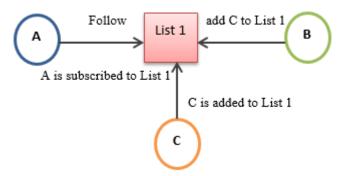


Figure 4: Relationships between the lists and users

Twitter uses both the services provided by manually and computerized to give spam free environment. In twitter the manual services enables the users to report on spammers through their profile details. The approaches which belong to manual will consume more time and is unable to recognize spammers completely among mass people.

Twitter considers different factors like (1) posting fake information on many accounts or several fake news on single account, (2) to follow or unfollow many accounts in short time, (3) having many spam complaints on an account, (4) instantly hits on like, follow and retweets (5) posting harmful links (6) posting tweets which are not related to current aspects[18]. The Twitter Spam detection features are classified into three categories. Those are (1) Features based on

Account. (2) Features based on tweets and (3) Interaction between a sender and receiver. Each of the above categories are discussed in the below.

## 1. Features based on Account

The Spammers are identified through analyzing theirs' details provided in Twitter account which contains some essentials and are listed in the Table 1. Since some of them can be controlled by the user whereas some other cannot be controlled by the user [19].

Feature	Description	Can user be controlled?
User name	Unique identifier of account	Yes
Profile picture	Display picture of account.	Yes
Theme colour	The choice of theme colour of account.	Yes
Date of birth	Birth date information of account	Yes
Home page	Account's web page	Yes
Place	Location	Yes
Date of creation	The date when account created.	Yes
Total Tweets	Number of tweets that account has.	No
Following	Total number of accounts that account follows.	No

# Table 1: Account based spam detection features.

## 2. Features based on Tweets

Spammers always tend to post some unwanted tweets to have people's attention. Those spammers can be recognized by analyzing the tweets they posted. It is essential to reduce spam tweets and the users must be provided an environment where there are no spams. It is an objective of Twitter. Every tweet comprises of the data and is listed in Table 2.

# 3. Graph-based Features

Twitter is said as a network of users where a user associates with the Tweets. This can be represented in the form of a graph. In that graph, users and the tweets are represented through nodes whereas the links between them represents the relationship. By generating a graph for representing the users along with their interactions we can evaluate the occurrences of spams based on the distance between tweet's sender and mentions. The Table 3 the featured related to that graph are listed.

## ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)

Table 2: Tweet based spam detection features.

Tuble 2. Tweet bused spuil detection feutures.				
Feature	Description	Can user be controlled?		
Sender	who sends tweets	Yes		
Mentions(@)	Used in tweets	Yes		
Hashtags(#)	Used in tweets	Yes		
Link	Used in the tweet.	Yes		
Likes	Number of likes that a tweet has.	No		
Retweets(RTs)	Number of <b>Retweets</b> that a tweet has.	No		
Replies	Replies received by a tweet.	No		
Sent date	Date when the tweet is sent.	Yes		
Place	Place where the tweet posted	Yes		

Table 3: Grap	h Based features
---------------	------------------

Feature	Description	Can user be controlled?
Distance	Shortest path length between the users	No
Connectivity	Connection strength	No

## V. TWITTER SPAM DETECTION METHODS

Under this section, Twitter spam detection techniques are discussed. The proposed methods are classified into four methods. They are (A) Account-based spam detection methods, (B) tweet-based spam detection methods, (C) graph based spam detection methods, and (D) hybrid spam detection methods.

#### 5.1 Account-based Spam Detection Methods

These methods rely on the listed features in Table 1. Lin and Huang [20] recommended an approach for Twitter spam recognition based on two features. 1. URL rate which mentions the ratio of tweets count with URL in total tweets. 2. Interaction rate that states ratio of count of tweets which are of interacting among total tweets count.

#### 5.2 Tweet-based spam detection methods

These methods are on the basis of features of tweet that are listed in the Table 2. The approaches to filter URLs uses crawlers either static or dynamic to examine recently found URLs. Besides to detect malicious URLs they will use URL otherwise website blacklist. These models use various features like URL and DNS information, redirections of URLs including source code (HTML). While spam detection some of the features are taken into sight like URLs length and domain details, brands involved in URLs, misuse of URL aliasing and

so on. A filter called Prophiler [21] uses the techniques of static analysis for detecting the harmful data of website. The Prophiler's features are considered from (1) Website's HTML information like elements count within a specific region, elements count in malicious data, and count of involved URLs. (2) JavaScript related code like ratio of key-words to words, shellcode existence probability and number of DOM updating functions and (3) URL which is relatively closed like few of malicious URL patterns, existence of sub domains otherwise IP addresses in the URLs.

# 5.3 Graph-based Spam Detection Methods

These methods are on the basis of features of tweet that are listed in the Table 2. Song et al. [29] evaluated distance and relationship among sender tweets and also mentions. The distance is defined by the shortest path length between a sender's tweets and mentions whereas connectivity is defined by the interaction between the users. The methods use graphical representation to describe Twitter's features with nodes and the edges. Graph models are the best way to represent the data related to interconnectivity otherwise topology. Hence graphs are generally used by the social networking sites like Twitter, Facebook which majorly created over users, concepts and interactions which are bi-directional. Even though it gives best performance regarding accurate rate and consideration to filter spam from the legitimate users, these are provided in hybrid spam detection methods because they are integrated with the other methods for spam detection.

## **5.4. Hybrid Spam Detection Methods**

These methods use the combination of spam detection methods discussed in earlier sub sections so that to give highly robust methods for the same that evaluates the probability spam detection in all the way. Gao et al [24] suggested an approach on the basis of profile of tweet's sender, communication history, group size, and time interval on average, tweet's URLs on average. Chen et al [25] provided a real-time spam detection method for Twitter on the basis of 12 insignificant features that extracted from dataset comprising about 6.5 million spam tweets. The tweet-based based features of the proposed method are words count in every tweet, the count of URLs per every word, how many number of words, characters, hash tags, mentions, URL are used to tweet. Chu et al. [26] proposed a method to classify Twitter accounts as manual, bot and Cyborg based on both the account and tweet based features. For this classification they used the features are ratio of tweets count that includes URLs, ratio of count of followers to friends and so on. Amleshwaram et al. [27] introduced a hybrid Twitter spam detection method on the basis of both the account and tweet-based features.

## VI.CONCLUSION

Twitter is a well-known micro-blogging site where people can post something in short. The popularity captures the attention of spammers who are intended to spread malicious content through tweets. So to provide spam free environment in Twitter we must filter the spammers from the legitimate users. In this paper we have discussed role of machine learning and its sub categories in spam detection. We have explained the methods to extract the features from these micro blogging websites, which are very useful to detect the fake news or spam messages. Also explained the significance of deep leaning in the context of spammers filtering. We also depicted the features of spam detection in twitter along with their classification. We also, presented the twitter based fake detection methods along with the issues involved in such method. In this paper we mainly concentrated on the recent methods to detect the fake news and the scope of it in the current research and will come up with algorithms to improve the fake detection results in our next work.

#### REFERENCES

[1]. Anderson, J. Even social media-savvy teens can't spot a fake news story. Quartz 2017; Available from: <u>https://qz.com/927543/even-socialmedia-savvy-teens-cant-</u>

spot-a-fake-news-story/.

[2]. Bell, E. Facebook is eating the world. Columbia Journalism Review 2016; Available from: http://www.cjr.org/analysis/facebook\_and\_media.php.

[3]. Conroy, N., Rubin, V., and Chen, Y., Automatic deception detection: methods for finding fake news. Proceedings of the Association for Information Science and Technology, 2015. 52(1): p. 1-4.

[4]. BBC, N. The rise and rise of fake news. BBC Trending 2016; Available from: <u>http://www.bbc.com/news/blogs-trending-37846860</u>.

[5]. N.K. Alex Cheng, Mark Evans, Inside the Political Twittersphere, Sysomos. (2009). https://sysomos.com/inside-twitter/politicaltwittersphere (accessed February 5, 2017).

[6]. Twitter Usage Statistics - Internet Live Stats, Internet Live Stats. (2017). http://www.internetlivestats.com/twitter-statistics/ (accessed February 5, 2017).

[7]. L. Jiang, M. Yu, M. Zhou, X. Liu, T. Zhao, Targetdependent Twitter Sentiment Classification, in: Comput. Linguist, 2011: pp. 151–160.

[8] S. Liu, X. Cheng, F. Li, F. Li, TASC: Topic-Adaptive Sentiment Classification on Dynamic Tweets, IEEE Trans. Knowl. Data Eng. 27 (2015) 1696–1709. doi:10.1109/TKDE.2014.2382600. [

[9] H. Saif, Y. He, M. Fernandez, H. Alani, Semantic Patterns for Sentiment Analysis of Twitter, in: Proc. 13th Int. Semant. Web Conf., Trentino, Italy, 2014: pp. 324–340.

[10] D. Goodin, Mystery attack drops avalanche of malicious messages on Twitter, Ars Tech. (2014). http://arstechnica.com/security/2014/04/mystery-attack-

dropsavalanche-of-malicious-messages-on-twitter/ (accessed February 5, 2017).

[11]. Vishwarupe, Varad & Bedekar, Mangesh & S. Pande, Milind & Hiwale, Anil. (2017). Intelligent Twitter Spam Detection: A Hybrid Approach.

[12]. J Langford, Tutorial on practical prediction theory for classification. J Mach Learn Res 6(3), 273-306 (2005)

[13]. R Bekkerman EY Ran, N Tishby, Y Winter, Distributional word cluster vs. words for text categorization J Mach Learn Res 3, 1183-1208 (2003)

[14] Buntain, C., & Golbeck, J. 2017. Automatically Identifying Fake News in Popular Twitter Threads. 2017 IEEE International Conference on Smart Cloud (SmartCloud), 208-215

[15] D. Kim, Y. Jo, I.-C. Moon, A. Oh, Analysis of Twitter Lists as a Potential Source for Discovering Latent Characteristics of Users, in: CHI 2010 Work. Microblogging What How Can We Learn From It, Atlanta, Georgia, USA, 2010. doi:10.1.1.163.7391.

[16] Y. Yamaguchi, T. Amagasa, H. Kitagawa, Tag-based User Topic Discovery Using Twitter Lists, in: 2011 Int. Conf. Adv. Soc. Networks Anal. Min. (ASONAM 2011), Kaohsiung, Taiwan, 2011: pp. 13–20. doi:10.1109/ASONAM.2011.58.

[17] Using Twitter lists, Twitter. (2017). https://support.twitter.com/articles/76460 (accessed February 5, 2017).

[18] A.H. Wang, Don't follow me: Spam detection in Twitter, in: SECRYPT 2010 - Proc. Int. Conf. Secur. Cryptogr., Athens, Greece, 2010: pp. 1–10. Doi: 978-989-8425-18-8.

[19] Reporting Spam on Twitter, Twitter. (2017). https://support.twitter.com/articles/64986 (accessed February 5, 2017).

[20] K. Lee, J. Caverlee, S. Webb, And Uncovering Social Spammers: Social Honeypots + Machine Learning, in: Proc. 33rd Annu. Int. ACM SIGIR Conf. Res. Dev. Inf. Retr., Geneva, Switzerland, 2010: pp. 435–442. doi:10.1145/1835449.1835522.

[21] D. Canali, M. Cova, G. Vigna, C. Kruegel, Prophiler: A Fast Filter for the Large-Scale Detection of Malicious Web Pages, in: WWW '11 Proc. 20th Int. Conf. World Wide Web, Hyderabad, India, 2011: pp. 197–206. doi:10.1145/1963405.1963436.

[23] G. Stringhini, C. Kruegel, G. Vigna, Detecting Spammers on Social Networks, in: 26th Annu. Comput. Secur. Appl. Conf. (ACSAC 2010), Austin, Texas, USA, 2010: pp. 1–9.

[24] H. Gao, Y. Chen, K. Lee, D. Palsetia, A. Choudhary, Towards Online Spam Filtering in Social Networks, in: 19th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS 2012), San Diego, California, USA, 2012.

[25] C. Chen, J. Zhang, X. Chen, Y. Xiang, W. Zhou, 6 Million Spam Tweets: A Large Ground Truth for Timely Twitter Spam Detection, in: 2015 IEEE Int. Conf. Commun.,

# ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)

IEEE, London, UK, 2015: pp. 7065–7070. doi:10.1109/ICC.2015.7249453.

[26] Z. Chu, S. Gianvecchio, H. Wang, S. Jajodia, Who is Tweeting on Twitter: Human, Bot, or Cyborg?, in: 26th Annu. Comput. Secur. Appl. Conf. (ACSAC 2010), Austin, Texas, USA, 2010: pp. 21–30. doi:10.1145/1920261.1920265.

[27] A.A. Amleshwaram, N. Reddy, S. Yadav, G. Gu, C. Yang, CATS: Characterizing Automation of Twitter Spammers, in: 2013 5th Int. Conf. Commun. Syst. Networks (COMSNETS 2013), Bangalore, India, 2013. doi:10.1109/COMSNETS.2013.6465541.

# **Author Profile:**

**Mr. T. Venkata Rathnam** is currently working as Assistant Professor in the Department of Computer Science & Engineering in AITS, Tirupati - JNTUA. Received Master's Degree from JNTUA in 2012 and Bachelor's Degree in 2008 & has Six Years of Experience and taught various subjects in Computer Science stream, organized various national conferences & workshops, guided many students in developing their projects in both UG & PG level and Published papers in conferences and journals. My Research interests are Big Data analytics and Image Processing.

**Ms. N. Divya Jyothi** is currently working as Assistant Professor in the Department of Computer Science & Engineering in AITS, Tirupati, - JNTUA. Received Master's Degree from JNTUA in 2012 and Bachelor's Degree in 2005 & has Six Years of Experience and taught various subjects in Computer Science stream, organized various national conferences & workshops, guided many students in developing their projects in both UG & PG level and Published papers in conferences and journals. My Research interests include Computer Networks, Big Data, Image Processing and Functional Programming.