



A Systematic Review on the Suspicious Profiles Detection on Online Social Media Data

ASHA^{1*} and DR. BALKISHAN²

^{1,2}Department of Computer Science and Application, Maharshi Dayanand University Rohtak, India.

Abstract

Escalating crimes on digital facet alarms the law enforcement bodies to keep a gaze on online activities which involve massive amount of data. This will raise a need to detect suspicious activities on online available social media data by optimizing investigations using data mining tools. This paper intends to throw some light on the data mining techniques which are designed and developed for closely examining social media data for suspicious activities and profiles in different domains. Additionally, this study will categorize the techniques under various groups highlighting their important features, challenges and application realm.



Article History

Received: 14 July 2017
Accepted: 08 August 2017



Keywords

Suspicious Discussions,
Online Social Media Data,
Data Mining,
Multimedia technology.


Introduction

Human behavior and social interactions are greatly influenced by the digital and multimedia technology. In the age of information and internet, online data is growing in an exponential manner. Research reveals that a variety of social media platforms on Internet such as Twitter, Facebook, YouTube, Tumblr, Blogs and discussion articles are in constant use by activist groups for dispersion of their thoughts, viewpoints and beliefs. They exploit this communication channel for promoting radicalization, recruiting members and creating online virtual communities sharing a common agenda. These malicious users who take advantages of this technological feat to

publish illegal and suspicious contents (images, videos, texts ...) in order to exchange data online and share ideas that could affect the security of countries or institutions. Advent of these interacting networks, led to the increase of countless crimes, as they offer ease to criminal conversations and transfer of data (suspicious messages). As an example, the media sharing websites for YouTube allow to publish videos in relation to "how to create a bomb". The social network Facebook and the micro blog Twitter also help criminals to coordinate and manage online suspect actions. As per a recent record, there is found a crime percentage¹⁶ of seven big Indian cities as shown in figure 1.

CONTACT Asha  asha.rathee08@gmail.com  Department of Computer Science and Application, Maharshi Dayanand University, Rohtak, India

© 2017 The Author(s). Published by Enviro Research Publishers

This is an  Open Access article licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-nc-sa/4.0/>), which permits unrestricted NonCommercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

To link to this article: <http://dx.doi.org/10.13005/ojcs/10.03.13>

Crime Rate

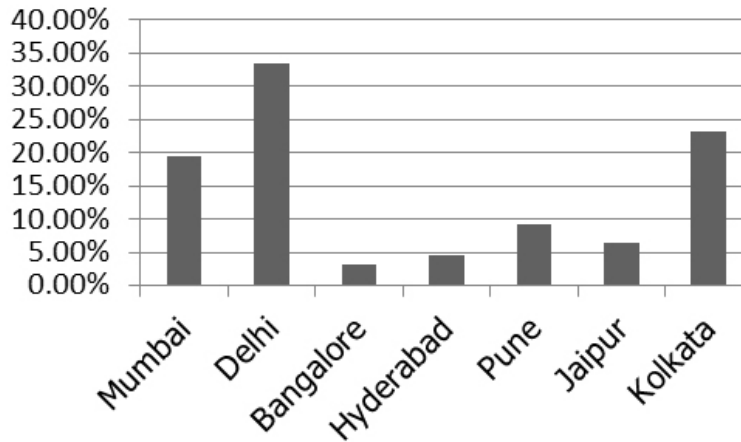


Fig. 1: Crime Percentage of seven big Indian Cities

A great survey (Gladwell and Shirky 2011) shows that the popular social networking websites Facebook and Twitter have over 1 billion and over 240 million active users respectively¹. People share several news related articles and also comments on the posts of other people, thus making news experience more participatory than before. In 2010, according to the report by CNN, 75% of the news was forwarded to other people through email and 37% of the news items were shared on Facebook and Twitter. The network of the users of the social media is becoming the fastest and effective way to for the news dispersion, to comment, review, and communicate etc. throughout the whole world. The websites have their freely available API's like Twitter has is API named as Twitter API, thus allowing the availability of the datasets.

Thus for detecting suspicious discussions on the social media dataset, numerous data mining methods have been adopted till date. Through this, suspicious activities can be uncovered by analyzing the interests of all users. The main hurdle faced by researchers in doing so, is the lack of information retrieval and data analysis tools for real time data of social media websites. The resultant database is quite huge and thus to extract desired knowledge from the large search space of social data, an intelligent data mining algorithm is required. The basic process of suspicious activity identification is shown in figure 2.

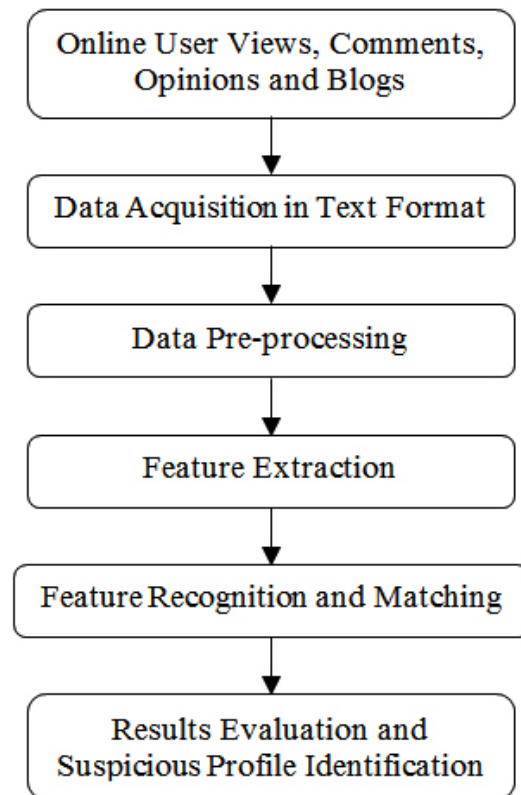


Fig. 2: Basic Process of Suspicious Activity Detection

Moreover, the involvement of massive numbers of parameters in the search space makes the extensive search infeasible. Consequently, proficient search

approaches are of imperative significance. There are numerous papers published till now in this domain. However, so far no review paper is available in this domain which consolidate the current researches. Our paper aims to provide a review of the work done in this field by various researchers and highlight the future research direction.

This paper is structured by firstly discussing the various issues and challenges in handling online data, followed by the different categories to divide the techniques available in this arena. Section 4 and 5 reviews the work done by various researchers with a comparative analysis. Last section concludes the paper by providing research directions for new researchers.

Challenges In Social Media Data

Presently, the individuals are fortunate enough to share and articulate their opinions and viewpoints concerning various aspects of life on a single message board, Social website data. This data actually signify massive virtual space, where anyone can hold discussion in the form of posted messages. User preferences are generally captured by analyzing their attitudes and behaviors mentioned on the websites as comments. To measure a user's loyalty and to keep track of their sentiments towards any topic is achieved by monitoring the suspicious activities and discussions done through their posts on the social media websites. The main hurdle faced by researchers in doing so, is the lack of information retrieval and data analysis tools for real time data. The resultant database is quite huge and thus to extract desired knowledge from the large search space of online social media data, an intelligent data mining algorithm is required. Moreover, the involvement of massive numbers of parameters in the search space makes the extensive search infeasible. Consequently, proficient search approaches are of imperative significance. Thus, the study and analyses of data from online social websites' textual data consists of numerous issues and challenges. The data available is not in ready-to-use format. Some of the major problems are discussed below:

Grammar and Spellings

Most of the users make a lot of semantic or even spelling mistakes when they post something on

the web. Using datasets, these mistakes are processed during the pre-processing phase of any application.

Trustworthiness

The number of user's views on different subjects signifies the importance of the data on the web. Unfortunately, numerous fake accounts are made to give these posts a fake view and also fake reviews are also given to either push or to pull a post or an entity on the web platform.

Format

Every other online website exhibits their own way or format for data posting and also the different users have different style of posting. For example: hashtag (#) is used when subjects are to be tagged or @ is used to refer different users. Hence, each website needs to be studied separately.

Language

The option to post views or data in different languages is also available in online websites. Also the translator option is available to understand the other language's post.

Categories of Techniques Employed

The online suspicious detection activities can be categorized under different heads depending on the way they handle the data. Researchers have tried to group the developed techniques for monitoring suspicious discussions based on different criteria's. However, the one proposed by Murugesan, Devi et al. 2016², received the acceptance. These categories are presented below with their specifications and related work.

Brute Force Algorithms

In brute force strategy type, the relations between inflected and root forms are contained by the stemmer's lookup table. A word is stemmed by querying the table when inflection matching to stem is found. When matching inflection is found, the root form associated with it is returned.

Matching Algorithms

Matching algorithms use stem database (Example: a document set containing stem words). The algorithm searches the stem database for a match of the word that needs to be stemmed. Different

constraints like the relative length of the stem. For example the stem “inter” of the words “international” or “interpersonal” should not be considered as stem of the word “interest”.

Emotional Algorithms

Emotional algorithm is used to detect the emotions of the human beings via video, audio, text and so on. In online websites users post their comments or share their thoughts mainly in a text format. Following methods are used to detect emotions in the text viz. Keyword Spotting Technique, Learning-Based Methods, Hybrid Methods.

Keyword Spotting Technique

The keyword spotting technique or pattern matching involves the process of finding the keywords occurrences from a already give substring set. In the past, the problem has been studied and various algorithms have been suggested for its evaluation. In terms of emotion detection, this technique involves pre-defined keywords. These words are classified as happy, fear, disgust, disgusted, exclaimed, dull etc. The input to this technique will be the text and then the tokenization of the text will be performed. Words in the textual data which are related to the emotion keywords will be identified and analysed. Sentence is checked for the presence for negation and identified emotion class is delivered as output.

Learning-based Methods

Learning-based methods have different way for problem evaluation. Initially, the methods involve problem to identify the emotions from the given input data but now days it considers the problems of input text classification into different emotions. These methods are different from keyword-based methods. Learning-based methods use previously trained classifier for emotion identification. It makes use of different machine learning classifiers like Naïve Bayes, Support Vector Machine etc to identify the emotion present in the textual data.

Hybrid Methods

The results acquired by only using keyword-based technique and learning-based technique are not satisfactory. So, some systems make use of the hybrid approach. This approach combines the features of the both of the techniques thus

improving accuracy and output results. The hybrid based system proposed by Wu, Chuang and Lin is one of the most significant systems. The system utilizes a rule-based using hybrid approach and extracts the semantics related to specific emotions. The Chinese lexicon ontology is extracted to get the attributes. These attributes and semantics contain emotions. Hence, emotion keywords are replaced by rules and served as features for training the classifier. Unfortunately, the emotion categories find out by this approach are limited.

Soft computing techniques

These methods have been applied to text document clustering as an optimization problem. A soft clustering algorithm such as fuzzy c-means has been applied in for high-dimensional text document clustering. It allows the data object to belong to two or more clusters with different membership. Further, it was combined with harmony search to improve the efficiency of document clustering. An innovative field of nature inspired methods were also employed like PSO (Karol and Mangat 2013)³, GA (Song and Park 2006)⁴, ACO (Azaryuon and Fakhar 2013)⁵ and bees algorithm (AbdelHamid, Halim et al. 2013)⁶. To develop more efficient hybrid approaches they were further combined and successfully applied to text mining (Premalatha and Natarajan 2010)⁷.

Existing Work

In order to perform experiments, the scarcity of real data publically available and lack of properly researched methods and techniques publications are the two most often considered criticisms related to the research of suspicious detection based on data mining. Table I below provides the briefs of various applications developed so far using the online or social media data.

The past researches focused on mining facts but the recent research focuses on mining opinions. Detection of opinion from the web data deals with numerous things. (Liu, Hu *et al.*, 2005, Mishne and Glance 2006)^{8,9} and their applications. A recent paper on fraud detection (Phua, Lee *et al.*, 2010)¹⁰, illustrates various categories of frauds identified by analyzing the web contents (listed in table) for example frauds related to home insurance, crop insurance, automobile insurance and medical insurance. In order to identify the

general trends of these suspicious or fraudulent transactions and applications is mainly focused by these detection systems.. Besides these domains, this survey paper also identifies other probable areas where suspicious discussions are monitored

using in text mining. A basic process of text mining approach is shown in figure 3. Surveillance systems depends on the spatio and spatial temporal data for the detection of chemo terrorist, bio terrorist and terrorist.

Table 1: Various applications developed till date using the online or social media data

Author	Applications
Yang, Pierce <i>et al.</i> , 1998	Finding novel events in a temporarily ordered stream of news stories
Bentley 2000	Frauds related to home insurance
Little, Johnston <i>et al.</i> , 2002	Crop insurance
Smith 2002	Browsing document collections in order to detect events
Wong, Moore <i>et al.</i> , 2003	Uncover simulated anthrax attacks from real emergency department data
Hutwagner, Thompson <i>et al.</i> , 2003	Early Aberration Reporting System (EARS)
Heino and Toivonen 2003	Usage logs of doctors' reference database and HMMs to influenza time series
Goldberg, Kirkland <i>et al.</i> , 2003	Financial crime detection system . The Securities Observation, News Analysis, and Regulation (SONAR)
Otey, Parthasarathy <i>et al.</i> , 2003	Intrusion detection at the secure NetworkInterface Cards (NIC) level
Gruhl, Guha <i>et al.</i> , 2004	Topic propagation throughout weblogs, track online chatter over a period of time
Kumaran and Allan 2004	Identifying new events from the discussions
Yamanishi, Takeuchi <i>et al.</i> , 2004	Medical insurance
(Phua, Alahakoon <i>et al.</i> , 2004, Viaene, Derrig <i>et al.</i> 2004) ^{10,11}	Automobile insurance
Ku, Liang <i>et al.</i> , 2006	Enable the tracking of online opinions in weblogs
Huberman, Romero <i>et al.</i> , 2008	Political advertising
Ginsberg, Mohebbi <i>et al.</i> , 2009	Predicting outbreaks of influenza
Dodds, Harris <i>et al.</i> , 2011	Measuring people's happiness and mood
Choi and Varian 2012	Reproducing economic indices
(Vallina-Rodriguez, Scellato, <i>et al.</i> , 2012) ¹²	Political discussion and Election prediction
(Boutet, Kim <i>et al.</i> , 2012) ¹³	
Imran, Castillo <i>et al.</i> , 2015	Crisis response
Kempe, Kleinberg <i>et al.</i> , 2015	Analyse the diffusion of ideas in social networks
Schober, Pasek <i>et al.</i> , 2016	Highlights how participants view different elicitation techniques from surveys to social media data and the nature of the data

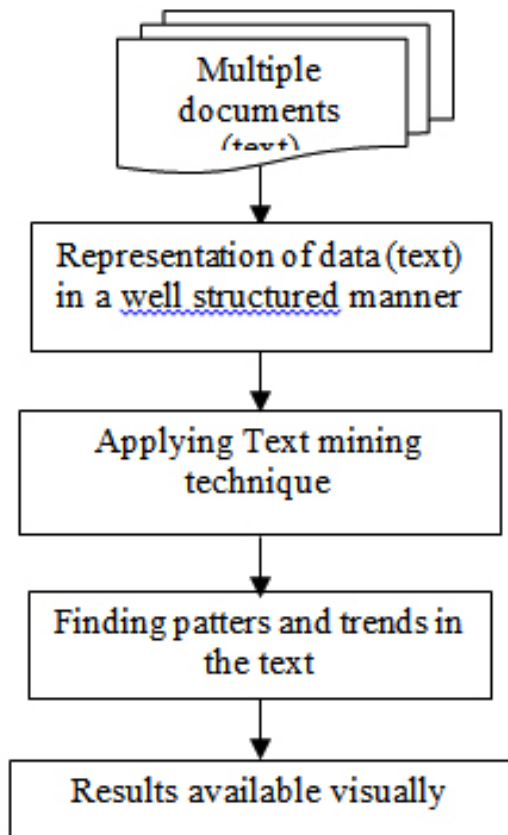


Fig. 3: Text Mining Process

Recently the Facebook static messages are scanned to identify criminal's behavior. Also, in 2015, authors (Siguenza-Guzman, Saquicela et al. 2015)¹⁴ presents a literature review of data mining applications in academic libraries. In this they have identified various techniques to monitor special category of words required for a specific journal or library. In 2016, authors Diaz, F. (Diaz, Gamon *et al.*, 2016)¹⁵ discusses online and social media data as an imperfect continuous panel survey. One more research article (Tayal, Jain *et al.*, 2015)¹⁶ identifies various data mining techniques for crime detection and criminal identification specifically in India.

Study Gap

In recent years, much research has focused on understanding the expression of individuals' opinion online, and exploring its use as an alternative data

collection modality for surveys and fundamental ways to gather the information and predict opinion, identify knowledge, support, and related tasks. However, finding accurate information in social big data is becoming a challenge for public and private research organization. Moreover, the evolution of internet has led to the growth of more innumerable cybercrimes. Criminals uses social networking websites, cell phones, messenger applications to send suspicious messages, thus making dynamically tracing their activities more difficult. Table II gives the particulars of work done by various authors during the span of time and the corresponding study gap.

Previously, the text mining techniques were based on brute force approaches, stemming algorithms, and keyword identification techniques. But due to the huge and continuous real time data, these techniques failed to achieve desired success rate. As a result, researchers shift their focus towards intelligent data and text mining approaches, which has the caliber to tell something about the world, outside the data collections themselves. Novel based investigation of the text-mining approaches should be based on the process of deliberately creating new knowledge that was not existed before and cannot be simply discovered or retrieved. The process is manual in nature i.e. mostly done by humans only and cannot be automated easily. Artificial Intelligence can be used to facilitate this novel investigation as it simulates human behaviour and intelligence. Such an automatic system could be called either as intelligent text mining (for considering the structured textual data) or intelligent data mining (for considering structured data in the form alphanumeric and numeric fields). Keeping this in mind, the present research work will consider the swarm intelligence mechanisms (subcategory of soft computing and artificial intelligence domain) to design a data mining technique which will efficiently and effectively monitor the suspicious discussions on the social media websites' data. This will surely provide an upper hand to the law enforcement agencies throughout the world, which are in ultimate need of these kinds of systems to have prior knowledge about the crimes.

Table 2: Study gap and work done by various authors

Paper	Author & Year	Worked On	Gap
Cybercrime Profiling: Text mining techniques to detect and predict criminal activities in microblog posts	(Alami and Elbeqqali 2015) ¹⁷	hashtags on Twitter (e.g., #arabspring, #BostonAttack) were used especially to target and detect suspicious topics and eventual illegal events. Similarity approach is used in text analysis to detect suspicious posts.	Based on predefined suspicious words database. Resulting in limited text corpus database.
Automated Monitoring Suspicious Discussions on Online Forums Using Data Mining Statistical Corpus Based Approach	(Murugesan, Devi <i>et al.</i> , 2016) ¹⁸	Monitor discussion for possible illegal activities and download suspected postings that are in text formats as evidence for investigation.	Based on traditional approach of similarity matching between the words
Detecting suspicious profiles using text Analysis within social media	(Alami and Beqqali 2015) ¹⁹	Text analysis posted generally on social media by users in order to discover the suspicious published contents with the deduction of the suspicious behavior users on the web	Using similarity distance leading to high execution time and lower precision
Effective Sentiment Analysis of Social Media Datasets using Naive Bayesian Classification	(Gurkhe, Pal <i>et al.</i> , 2014) ²⁰	Approach for automatically classifying the sentiment (positive, negative or neutral) of social media data	Dataset is small, The accuracy falls when testing with neutral labels
Latent Text Mining for Cybercrime Forensics	(Lau and Xia 2013) ²¹	Latent text mining model for cyber-attack forensics based on a real-world data set crawled from Twitter and Blog sites	Based on un-supervised LDA-based method
Mining network data for intrusion detection through combining SVMs with ant colony networks	(Feng, 2014) ²²	The proposed approach combines the SVM method with the Self-Organized Ant Colony Network (CSOACNs) based Clustering to exhibit the advantages of both CSOACNs and Support Vector Machine (SVM) method. A standard benchmark KDD99 data set is used for the implementation and evaluation of algorithm.	CSVAC algorithm can be enhanced to generate more SVM classifiers to handle multiclass cases
		Experiment results show that CSVAC (Combining Support Vectors with Ant Colony) outperforms SVM or	

		CSOACN alone in terms of both run time efficiency and classification rate.	
Identifying Digital Threats in a Hacker Web Forum	(Macdonald Frank <i>et al.</i>) ²³	The hackers' language was analyzed to detect the potential threats against critical infrastructures with the help of automated analysis tools. Parts of speech tagger was used to analyze the posts and a list of keywords is determined which is used to query the data. Then, a sentiment analysis tool is used to score these keywords, which were further analyzed to determine the method's effectiveness.	Dictionary used in the proposed work is SentiStrength's which doesn't include many words specific to the hacker jargon and subculture.

Conclusion and Future Work

In this paper, we did a detailed review of various existing types of system using text analytics to detect suspicious user in social media. Basically, we found that the techniques developed in this domain, focuses on text analysis in order to discover the suspicious contents with the deduction of the suspicious behavior users on the web. Study revealed that we need to analyze the user's behavior based on tweets, comments, links shared etc. information available with respect to the user.

Also, suspicious behaviors can be categorized under groups such as terrorist activity, financial laundering, or others. Using this categorization, the corpus of probable suspicious words can be build which will further assist in developing more refined and reliable techniques for detecting these activities. An important aspect of this study divulges that, search strategies based on swarm based algorithms may prove their caliber and superiority in this domain.

References

- Gladwell, Malcolm, and Clay Shirky. "From innovation to revolution: Do social media make protests possible?." *Foreign Affairs* 90, no. 2 (2011): 153.
- Murugesan, M. Suruthi, R. Pavitha Devi, S. Deepthi, V. Sri Lavanya, and Annie Princy. "Automated Monitoring Suspicious Discussions on Online Forums Using Data Mining Statistical Corpus Based Approach." *Imperial Journal of Interdisciplinary Research* 2, no. 5 (2016).
- Karol, Stuti, and Veenu Mangat. "Evaluation of text document clustering approach based on particle swarm optimization." *Open Computer Science* 3, no. 2 (2013): 69-90.
- Song, Wei, and Soon Cheol Park. "Genetic algorithm-based text clustering technique." In *International Conference on Natural Computation*, pp. 779-782. Springer Berlin Heidelberg, 2006.
- Azaryuon, Kayvan, and Babak Fakhar. "A novel document clustering algorithm based on ant colony optimization algorithm." *Journal of mathematics and computer Science* 7 (2013): 171-180.
- AbdelHamid, Nihal M., MB Abdel Halim, and M. Waleed Fakhr. "Bees algorithm-based document clustering." In *ICIT The 6th International Conference on Information Technology*, 2013.
- Premalatha, K., and A. M. Natarajan. "Hybrid PSO and GA models for document

- clustering." *Int. J. Advance. Soft Comput. Appl* 2, no. 3 (2010): 302-320.
- 8 Liu, Bing, Mingqing Hu, and Junsheng Cheng. "Opinion observer: analyzing and comparing opinions on the web." In *Proceedings of the 14th international conference on World Wide Web*, pp. 342-351. ACM, 2005.
- 9 Mishne, Gilad, and Natalie S. Glance. "Predicting Movie Sales from Blogger Sentiment." In *AAAI spring symposium: computational approaches to analyzing weblogs*, pp. 155-158. 2006.
- 10 Phua, Clifton, Daminda Alahakoon, and Vincent Lee. "Minority report in fraud detection: classification of skewed data." *Acm sigkdd explorations newsletter* 6, no. 1 (2004): 50-59.
- 11 Viaene, Stijn, Richard A. Derrig, and Guido Dedene. "A case study of applying boosting Naive Bayes to claim fraud diagnosis." *IEEE Transactions on Knowledge and Data Engineering* 16, no. 5 (2004): 612-620.
- 12 Vallina-Rodriguez, Narseo, Salvatore Scellato, Hamed Haddadi, Carl Forsell, Jon Crowcroft, and Cecilia Mascolo. "Los twindignados: The rise of the indignados movement on twitter." In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pp. 496-501. IEEE, 2012.
- 13 Boutet, Antoine, Hyoungshick Kim, and Eiko Yoneki. "What's in your tweets? I know who you supported in the UK 2010 general election." In *The International AAAI Conference on Weblogs and Social Media (ICWSM)*. 2012.
- 14 Siguenza-Guzman, Lorena, Victor Saquicela, Elina Avila-Ordóñez, Joos Vandewalle, and Dirk Cattrysse. "Literature review of data mining applications in academic libraries." *The Journal of Academic Librarianship* 41, no. 4 (2015): 499-510.
- 15 Diaz, Fernando, Michael Gamon, Jake M. Hofman, Emre Kıcıyman, and David Rothschild. "Online and social media data as an imperfect continuous panel survey." *PLoS one* 11, no. 1 (2016): e0145406.
- 16 Tayal, Devendra Kumar, Arti Jain, Surbhi Arora, Surbhi Agarwal, Tushar Gupta, and Nikhil Tyagi. "Crime detection and criminal identification in India using data mining techniques." *AI & SOCIETY* 30, no. 1 (2015): 117-127.
- 17 Alami, Salim, and Omar Elbeqqali. "Cybercrime profiling: Text mining techniques to detect and predict criminal activities in microblog posts." In *2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, pp. 1-5. IEEE, 2015.
- 18 Murugesan, M. Suruthi, R. Pavitha Devi, S. Deepthi, V. Sri Lavanya, and Annie Princy. "Automated Monitoring Suspicious Discussions on Online Forums Using Data Mining Statistical Corpus Based Approach." *Imperial Journal of Interdisciplinary Research* 2, no. 5 (2016).
- 19 Alami, Salim, and Omar El Beqqali. "Detecting Suspicious Profiles Using Text Analysis Within Social Media." *Journal of Theoretical & Applied Information Technology* 73, no. 3 (2015).
- 20 Gurkhe, Dhiraj, Niraj Pal, and Rishit Bhatia. "Effective Sentiment Analysis of Social Media Datasets using Naive Bayesian Classification." *International Journal of Computer Applications (0975 8887)* 99, no. 13 (2014).
- 21 Lau, Raymond YK, and Yunqing Xia. "Latent Text Mining for Cybercrime Forensics." *International Journal of Future Computer and Communication* 2, no. 4 (2013): 368.
- 22 Feng, Wenying, Qinglei Zhang, Gongzhu Hu, and Jimmy Xiangji Huang. "Mining network data for intrusion detection through combining SVMs with ant colony networks." *Future Generation Computer Systems* 37 (2014): 127-140.
- 23 Feng, Wenying, Qinglei Zhang, Gongzhu Hu, and Jimmy Xiangji Huang. "Mining network data for intrusion detection through combining SVMs with ant colony networks." *Future Generation Computer Systems* 37 (2014): 127-140.