IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 5, Ver. II (Sep - Oct 2018), PP 27-35
www.iosrjournals.org

Detecting Vulnerable User in Twitter Using Tweet Description Logic Rule Generation

S. Revathi[1], Dr.M.Suriakala[2]

[1] Asst.Professor, Dept of Computer Application, A.M. Jain College, Chennai, India.
[2] Asst.Professor, PG & Research, Dept of Computer Science, Dr.Ambedkar Govt Arts College, Chennai, India.
Corresponding Author: S. Revathi

Abstract: *In today's modern era, Social media have become a mandatory, exciting and mundane apparatus in our lives and diverse informal organizations have distinctive focused set of people. Among these networks, twitter standout in the top list that has nearly 313 million dynamic clients on a monthly basis with a whopping 500 million of tweets each day. The commonly shared information on Twitter varies from current affairs, occasions, superstars in every field to government or political issues. Therefore, there is a need to conduct targeted research on identifying approaches for vulnerable user identification in twitter. The proposed system is used in identifying the maximum set of profile data that are necessary for identifying vulnerable user in twitter and identify the appropriate data mining approach for such task. The proposed system is used in identifying the maximum set of profile data that are necessary for identifying vulnerable user in twitter and identify the appropriate data mining approach for such task. This research has been proposed with data mining techniques of Tweet Description Logic Rule Generation algorithm for finding and analysis to the vulnerable user and attackers. Such profiles are distinguished by implementing the above algorithm which considers the targeted user followers and the sharing Threshold Limit as its parameters. Trial results assures of following: The suggested technique beats different models in regard of accuracy, efficiency and least time. Also, the assessment reveals that the identification rate of current method is significantly more compared to other methods.*

Keywords: *Privacy leak, Twitter, Online Social Networks, security, machine learning, fake follower, online social activities.*

Date of Submission: 23-09-2018 Date of acceptance: 08-10-2018

I. Introduction

Today every single life is dominated by massive utilization of Web and Social Media. It has penetrated in the lives of every individual these days. Users are consistently operating on applications mainly Whatsapp, Instagram, Face book, Twitter, and so on. They perform multi or varied tasks that include posting and sharing information, commenting, going live, and posting sound, video, photographs and refreshing status.

Talking about Twitter, it boldly stands in the forefronts the much prominent online interpersonal organization and a mini blogging media for posting texts otherwise called tweets, upheld by a colossal environment. It proclaims that it comprises of nearly 140 million dynamic clients generating 340 million plus messages per day and to top it all somewhere around one million enlisted applications developed by 750,000 plus IT professionals. Client applications are incorporated for different operating systems like IOS, Android, Mac and Windows and applications that includes news sources, URL shortening, picture sharing. For such external services, Twitter gives an option of tweets that can range up to characters with a length of 140 holding just messages. In this way, when clients need to post muddled data like news and variety of media stuff, they ought to incorporate the concerned website address into the tweet as the entire website address size and related writings may surpass 140 characters. The primary concern of the research is to distinguish the unsafe client via screening through the malevolent accounts i.e. only one individual can open account with counterfeit data thereafter send request and thus easily inject malware by texting and post sharing. Hence, the prime agenda of the research lies in selecting distinguished methods for identifying fake user or client ID. The suggested framework is utilized in recognizing numerous set of profile information that are vital for distinguishing unsafe client in twitter and thereafter apply the suitable strategy concerning Data Mining for such undertaking. This paper study proposes the following method of Tweet Description Logic Rule Generation algorithm for finding and analysis to the vulnerable and attackers. Such user related profiles are distinguished by implementing the above algorithm which considers the targeted user followers and the sharing Threshold Limit and thereafter the account of fake user is aborted or disabled and deleted once the threshold limit is exceeded.

Our research claims that with restricted profile information our technique aids in detecting fraud profiles with 97% accuracy with only 2.67% standing out negative, when compared to other current strategies that consider massive volume of data set along with more user data. In proposed system developed different stages are Social network creation, uploading information, Monitoring user activity, detecting malicious user, Data mining approaches, removing malicious User. With the help of certain parameters fraud user accounts can be differentiated from the genuine ones. This in return helps to lessen malevolent or harmful actions. Trial results assures of the fact that suggested technique beats different models in regard of accuracy, efficiency and least time. Also, the assessment reveals that the identification rate related to the current method is significantly more compared to other methods.

Following is a brief assortment of the journal. The 2nd section states the prior author's working. The 3rd section enlists various machine based methods and also outlook of varied levels. The 4th Section, presents the tests outcome. In the final or terminating part of 5th Section the future upcoming work is laid down.

II. Related Work

Social media acts as a huge gathering of common people who can make new friends, trace old ones, and post their memorable moments and life happenings and information related to every arena. Author's Malik Mateen et, al [1] presented a hybrid technique based on graph and content related parameters which helps in detecting the spammers on Twitter. Using this strategy an analysis was made on actual Twitter related dataset having around 11 thousand clients and roughly around 400k plus tweets.

According to analysis done by Gee et. Al [2], the level of spam that has spread across social media is depicted. To achieve this, the author builds up honey user profiles on various social networking sites. The prime aim being examining spammer's way of conduct and pattern of dealing thereafter suggesting solutions or methods to highlight and prevent spam actions.

Guojun et al. 2017 introduced and presented web crawlers for making the pupil aware of threat and attack of any form or type. It was presented that interactive web crawlers when enforced can help in being vigilant, which undoubtedly leads to lowering the attack risk intervals amidst unguarded disclosure and recovery [4]. Macdonald et al. 2015 executed web crawlers to detect potential damage by checking harmful or hostile forums. Author laid importance on carefully examining informal origins for the protection of cyberspace [3].

Anupama Aggarwal et, al [5] presented the clients with artificially bolster their social status with help of black-market web resources. This approach detects those users who alter their supporter or follower count ratio by making use of an unsupervised local neighborhood detection methodoloy. The users neighborhood is examined based on certain rigid parameters that projects client resemblance related to desired follower count. This count estimation founded on the proposed method projects a precision of 84.2% while giving least error count. Also it's found that the node embedding algorithm praising beats the content based techniques which are helpful in recognizing hateful and aborted users. Thus by focusing on user an outlook of hate speech is portrayed, leading to proper identification and knowledge of this serious issue. [6]

In a correlative case study that was organized to examine and bring out an appropriate and compelling methodology for addressing the class imbalance issue. Yet another finding based on Twitter spam detection was performed pertaining to various classic strategies. The test outcome reveals that a fuzzy based ensemble learning can remarkably enhance the categorization performance on imbalance ground truth Twitter data[7].

Girisha Khurana, Mr. Marish Kurma [8]. The emphasis is laid upon identification of spam clients in Twitter. The spam classifier or content based approach is made enforced for doing so. It also extends to social concepts in Twitter, goal of spammers and their various types. The Honey-profile strategy is being made use of. These profiles maintained the log information of clients from different networks. All the friend requests coming were accepted but no friend request was sent Mohammad Rakib Amin, Mehedee Zaman, Mohammed Atiquzzaman, Md. Shohrab Hossain [9] Now the task was to examine the behavior and character of fraud users, hence 2 kind of strategies were implemented, The system call based detection and the other being Network based detection. For the computation 1260 malwares and 227 non malware users were brought under the observation. Bravo-Marquez et al. [10] suggests word-level categorization that portrays the generation of opinion lexicons resulting from tweets that lacked label. Then the Sentiment Analysis was made use of for categorizing words falling under good, bad or unbiased. Vectors which represents the tweets are classified into semantic that is related to word cluster and the other is bag of words. The outcome reveals that semantic ones assure to be pretty good in contrast to the other one. The approach centers around creating a system that is related to machine learning which makes use of metadata resulting from tweets and data based on machine activities that revolves around fake URLs which has 0.99 F-measure(utilizing 10-fold cross validation) and 0.833 (based on invisible data test) at 1 s in relation with URL [11].

A 5 minutes recorded system-level machine task was performed to fetch different behavior patterns along with Web servers (Rana, Awan, Burnap & Javed, 2015). The expectation was to create a machine classifier which could differentiate between fake and considerate URLs having F-measure as 0.72 when the test was performed on invisible data. The prime focus on the earlier workout was establishment of a machine classifier that could trace a URL in a 5 minute interval [12].

Twitter is being made use of to perform a spectrum of cyber attacks. Lately in the year 2015 the Russian hackers made use of Twitter to hack the US Pentagon's email servers (Robinson, 2015[13]).

During this research it was revealed that various attributes linked with Twitter can be helpful to highlight abnormal and doubtful accounts (like spam or malevolent links). Cao and Caver lee closely examined the Twitter accounts to mark the spam infected tweets, that was related to user accounts meta-data, spam and malicious URL (Cao & Caver lee, 2015[14]). According to their findings it was laid down that it was complicated to alter these kinds of behavioral aspects. Xiang, Oliver, Chen, Zhang and Zhou (2016) made use of machine based spam template of Finite State, which depicted that such malicious users can generate nearly 2000 tweets from merely one template. All the more such users made use of number of different accounts to generate well patterned spam that was difficult to detect [15].

Language tools are being implemented to detect these spam infected tweets. First, collection of all the tweets from every kind of latest and varied topics takes place which is then marked or labeled as safe or unsafe. Thereafter various parameters were retrieved using the language model. The tweets were then segregated as spam from those that were not spam. Hence by implementing our existing system in Twitter the spam becomes clearly noticeable and one can figured out by targeting and examining the tweets instead of figuring out the accounts of such users [16].

The social network of Twitter revolves around tracking events and the user profiles. Strategies like spammer’s identification and users' classification can be enforced to prevent Twitter uploaded with irrelevant and junk content. A methodology is implanted that make use of haphazard attribute sampling within a Machine Learning based System that is like a gray box, along with the help of a method namely the Random Forests variant which can detect Twitter spammers . Two types of dataset are brought under consideration, first a very happening one and the other being completely new one. Among these two, the new one holds the users that are marked as malicious or spammers, characterized with 54 attributes. The outcome portrays a visible effect of improved feature sampling method [17].

The approach is found as quiet tough as the skilled methods make use of network data in abundance which acts as an attribute for techniques concerning machine learning. Availability of these sorts of datasets which populate social networking data for real time based forecast is often rare. Since the ever demanding social media is populated with content polluters, the sole purpose that concerns the research rests on to implement a strategy to recognize them in actual time. Australia suffered from the serious concern of civil unrest event prediction; hence we implemented our methodology to trace out content polluters from every single tweet excluding the historical data related to a particular user account. These bots exhibit certain features hence relevant measure is suggested for identifying such users [18].

Yang et al. [19] researched that bot accounts related to OSN connect to one another by fluke and behave very naturally amidst the existing users. The spams are easily distinguished on social groups by referring to the content along with the network data [20]. Among the various bot detecting models by different researchers Lee et al. [21] filtered the unknown users in social websites and occupied them to spread and post any type of information whether correct or misleading ones. A method was laid to understand and grasp user social etiquettes and interactions along with the re-tweet time interval.

III. Proposed Work

3.1 Project overview

Social Media or network is the most wanting and leading priority in the lives of every individual today to get instantly connected to ones which are close by as well as those who are remote. Be it Instagram, Facebook, Snap chat, Twitter and many more on the list. People have dedicatedly connected themselves with their online account in a trustworthy manner. One of such social grouping network in the limelight is Twitter which allows worldwide users to post their views and comments which are termed as tweets. With some good follows the evil. Spammers are such evil prevailing in social networking circle which acts as fake or fraud users whose sole purpose is to perform heinous activities and harm the other users by sending irrelevant tweets. Every social networking website along with the well known and happening Twitter gives prime importance to protect and guard the authorized users from such fraud accounts. One such strategy is the Tweet Description Logic Rule Generation algorithm which relies on machine learning and is efficient in detecting and examining the fake and malevolent profiles. This technique utilizes the followers or supporters counts and the sharing threshold limit to target such malicious users.

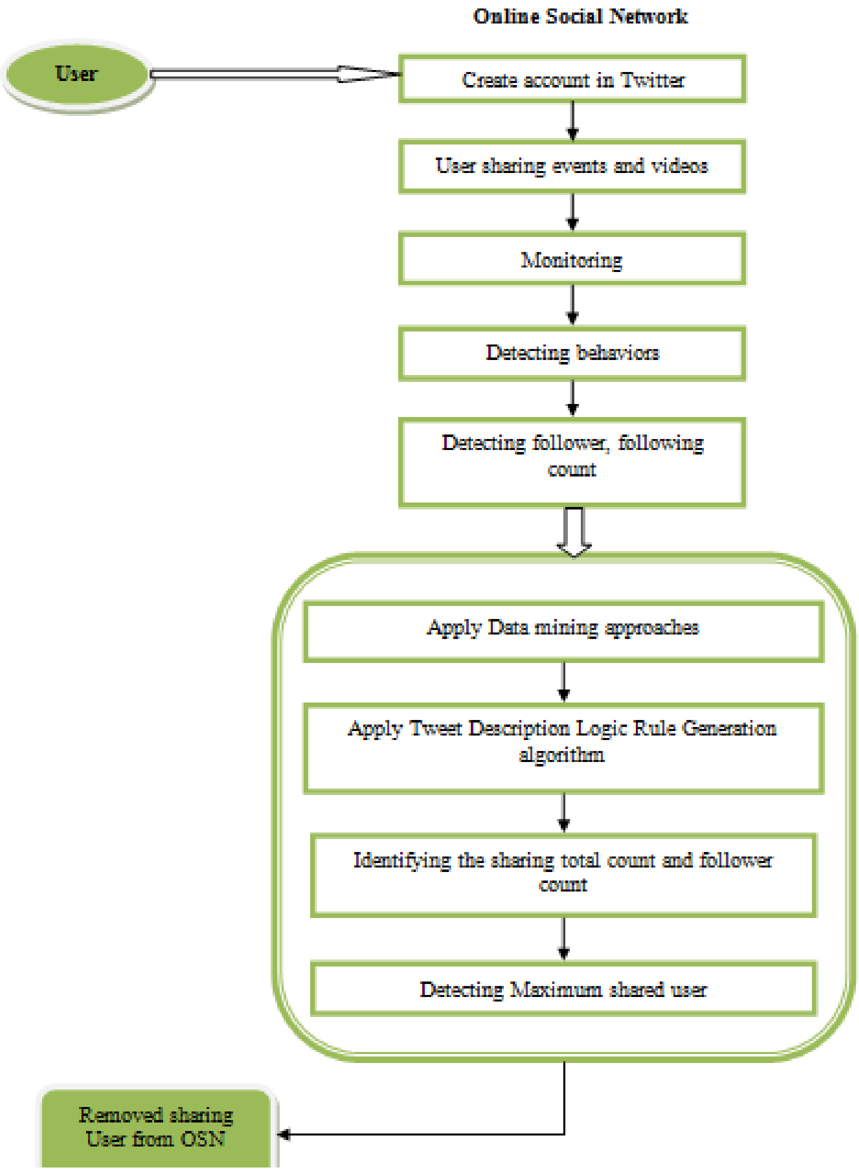
Online Social Network
User
Create account in Twitter
User sharing events and videos
Monitoring
Detecting behaviors
Detecting follower, following count
Apply Data mining approaches
Apply Tweet Description Logic Rule Generation algorithm
Identifying the sharing total count and follower count
Detecting Maximum shared user
Removed sharing User from OSN

Figure 1: Overall Proposed architecture

3.2 Datasets

Data set used in this paper is a Twitter user account details collected from the GitHub data repository which contains both real and fake identities. Following Account attributes are foreseen for observation namely Domain Name, Email Id, Screen Name, Longitude and Latitude etc. The proposed method is implemented using Java environment. It needs dataset with a mixture of real and false accounts labeled accordingly. The training and testing dataset are made use of for proper evaluation of the algorithms. Any public data source can act as a resource for dataset. The demanding concern is in retrieving dataset related to user accounts as there occurs privacy terms and conditions.

3.3 Online Social network

These networks acts as an common platform where people from different corner of the world form a community and dynamically interact among each other by sharing and posting their views, outlooks, comments etc... Every social network organization deploys a manager whose sole purpose is tracking, screening, analyzing and most of all presenting and mentoring the organization, brand or a person’s existence in the world of social media. Twitter provides a graphical interface making use of which the user interaction becomes more interactive among each other via visual indicators and graphic based icons unlike the interfaces that are merely text based labels and has text navigation. Twitter offers 3 kinds of users that is, Owner Account, other users and TPS. The user holding Owner account transfers private data in the system and a varied nature of personal or public data is stored within data repository via third party server. The Owner presenting any information can be made use of by the Normal users.

3.4 Uploading information

Social Media have spread their wings exponentially in every corner of the world. Undoubtedly it projects itself as a mandatory part of every ones priority. People are ceaselessly creating and building up networks portraying their status, relations, wealth and even intimate information for purely vanity purpose. This trend of socialism indeed leads to uninvited risks and problems that is usually overlooked. Initially, in any social media groups ones image and the personal data is acquired. Once the image and information is fetched it can undergo a wide range of processing techniques to go apt with the requirement. These images are often of different types such as natural, face uplift or professional and of considerably any size. The user demands that the image uploaded on his profile page must remain private to his own friend circle which can be somewhat done by using the private setting provided by the social sites. Later this matter can be visible anywhere in the public.

3.5 Protected system

Any unauthorized third party access can be blocked without intimating the owner of the image. Once the private settings are applied on image any user without authorization cannot make use of the image but can only view it. Thereafter provision of hardware is made which includes mouse and keyboard related controls. Any kind of operation related to mouse is suspended and the option of print screen is also disabled. These hardware controls value is fetched which helps to make the code inactive and thereafter as false.

3.6 Monitoring

It signifies tracking and examining the behavior of fraud or fake users in. Messaging option in Twitter can be both private and public. Also the user can look or search upon for any public Users or posts. The module allows to send a friend request at the same time accept a friend request. In relation to social behavioral aspects and measures, the social profile of an user can be framed. Concerning these social profiles the applications are build up which distinguishes genuine profiles with that of fake ones. A social build up profile gives an overview and genuine approach which helps effectively to enlist unique individuals social patterns.

3.7 Detecting behaviors

The user behavior in the field of social networking media is classified as introversive and extroversive. Image/photos uploading and messaging and sharing views are defined under extroversive behavior that may invite the attention of other users; whereas surfing profiles of other users and finding in inbox inhibits introversive behaviors that has no significant impact on others. The social behavior of a user can be judged by his interaction with his friend circle online and thus forms the Extroversive Behaviors. A large volume of social media group activity is build up or is comprised by the Introversive behaviors which forms and builds up the main backbone of user’s social attributes.

3.8 Detecting follower count

Internet Users are extensively making use of Social Media for exchanging information amidst each other which has definitely lead the social media value in context with number of shares, likes and followers. This exponential raise in public ratings makes the social media highly demanding, reputed, authoritative and dominant. There are certain fishy users that alter and increase their count of followers but it can be detected via unsupervised local neighborhood detection technique. Here the user neighborhood is identified using rigid parameters which give an evaluation having actual follower count. The suspicious user follower count is fetched from a huge Twitter sample by evaluating its neighborhood.

3.9 Data mining approaches

The Mining method works by firstly processing the available data and based on that drawing out various useful patterns which are further useful for analysis and examining. It has now become an integral and important part for many years especially in those areas where data in massive volume is involved and needs to be managed. But larger and larger the data the more intensive the approach of data mining must be implemented, mainly because of the reason of huge size the information is bearing. With this massive collection of data fetching or drawing out sober and brief and clear cut patterns is unrealistic.

3.10 Tweet Description Logic Rule Generation algorithm

Creating too many online friends now days is a social status and such users keep on seeking to build up new friends. Their likings or interests may suffix by the likings of his/her internal and external friends. In this work it uses Tweet Description Logic Rule Generation algorithm for detecting and discovering to the vulnerable user and attackers and attackers. In these experiments to find the best unit set of features that is able to Protect the vulnerable friend on Twitter. For this its required to dig out and examine these attributes that delivers best precision and is very effective in tracking the malicious users. Thereafter the follower count is tracked and the malicious user has the greatest count figure.

3.11 Algorithm

```
Step: 1 Begin
Step: 2 Let consider set of S user in community $S_n$
S = {$s_1$, $s_2$,….. $s_n$}
Input I = {$I_1$, $I_2$,,,,, $I_n$}
Step: 3 Assuming sharing threshold to 0 for every users s,
for i = 1 to $s_n$ do
u[i] = 0;
end for
Step: 4 Follows and follower count detecting
For each $S_i$ & $S_j \in OSN$ Do
$C_{ij}$ → follows and follower count;
$S_i$ & $S_j$ ←$C_{ij}$ ;
If(($S_i$ & $S_j$ )<= $C_{ij}$)
Assumed → Malicious user (may be);
If(($S_i$ & $S_j$) >= $C_{ij}$ )
Assumed → Normal user;
Step: 5 Extroversive behaviors = $\sum_i^n S_i$ i=1, 2……n
Introversive behaviors = $\sum_j^n S_j$ j=1, 2……n
Step: 6 User Identify creations
For each $S_i$&$S_j \in OSN$ Do
$I_n$→ Regular Activity;
$S_i$ & $S_j$ ←$I_n$ ;
end for
Step: 7 if any privacy vulnerable happens
Step: 8 check every user u[i] sharing percentage per day
thershold = 20;
MisActivity[$S_i$&$S_j$]= 30;
Step: 9 Find vulnerableusers in OSN;
for i = 1 to $S_n$ do
if sharing count (n[i]) ≥ threshold && $S_i$,$S_j$≥ MisActivity) && (( $S_i$ & $S_j$ )<= $C_{ij}$)then{
For each($S_j$≥ MisActivity ) do{
For each($C_{ij}$≤ Maximum ) do{
n[i] $S_j$,→ Sharing user
Remove → $S_i$, $S_j$;}
Remove (n[i])
else
n[i] → Non Sharing user
Continue (n[i], $S_i$,$S_j$)
end if }
end for} end for}
```

3.12 Advantages

❖This tool identifies the malicious user and activity.
❖Users profile will be secured and guarded from attackers.
❖Though this approach is significantly not very intense but it's a way of secure option for users account against fake users and lessening such harmful activities.

IV. Result and Discussion

The approach was focused on tracking malicious users on social media site Twitter by finding efficient attributes for detection. Privacy hacking is a serious issue in social media since few users are responsible in fiddling with others privacy and making wrong use of it.

The solution to this issue is presented as the Tweet Description Logic Rule Generation algorithm that tracks and detects suspicious and harmful user in social groups. Also with this algorithm the privacy attack is reduced at a larger extent resulting in providing accurate results in finding suspicious users. Various researches has been included for assembling the attributes, thereafter they are examined and analyzed first, and then they are weighted. With help of various experiments and trials least attribute set is derived with utmost precision.

Table 1: Comparison Classification Techniques

S.No	Techniques	Accuracy (%)	Time (MS)
1	Random forest	87.19	0.89
2	SVM	84.56	0.61
3	Sequential Minimal Optimization	68.45	0.94
4	Tweet Description Logic Rule Generation	93.12	0.56

Table 1, displays the outcome in Detecting vulnerability user profile processing used in Classification techniques in comparison with various Machine Learning methods like SVM, Sequential Minimal Optimization, Random forest and Tweet Description Logic Rule Generation. The Tweet Description Logic Rule Generation (TDLRG) method is more efficient and leads to better output compared to other techniques.

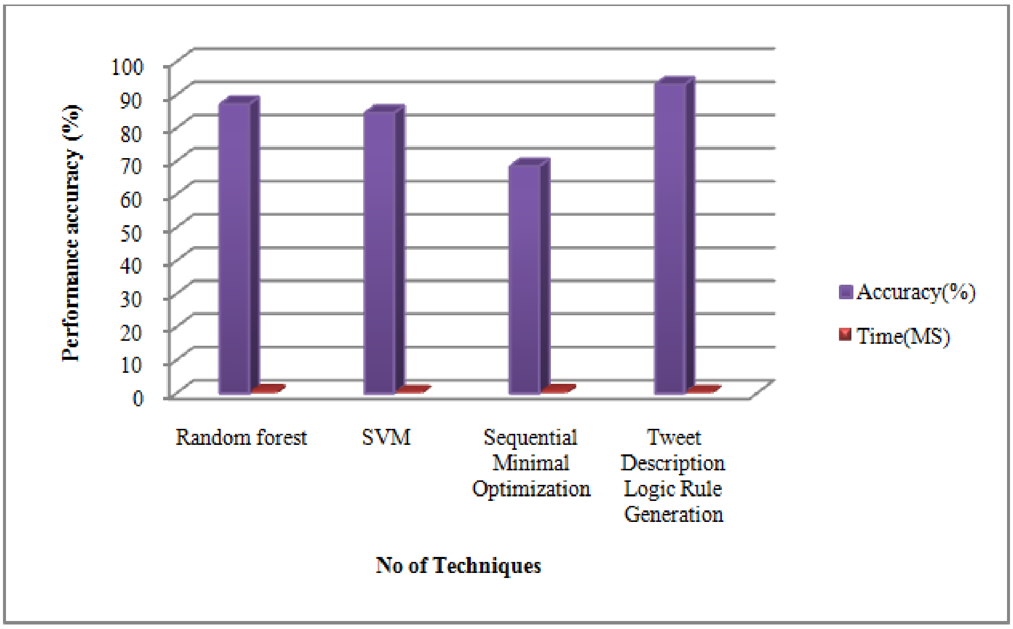

Figure 2: Comparison of Results

Figure 2, displays performance into Detecting vulnerability user profile processing used in Classification techniques comparing with varied techniques related to Machine Learning namely Random forest, Sequential Minimal Optimization, SVM and Tweet Description Logic Rule Generation. The computation results in Tweet Description Logic Rule Generation (TDLRG) method performing effectively compared to other methods.

Table 2: Comparison of Performance evolution

S.No	Techniques	Datasets Size				
		1000	2000	3000	4000	5000
1	Random forest	8.3	8	8.1	7.8	7.2
2	SVM	8.7	8.4	8.1	7.7	7.3
3	Sequential Minimal Optimization	8	7.6	7.3	6.9	6.6
4	Tweet Description Logic Rule Generation	9.3	9.4	9.1	8.7	8.4

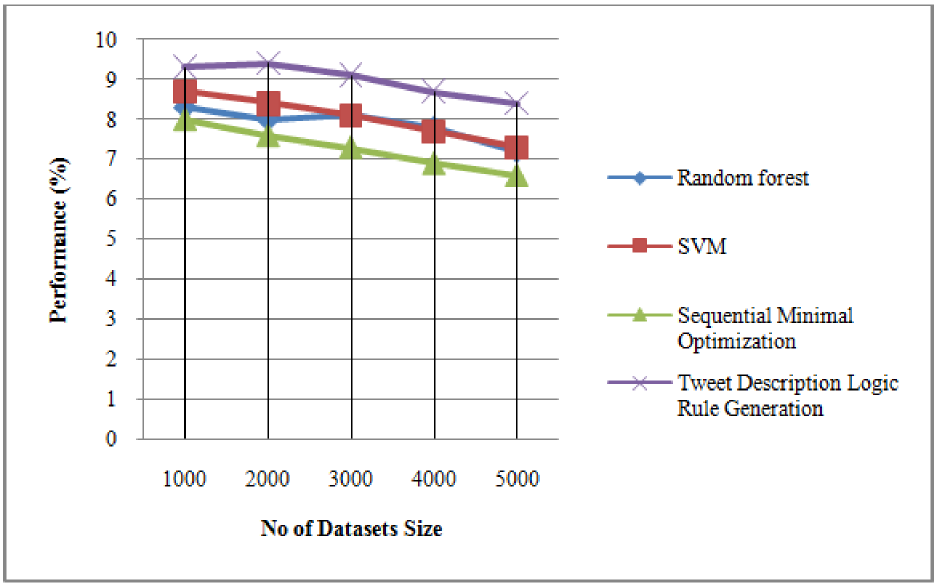

Figure 3: Graph of Performance evolutions

Table 2, Figure 3 depicts the Performance evolution comparison in contrast with other methods namely Decision tree, Random forest, and Web Description Logic Rule Generation. The suggested approach that implements Web Description Logic Rule Generation (WDLRG) reveals great outcome in comparison with others.

Actual time based datasets that holds a size of 5000 datasets the curve displays a figure of 8.4points for the Accuracy Performance. In case of size with 1000 datasets, the curve displays a figure of a point of 9.3 that depicts the network performance. This means that in the network provided, in case of least dataset size, there is Maximum Performance and with a high Datasets size the performance is minimum.

V. Conclusion

It can be claimed and put forth that the world of Social Media has drastically transformed one's lifestyle but has also become a bane. It's like a boon as one can instantly communicate and share any information worldwide with anyone. But bane in a sense that one must be careful against unauthenticated and heinous users as there occurs a high risk of privacy and security related issues. To help out the OSN users our proposed method of detecting these malicious users makes aware and assures protected and guarded accounts. It detects the link between genuine users and fraud ones. Based on Twitter, the research proposes a methodology for the detection of malicious users and safeguarding the genuine accounts from the attackers. The basis for this approach was determining the effective attributes for tracking purpose. Various researches has been included for assembling the attributes, thereafter they are examined and analyzed first, and then they are weighted. With help of various experiments and trials least attribute set is derived with utmost precision. It's concluded that Tweet Description Logic Rule Generation technique eliminates heinous users from social media. Also it is evident from the research work that our strike can accommodate Twitter user's security with great precision.

References

[1]. Malik Mateen, Muhammad Aleem, Muhammad Azhar Iqbal, Muhammad Arshad Islam, "A Hybrid Approach for Spam Detection for Twitter", IBCAST, 2017, pp. 466 – 471.

[2]. M. Verma and S. Sofat, "Techniques to detect spammers in twitter-a survey", IJCA, Vol. 85, No. 10, 2014, pp. 27 - 32.

[3]. ZHENG Guojun, JIA Wenchao, SHI Jihui, SHI Fan, ZHU Hao, LIU Jiang, "Design and Application of Intelligent Dynamic Crawler for Web Data Mining", IEEE, pp. 1098–1105.

[4]. Mitch Macdonald, Richard Frank, Joseph Mei, and Bryan Monk, "Identifying Digital Threats in a Hacker Web Forum", IEEE/ACM ASONAM, 2015, pp. 926–933.

[5]. Anupama Aggarwal, Saravana Kumar, Kushagra Bhargava, Ponnurangam Kumaraguru, "The Follower Count Fallacy: Detecting Twi.er Users with Manipulated Follower Count", In Proceedings of SAC 2018: Symposium on Applied Computing , Pau, France, April 9–13, 2018 (SAC 2018), 8 pages. DOI: 10.1145/3167132.3167318.

[6]. Manoel Horta Ribeiro, Pedro H. Calais, Yuri A. Santos, Virg´ılio A. F. Almeida,Wagner Meira Jr., "Characterizing and Detecting Hateful Users on Twitter", ICWSM 2018.

[7]. Chaoliang Li ,Shigang Liu, "A comparative study of the class imbalance problem in Twitter spam detection", Concurrency and Computation: Practice and Experience, 30, 5, (2018). 17 September 2017 https://doi.org/10.1002/cpe.4281

[8]. Girisha Khurana, MrMarish Kumar "Review: Efficient Spam Detection on Social Network", IJRASET 2015, Vol. 3, Issue. 6, pp. 76 – 80.

[9]. Mohammad Rakib Amin, MehedeeZamanMd, Shohrab Hossain "Behavioral Malware Detection Approaches for Android" IEEE ICC 2016.

[10]. F. Bravo-Marquez, E. Frank, and B. Pfahringer, "From Unlabelled Tweets to Twitter-specific Opinion Words", Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval - SIGIR'15, pp. 743–746, 2015.

[11]. Amir Javed, Pete Burnap, Omer Rana, "Prediction of drive-by download attacks on Twitter", Information Processing and Management, 2018., pp. 1 – 13.

[12]. Burnap P, Javed A, Omer F. Rana & Awan M S, "Real-time classification of malicious URLs on twitter using machine activity data", IEEE/ACM ICASNAM 2015, pp. 970 – 977.

[13]. Robinson, W. Russia hacked pentagon's joint chiefs of staff and shut down its email system — daily mail online, 2015.

[14]. Cao C, & Caverlee J, "Detecting spam URLs in social media via behavioral analysis", Advances in Information Retrieval, pp. 703 – 714.

[15]. Chao Chen, Jun Zhang, Yang Xiang, and Wanlei Zhou, "Spammers are becoming 'smarter' on twitter", IT Professional, Vol. 18, No. 2, pp. 66 – 70.

[16]. Sagar Gharge, Manik Chavan, "An integrated approach for malicious tweets detection using NLP", ICICCT 2017, pp. 435 - 438.

[17]. Claudia Meda, Edoardo Ragusa, Christian Gianoglio, "Spam detection of Twitter traffic: A framework based on random forests and non-uniform feature sampling", 2016 IEEE/ACM ASONAM 2016, pp. 811 – 817.

[18]. Mehwish Nasim, Andrew Nguyen, Nick Lothian, Robert Cope, and Lewis Mitchell, "Real-time Detection of Content Polluters in Partially Observable Twitter Networks", International World Wide Web Conference Committee, 2018.

[19]. Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben Y Zhao, and Yafei Dai, "Uncovering social network sybils in the wild", 2011.

[20]. Xia Hu, Jiliang Tang, and Huan Liu, "Online Social Spammer Detection", AAAI 2014, pp. 59 – 65.

[21]. Kyumin Lee, Jalal Mahmud, Jilin Chen, Michelle Zhou, and Jeffrey Nichols, "Who will retweet this?: Automatically identifying and engaging strangers on twitter to spread information", ACM, pp. 247 – 256.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

S. Revathi. " Detecting Vulnerable User in Twitter Using Tweet Description Logic Rule Generation." IOSR Journal of Computer Engineering (IOSR-JCE) 20.5 (2018): 27-35.