An Extended Work Architecture for Online Threat Prediction in Tweeter Dataset

Dr. Savita Kumari Sheoran[1] and PartibhaYadav[2]

Indira Gandhi University Meerpur, Rewari (Haryana) - INDIA

Abstract:
Social networking platforms have become a smart way for people to interact and meet on internet. It provides a way to keep in touch with friends, families, colleagues, business partners, and many more. Among the various social networking sites, Twitter is one of the fastest-growing sites where users can read the news, share ideas, discuss issues etc. Due to its vast popularity, the accounts of legitimate users are vulnerable to the large number of threats. Spam and Malware are some of the most affecting threats found on Twitter. Therefore, in order to enjoy seamless services it is required to secure Twitter against malicious users by fixing them in advance. Various researches have used many Machine Learning (ML) based approaches to detect spammers on Twitter. This research aims to devise a secure system based on Hybrid Similarity Cosine and Soft Cosine measured in combination with Genetic Algorithm (GA) and Artificial Neural Network (ANN) to secure Twitter network against spammers. The similarity among tweets is determined using Cosine with Soft Cosine which has been applied on the Twitter dataset. GA has been utilized to enhance training with minimum training error by selecting the best suitable features according to the designed fitness function. The tweets have been classified as spammer and non-spammer based on ANN structure along with the voting rule. The True Positive Rate (TPR), False Positive Rate (FPR) and Classification Accuracy are considered as the evaluation parameter to evaluate the performance of system designed in this research. The simulation results reveals that our proposed model outperform the existing state-of-arts.

Keywords:
Twitter, Threat detection, Spam, Malware and Cosine Similarity.

1. Introduction

Present day human socialisation activities as dominated by social networking sites, where he can create profiles, make a connection with other users as well as converse with them. There are numbers of networking sites present in social network space such as Twitter, Facebook, LinkedIn, and WhatsApp which facilitate users to share information in the form of audio, video, text including images [1]. Twitter, as a networking platform, is intended to help people converse through the tweets consisting of text message or http links limited to 140 characters. This exchange of tweets is the medium of communication among the users. With leap and bound hype in Twitter users, it becomes an attractive target for spammers where spam becomes the largest concern in this social networking platform [2]. Grier et al. (2010) have stated that 0.13% of the spam messages posted on Twitter and are double as compare to the email spam making it a central topic for research community engaged in regime of internet security. After creating a profile on social sites, the existing user enables to search for the new user according to his/her interest. In Twitter, the network is composed of social users, who connect with each other after replying or mentioning another user in their comments [3]. The structure of the user on Twitter is depicted in figure 1. From a given figure, the structure of Twitter working in which a user's tweets are only available to their followers. While forwarding tweets to a follower at the third level of hierarchy, his/her followers are rendered by the blue circle can access the user's tweets, when third follower in the second level of tweet structure re-tweets, users who are not followers of the original user can also access the tweet. As envisaged from the figure, Twitter's "user" → "follower" structure having a tree structure in which the flow of information goes down the tree. It should also be noted that unlike other social networks, the relationship among users and their followers may be asymmetric. Particularly when a user gets followers, neither of them will automatically follow each other; therefore, the user does not necessarily have to access all the tweets of their followers [4].

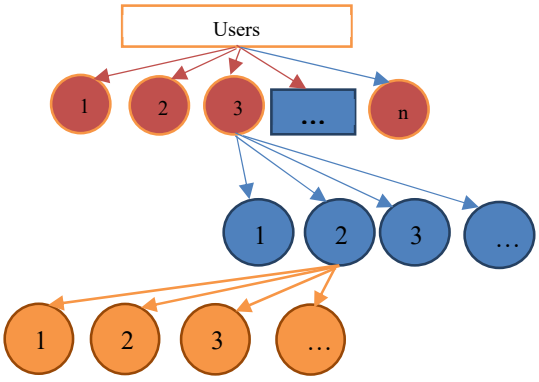


Figure 1: User Structure on Twitter

Spammers not only try to advertise products, but they have also been actively involved in misleading users by clicking on malicious links. Spammers on Twitter employ an

Manuscript received January 5, 2021
Manuscript revised January 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.1.14

enormous number of techniques to attract users into clicking malicious URLs [5]. As the users are free to share their information, so the groups are formed among such users who are more active and share information rapidly as compare to less connected users. Attackers can easily access relevant or personal information like passwords and bank details of genuine social users. Recently Twitter has been emerged as a newer platform for the cybercriminal as well as performs a number of malicious activities like Spam, phishing, Malware and so on [6].

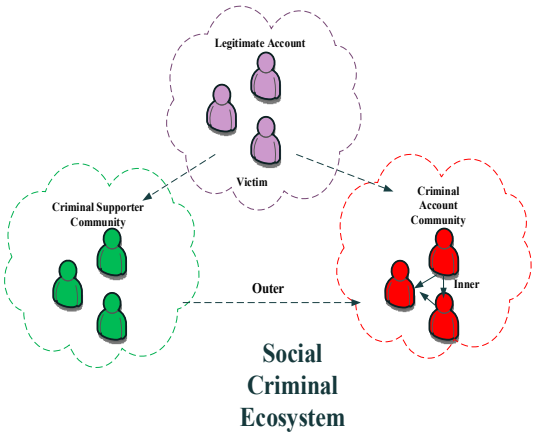


Figure 2: Structure of the Socio-Criminal Ecosystem

The representation of the social-criminal ecosystem of the social network is given in figure 2, particularly for the Twitter site where which a separate community is established by criminal users by using a unique user ID, including a supporter community encircled by the green circle that supports such users outside the community of criminal accounts [7]. There are two types of relations depicted in figure *viz.* inner and outer. Inner relationship indicated the interrelation between the criminal accounts linked through social means. The outer relationship is to represent the relationship between the criminal account and criminal supporters. This is consumed to reveals the features of close friendship, including criminal accounts. The threats that have been identified in this work are: Malware and Spam [8].The user can face various types of attacks while using Online Social Networking (OSN) sites. These attacks might be generated by the trusted third party or attacker can also used fake accounts for insulting social user. These attackers randomly send friend requests to other social media users. If the request is accepted by the victim, communication between attacker and these victim friends is started. For instance, someone who uses social engineering to invade a computer network may try to gain the trust of formal users and let them leak information that endangers network security. Social engineers trusted on both social help as well as their weaknesses. During emergency, social engineers call an authorized person and need to access the network immediately. In social networks malicious links posted by unwanted users to attract user traffics termed as Malware. Both of these untrustworthy activities are depicted in below sub-sections:

1.1. Spam

It is envisaged from the existing work that most of the Spam are found in emails but social sites also suffer from Spam or malwares. Spam can affect the information in a number of ways such as by sending them irrelevant information in the form of advertisement or by transferring messages continuously to the same IDs on the social network. In majority of existing works the Spam can be detected by collecting similarity data and extracting a pattern based upon data features. According to Beutel et al. (2013) spam has been detected by analyzing the relationship between users and the pages along with the time of the instant at which the edge has been initialized in the social graph [9]. Another similar work is done by Ahmed et al. (2012), which used the graph-based approach to show the connection among the social user, i.e., nodes, with their communication by the edge of the graph [10]. The weight of the edge is corresponding to real and fake user interactions in the form of shared URLs, pages, active friends. In our approach, spam detection is performed by using the Optimization-based Machine Learning (ML) technique as shown in figure 3.

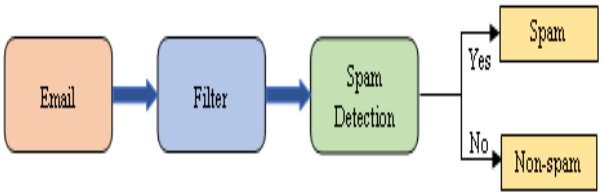


Figure 3: Workflow of Spam Anti-filter

1.2. Malware

It is a common type of cyber attack in which malicious software executes unauthorized actions. The malicious software encompasses a number of certain types of attacks named as ransomware, spyware All these are type of code which is enter into the network with the aim to affect genuine users or steal information from the authorized users. So it's challenging for a user and requires being overcome [11]. In prior days spammers utilized outmoded social networks such as email and newsgroups to affect the information of normal users through inserting worms and after installing them. The other sites that are also being affected by this attack are; Facebook and Twitter [12]. The way which is being followed by Malware to affect the information is represented in figure 4.

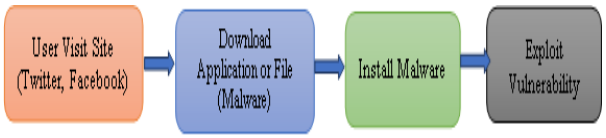


Figure 4: Malware Threat

In this paper, a framework has been developed for the detection of Spam including Malware particularly for the Twitter site. This mechanism is based on cardinal principle to find similarities among the extracted features such as crime-related keywords along with normal keywords including the URL features. The extracted features are optimized using a novel fitness function of the Genetic Algorithm (GA). After getting the optimized features such as URL the machine learning classifier namely Support Vector Machine (SVM) is trained according to the optimized features that lead to an improved detection method. The remaining section of this paper is organized as; the state of the art of malicious attacks like Spam and Malware detection techniques have been described in section 2. The explanation of the presented approach in steps is provided in section 3. The simulation has been performed in MATLAB based upon the considered parameters are described in section 4. Finally section 5 concludes the paper followed by a list of bibliographic reference.

2. Related work

There have been a number of approaches introduced in literature to provide detection and protection of social networks against Spam. The most known feature based on which it is identified the illegal one listed by Blanzieri et al. (2008)[13].To detect and classify a message as a malicious one, the techniques named content filtering are utilized by Sahamiet al. (1998) [14]. In social media platforms such as Twitter and Facebook the method of content-based is not effective because the Spam generally contains only a few words including URLs. So the URL blacklisting approach has been utilized by a few researchers with the aim to filter the Spam but this scheme is not yielding desired results due to heavy processing time as stated by Grier et al. (2010) [15]. Due to this reason a novel approach has been implemented to filter out Spam along with Malware from Twitter using optimization by utilizing the ML approach. Song et al. (2011) have utilized relation features, i.e. distance and interconnection among the transmitter and receiver of social user for detection of data as malicious or non-malicious. A list of Spam and non-spam has been identified and then trained the classifier on the basis of extracted features. The findings indicated that most of the Spam had been produced through the account rather than the receiver [16].Lin et al. (2017) have introduced an ML-based scheme for the detection of Spam on the basis of ground truth value as well as provided enhanced performance. The designed Spam detection Twitter model has been observed for scalability and performance has been analyzed on the basis of True Positive, False Positive, F-score, and Accuracy using distinct sizes of data with sort processing time [17]. Hai and Hwang (2018) have utilized deep learning as a classifier for the detection of Malware on the basis of their malicious activities. The obtained accuracy of detection 98.75% as compared to the other existing approaches have been achieved in their work [18]. Kaur and Sabharwal (2018) have utilized a forward neural network as the classifier which has been trained on the basis of extracted features *(+ve and –ve)* in social networks. To overcome the complexity of extracted features, genetic-based optimization has been utilized to get the optimized value [19].Jain et al. (2019) have presented a DL based spam detection system. Techniques such as CNN and Long Short term Memory (LSTM) approaches have been used. The designed model has been supported by the semantic words using WorldNet and ConcetNet approach. These techniques performed well with improved accuracy and F-score value [20].

In nutshell, the above literature survey reveals that the Spam and Malware message detection filters the document in a short message by utilizing a small number of feature sets. To accomplish this goal, the presented present used a slightly distinct mechanism from traditional content Spam analysis on the basis of the word model package. The approach used in this study is presented in the subsequent section.

3. Proposed Extended Work Architecture

In this research an innovative scheme has been developed through hybridization of GA with SVM approach to detect Spam and Malware users in Twitter network. The features of tweets has been refined as well as optimized on the basis of the fitness function of GA and utilized dynamically with the aim to train the structure of SVM. In the traditional approach the features are generally refined using a pre-processing approach and then applied to the complete dataset. SVM is an enhanced scheme that selects features dynamically for single users instead of utilizing similar features for the whole database. This happens because the features for each user are different that can segregate users from one another. However, a feature has a strong differentiating effect on one user group; it is observed that it's not required that different groups also have a similar effect. A discussion on link sharing rates reveals that new accounts and Spam accounts has typically higher than average rate for link sharing. After analyzing users average

link sharing rate, it has been observed that spam users took advantage of more images from news sites. If only the number of image sharing is filtered, it is impossible to find spam users but if this filter is applied to users with more sharing links than other users, the image sharing filter will become very different. The conclusion of this work is that each feature has a different impact on a single user group. As discussed in the above work we have to classify each user on the basis of URL shared and then grouped each URL on the basis of their features by utilizing the SVM technique along with the GA optimization approach. The designed secure framework for the Twitter site against Spam and Malware is depicted in figure 5 and steps followed .are mentioned there in subsequent sub-sections.

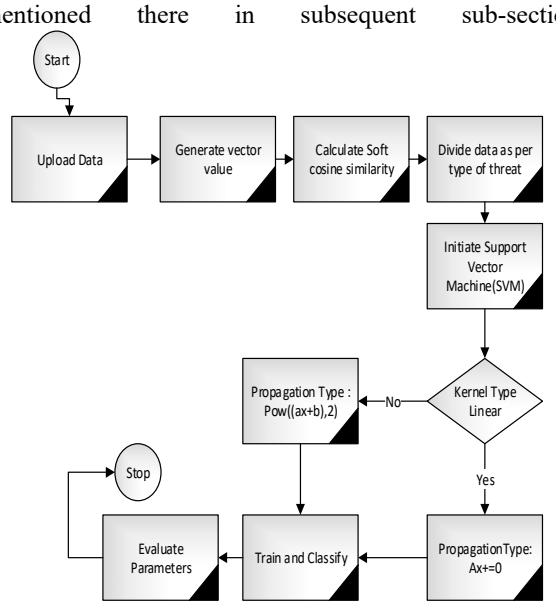


Figure 5: Proposed Workflow

3.1.Upload Test Data

Initially a mix data is being gathered from open social network site. The dataset composed of total 200K tweets including their URL. An assumption has been made that all tweets involves URL with the aim to attract social users towards malicious sites like Malware and Spam downloading [21].

3.2.Stop Word Removal

The stop words from collected data is removed through contrasting each row involves in the dataset with the stored stop words list has initiated from the stop words collected from website [22]. Some stop words utilized in the presented approach are listed in Table 1 below.

Table 1: List of Stop Word used in Research Study

"An"	"If"	"During"	"Before"	"After"	"Above"
"And"	"Or"	"Below"	"To"	"From"	"Up"
"But"	"Because"	"Down"	"In"	"Is"	"It"
"While"	"Until"	"Else"	"Than"	"Too"	"Very"
"Off"	"Of"	"Own"	"Can"	"Off"	"Will"
"The"	"At"	"Just"	"Don"	"Should"	"Now"

At the beginning the gathered data is uploaded and compared with the list of stored stop words in the database. If the words from the uploaded data are matched with the database words thereafter these words are removed retaining only the data that involves only the meaningful informative words [23]. The algorithm developed for stop words is provided below:

Algorithm: Stop Word Removal from t_{UD}

Where, t_{UD}→ User data from on the basis of social users
Sw_fd→The data free from stop words

```
initialize
    Upload dataset of stop words (Sw)
    Set, Count = 1
    For x = 1 → All tUD do
        For y = 1 → All Sw do
            If tUD(x, y) = Sw (x, y)
    Sw_fd (Count)=tUD (x,y)
                Count+= 1
            Else
    Sw_fd= ' '
    End_If
    End_For
    End_For
    Return: Sw-fd as a list of data that are free from stop words
    End_Func
```

3.3.Mention Ratio/URL as Content-based Features

In this work the mention ratio i.e. '@' and '#' have been utilized as properties of content including the URL. Since these are required features utilized by Twitter and also consumed by malicious users to mislead the normal tweet users. So the removal of such symbols from the tweet is necessary.

3.4.Mention Ratio

The Twitter users can be tagged through @ symbol. This feature is also been misused by spammers or malwares to mislead the authorized users. Spammers or malwares encourage and attract normal users to gain knowledge about the malicious sender [24]. The mathematical expression to compute the mention ratio is given in equation (1).

3.5.Word to Vector

After filtering stop words determine '#' and '@' in the uploaded tweets and then apply word to vector method. This model comes under the process of word embedding with the key objective is to study the vector representation obtained after word to vector method. In this method, the word is represented in vector forms on the basis of similarities among words in the test document [25].

3.6.Soft Cosine Similarity

This similarity measure is an extension of cosine similarity which can be used to measure similarity between two word vectors (x,y) by considering feature pairs in the defined vector space model. The difference between cosine and soft cosine similarity measure is that cosine similarity measured the cosine of the angle between the two vectors (x,y), whereas soft cosine similarity measure, analysed the similarity based on the vectors feature values. Let x and y are the two vectors, the soft cosine similarity calculated between these two is examined by equation (1).

$$Soft\ Cosine\ (x,y) = \frac{\sum_{i,j}^{N} S_{ij} x_i y_j}{\sqrt{\sum_{i,j}^{N} S_{ij} x_i x_i} \sqrt{\sum_{i,j}^{N} S_{ij} y_i y_j}} \quad \text{..... (1)}$$

Here, S_{ij} = similarity $(feature_i, feature_j)$

If $S_{ij} = 1$ and $S_{ij} = 0$ for i ≠ j then,

$$Soft\ Cosine\ (x,y) = \frac{\sum_{i,j}^{N} x_i y_j}{\sqrt{\sum_{i,j}^{N} x_i x_i} \sqrt{\sum_{i,j}^{N} y_i y_j}} = \frac{\sum_{i,j}^{N} x_i y_j}{\sqrt{\sum_{i,j}^{N} x_i^2} \sqrt{\sum_{i,j}^{N} y_i^2}} =$$

$\frac{x \,.\, y}{||x||||y||}$ = Cosine Similarity

It is to clear from the given formula that when there is no similarity among features of the objects; soft cosine measure becomes proportional to the regular cosine similarity. The algorithm for soft cosine similarity is provided below:

Algorithm: Soft-Cosine Similarity

Required Input:	Data_Value← Raw Data_Value in which similarity needed
Obtained Output:	$Sim_{Soft\text{-}Cos}$← Soft-Cosine similarity between Data_Value

Start
Similarity is stored in an empty array, $Sim_{Soft\text{-}Cos}$ = []
Sim-count = 0
For m = 1 → Length (Data_Value)
Current_Processing_Element = Data_Value (m)
For n = m+1 → Length (Data_Value)
Calculate the Soft-Cos similarity using given equation
L = |Soft-Cos (Current_Processing_Element) - Soft-Cos (Data_Value (n))|
$Sim_{Soft\text{-}Cos}$ [sim_count, 1] = Current_Processing_Element
$Sim_{Soft\text{-}Cos}$ [sim_count, 2]= Data_Value(n)
$Sim_{Soft\text{-}Cos}$ [sim_count, 3]=L
Increment array by one
End – For
End – For
Return: $Sim_{Soft\text{-}Cos}$// output examined by Soft_Cosine similarity between Data_Value
End – Function

3.7.Genetic Algorithm (GA)

Genetic Algorithm (GA) is a basic heuristic technique which works on Darwin's theory of evolution, and is also termed as evolutionary algorithm that computes the best solution on the basis of natural selection and crossover as given in figure 6. This feature selection approach is used to select the row features of the tweets obtained by utilizing Soft Cosine similarity measure index. Feature selection is one of the important task which is helpful into improve the training accuracy of the classifier such as Support Vector Machine (SVM) is used to train the system on the basis of optimized features according to the created fitness function provided by equation (2).

$$Fitness\ function = \begin{matrix} 1 & if\ (1-e)\times Fs > Ft \\ 0 & otherwise \end{matrix} \quad \text{..... (2)}$$

Were, Fs →Recent Attributes
Ft →Total of attributes in a given row

If the row values of the matrix satisfy the designed function, it is classified as spam or non-spam. If not so, then repeat the steps for the next subsequent row. By following these

steps, the redundant data has been filtered. Therefore, we obtained a reduced row that contained useful [26]. The steps followed by GA are shown in figure 6.

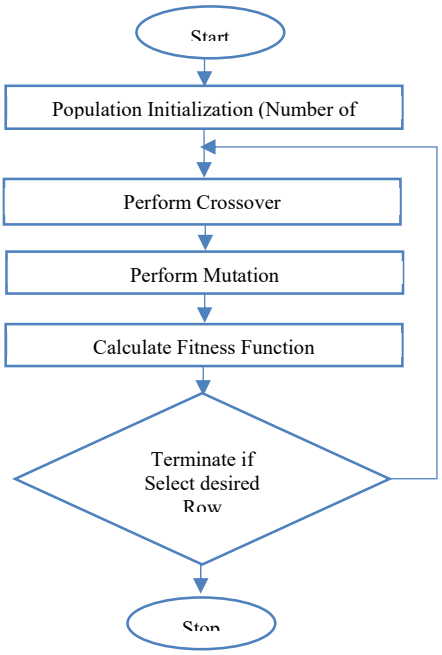


Figure 6: Genetic Algorithm (GA) Process

GA randomly produces a set of populations. A distinct gene is involved by each individual and therefore responsible for distinct solution corresponds to particular problem which is again encoded by the chromosomes. As per the requirement an objective function is decided. In GA mainly there are involves three operators such as: Selection, Crossover and Mutation.

(i) *Selection:* It is used for selection of individuals from the present generation that later consumed for upcoming generation. The selection of individuals with high fitness is eliminated, and individuals with fitness less than or equal to the fitness function is selected. The value of the row with the lowest value is called the parent and helps to generate new members called children.
(ii) *Crossover:* It generated a structured *exchange* of optimized data between solutions transforming 'good' data into enhanced ones.
(iii) *Mutation:* It helps to search best row using mutation threshold function.
(iv) *Termination:* The process of selecting attributes is terminated when the required row is selected and classified as spam and non-spam data [27].

The workflow of Genetic optimization approach is written in algorithmic form as below:

Algorithm: Genetic Algorithm (GA)

Input:	$Data_{features}$← Extracted feature from used Dataset
	$Fitness_{function}$←Fitness function
Output:	Of_D←Optimized Feature Data

Feature Selection initiated
Upload Data, Feature Data (f_D) = upload set of features
To optimize the F_d, Genetic approach is utilized
Decide basic operators and parameters of GA: Population Size (P) describing the number of properties
cr_O – Crossover Operators
m_O – Mutation Operators
Of_D – Optimized Feature Data
$Fitness_{function}$ = 1 (1-e) X Fs>Ft
0 Otherwise
Where, e = Mutation error generated in the process of optimization
F_s : It is current feature in f_D
F_t: It is the threshold featurewhich is equal to the average of all f_D
Compute the value off_D in terms of R
Set, Of_D = []
For x in range of R
$F_s = f_D(i) = Selected_{Feature}$
$F_t = Threshold_{Feature} = \sum_{i=1}^{R} f_D(x)$
$F(f) = Fit\_Fun\ (F_s, F_t)$
N_var = Count of all the variables
Best_prob = Of_D= GA (F(f), T, N_var, Set up of GA
End_For
Return: Of_Das an Optimized data
End_Function

3.8.Support Vector Machine (SVM)

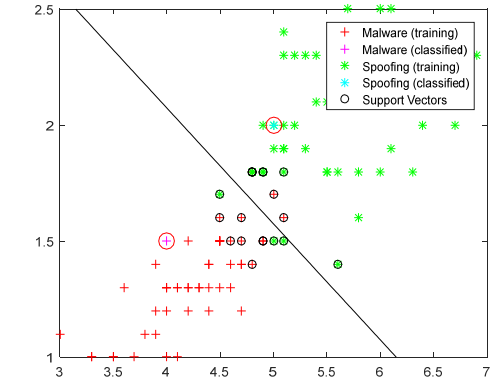
SVM is a supervised ML approach, which is used here to distinguish Twitter data as malicious and spoofing. SVM used a hyper plane structure to create difference between the malware as a spoofing from the normal data. Let the SVM is train by providing input in terms of (x_1y_1), (x_2y_2),……$(x_my_m) \epsilon P^N \times \{-1, +1\}$.

x_i→ Input value
y_i→Enter the assigned class for range $\{-1, +1\}$
Initially, separation between normalized and malicious data has been performed using linear function, If data is not

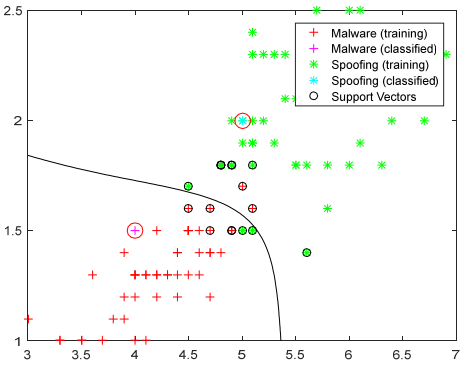
classified by linear function, then non linear function (($\varphi: P^N \rightarrow P^M$)) can be used with a novel feature space of P^M.
Using this as a non-linear function, the obtained hyper plane can be separated as per the equation (3)

$$\omega \times \varphi(x) + y = 0 \quad \text{..... (3)}$$
$\omega \epsilon P^M$ and yϵP

Training can be said to be optimal with the best hyper plane and the smallest error. To separate data from each other kernel function can be used. In this research work we consider Linear and Polynomial Kernel to train and to test the network as shown in Figure 7 (a) and (b). In which the red coloured plus (+) sign and green coloured cross (×) is represent the training data of SVM for Malware and Spoofing. To make a distinction classified data is represented by light pink coloured plus (+) and light green colored cross (×) and the data closest to hyper plane which termed as support vector is represented by circle. The data separation is done by polynomial kernel is more accurate as compare to linear kernel because of its straight line [28-29].



(a) Training



(b) Testing

Figure 7: Twitter data using Linear and Polynomial Kernel (a) Training and (b) Testing

4. Results and Discussions

After training the spam and malware detection of the social data, testing of the designed system has been performed by uploading the tweets as test data followed by measurement of similarity among the uploaded documents using Soft Cosine as similarity measure. The obtained data are compared with the data stored into the SVM database. Here, voting rule has been applied as a cross-validation scheme.

In addition to the ANN classifier, a voting classifier is also used. If the maximum value has been obtained, the true negative (TN) and false negative (FN) values are calculated for the uploaded data. If the classification result is equal to the test result, the true positive (TP) and false positive (FP) are calculated. Results based on TN, TP, FN and FP (for example, true positive rate (TPR), false positive rate (FPR) and classification accuracy) has been checked and will be discussed in this section.
The implementation of the work has been designed using MATLAB as simulator. Optimization, classification with similarity measures tools have been used for experimental purpose. For stop word removal Natural Language toolkit has been used. The performance has been measured based on the following parameters as represented by the equation (4), equation (5), and equation (6).

$$TPR = \frac{T_P}{T_P + F_N} \quad \text{..... (4)}$$

$$FPR = \frac{F_P}{F_P + T_N} \quad \text{..... (5)}$$

$$\text{Classification Accuracy (\%)} = \frac{T_P + T_N}{T_P + F_N + F_P + T_N} \text{ .. .. (6)}$$

Here, T_P→ Amount of tweets that are actually spam or malwares and also predicted as malicious.

F_N→ Amount of tweet that is being predicted as real but is spam and contains malwares.

F_P→Amount of tweets that is in reality valid but classified as affected one (Spam or malwares)
T_N→ Amount of appropriately predicted real tweets.

Table 2: True Positive Rate Count

Number of Uploaded Tweets	*Soft-cosine Similarity*	*GA With SVM*	
100	*0.8768*	*0.835*	
200	*0.8791*	*0.846*	
300	*0.8826*	*0.865*	
400	*0.8894*	*0.872*	
500	*0.8967*	*0.879*	
600	*0.9012*	*0.882*	
700	*0.9124*	*0.889*	

Figure 8 represents the TPR values examined for various techniques such as Soft Cosine and GA with SVM approach and the best results are illustrated by the proposed work that is GA with SVM in combination with hybrid similarity measure. TPR represents the tweet that is the sub part of spam or malware of the tested dataset that classified correctly. The average percentage TPR computed for Soft Cosine and GA with SVM approach are; 86% and 89% correspondingly.

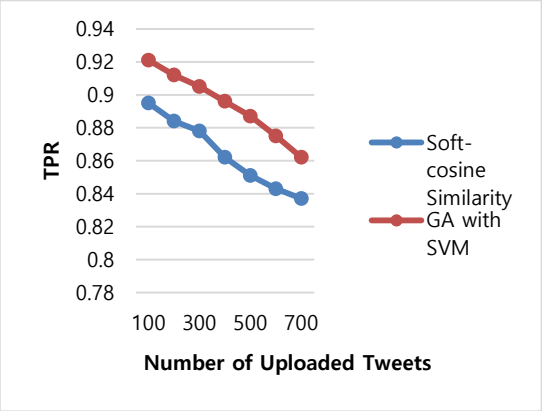


Figure 8: True Positive Rate for Uploaded Tweets

FPR is the amount of incorrectly classified datasets divided by the total number of existing relevant datasets that means it is the subpart of negative instances that classified incorrectly. This parameter represents the rate of tweets that are being posted by genuine user and have been predicted as spam or malware by the user accurately. The examined recall for the uploaded tweet ranges from 100 to 700 in the step of 100 is shown in Figure 9. The average FPR rate in percentage examined for the Soft Cosine similarity, and GA with SVM are; 89% and 86% correspondingly.

Table 3: False Positive Rate Count

Number of Uploaded Tweets	*Soft-cosine Similarity*	*GA With SVM*
100	*0.8768*	*0.835*
200	*0.8791*	*0.846*
300	*0.8826*	*0.865*
400	*0.8894*	*0.872*
500	*0.8967*	*0.879*
600	*0.9012*	*0.882*
700	*0.9124*	*0.889*

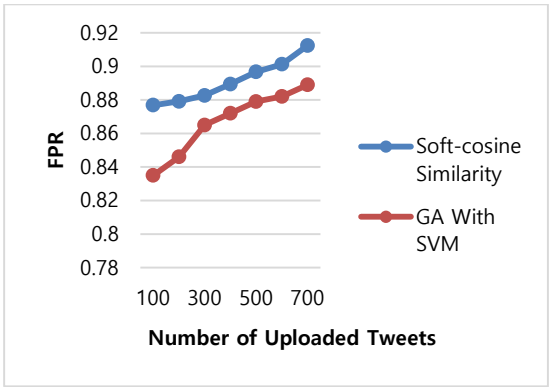


Figure 9: False Positive Rate for uploaded Tweets

Table 4: Classification Accuracy (%)

Number of Uploaded Tweets	**Soft-cosine Similarity**	**Accuracy**
100	0.843942	0.8869
200	0.861372	0.8961
300	0.852883	0.8992
400	0.873349	0.9072
500	0.886909	0.9124
600	0.894377	0.9235
700	0.909753	0.9561

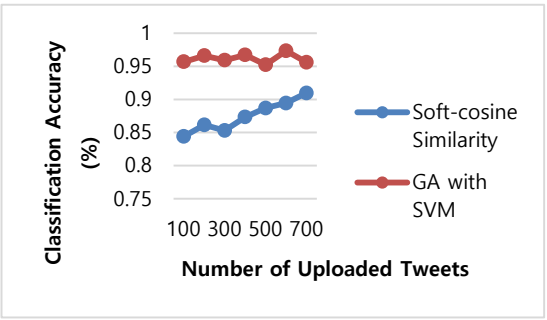


Figure 10: Classification Accuracy (%)

Accuracy is necessary to determine the percentage of accurately identified instances. The examined values of accuracy are illustrated in figure 10. The examined values of Classification Accuracy (%) for applied Soft Cosine similarity and GA with SVM are; 87% and 96% respectively.

Table 5: Comparison of Parameters

Proposed Work			Murugan and Devi (2018) [39]			Madisetty S. and Desarkar M.S. (2018) [38]		
TPR	FPR	Classification Accuracy	TPR	FPR	Classification Accuracy	TPR	FPR	Classification Accuracy
89%	86%	96%	86%	88%	93%	86%	96%	95%

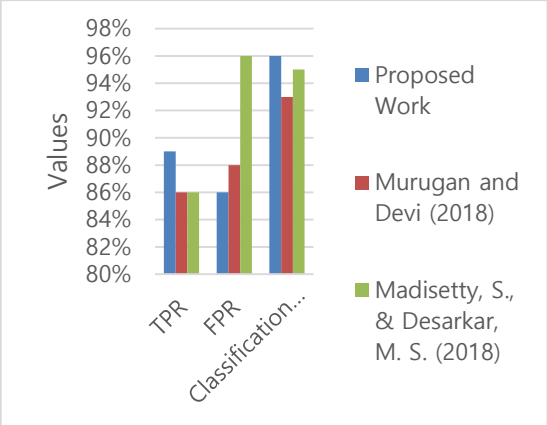


Figure 11: Comparison of Proposed Work with Existing Work

Comparison of the proposed work with the existing state-of-arts *viz.* Murugan and Devi (2018) and Madisetty, S., and Desarkar, M. S. (2018) is represented in figure 11 with the values summarized in Table 5. From the graph, it is clearly seen that, the values examined for TPR and Classification Accuracy (%) using the hybrid GA with SVM approach is higher compared to the existing, Murugan and Devi (2018) work there is an increment of 3.4 % and 4.03 % respectively and there is also an 2% degradation in terms of FPR. By considering the Madisetty, S., and Desarkar, M. S. (2018) work there is an enhancement in terms of TPR and Classification Accuracy (%) of 2.99% and 0.98% correspondingly along with in terms of FPR our work outperforms with reduction by amount of 9.8%.

5. Conclusion

Social media networks are the most frequently used means for information exchange as well as to advertise the business and many more throughout the entire world. Besides, the benefits of social media sites, malicious and malware activities are spread by the spammers into the network and have been used later to misguide the genuine users. In this paper, we have designed a secure threat prevention (Spam and malware) system for Twitter site. The work has used the advantage of Soft Cosine similarity measure. Based on the similarity tweets, the features have been optimized using novel GA approach and has been classified using Support Vector Machine with voting algorithm as a cross validation scheme. From the experiment, it has been observed that the examined TPR, FPR and Classification Accuracy in percentage of 89%, 86% and 96% has been achieved.

References

[1] Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. International journal of environmental research and public health, 14(3), 311.

[2] Phua, J., Jin, S. V., & Kim, J. J. (2017). Uses and gratifications of social networking sites for bridging and bonding social capital: A comparison of Facebook, Twitter, Instagram, and Snapchat. Computers in human behavior, 72, (pp. 115-122).

[3] Panek, E. T., Nardis, Y., &Konrath, S. (2013). Defining social networking sites and measuring their use: How narcissists differ in their use of Facebook and Twitter. Comput. Hum. Behav., 29(5), 2004-2012.

[4] Myers, S. A., Sharma, A., Gupta, P., & Lin, J. (2014, April). Information network or social network? The structure of the Twitter follow graph. In Proceedings of the 23rd International Conference on World Wide Web (pp. 493-498)

[5] Wang, D., Navathe, S. B., Liu, L., Irani, D., Tamersoy, A., &Pu, C. (2013, October). Click traffic analysis of short url spam on twitter. In 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (pp. 250-259). IEEE.

[6] Thomas, K., Grier, C., Song, D., and Paxson, V. (2011, November). Suspended accounts in retrospect: an analysis of twitter spam. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 243-258).

[7] Yip, M., Shadbolt, N., & Webber, C. (2012, June). Structural analysis of online criminal social networks. In 2012 IEEE International Conference on Intelligence and Security Informatics (pp. 60-65). IEEE.

[8] Kay, A. (2006). Social capital, the social economy and community development. Community Development Journal, 41(2), (pp. 160-173).

[9] Beutel, A., Xu, W., Guruswami, V., Palow, C., &Faloutsos, C. (2013, May). Copycatch: stopping group attacks by spotting lockstep behavior in social networks. In Proceedings of the 22nd international conference on World Wide Web (pp. 119-130).

[10] Ahmed, F., &Abulaish, M. (2012, June). An mcl-based approach for spam profile detection in online social networks. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 602-608). IEEE

[11] Rieck, K., Holz, T., Willems, C., Düssel, P., &Laskov, P. (2008, July). Learning and classification of malware behavior. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 108-125). Springer, Berlin, Heidelberg.

[12] Mohtasebi, S., &Dehghantanha, A. (2011, July). A mitigation approach to the privacy and malware threats of social network services. In International Conference on Digital Information Processing and Communications (pp. 448-459). Springer, Berlin, Heidelberg.

[13] Blanzieri, E., &Bryl, A. (2008). A survey of learning-based techniques of email spam filtering. Artificial Intelligence Review, 29(1), (pp. 63-92).

[14] Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998, July). A Bayesian approach to filtering junk e-mail. In Learning for Text Categorization: Papers from the 1998 workshop (Vol. 62, (pp. 98-105).
[15] Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010, October). @ spam: the underground on 140 characters or less. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 27-37).
[16] Song, J., Lee, S., & Kim, J. (2011, September). Spam filtering in twitter using sender-receiver relationship. In International workshop on recent advances in intrusion detection (pp. 301-317). Springer, Berlin, Heidelberg.
[17] Lin, G., Sun, N., Nepal, S., Zhang, J., Xiang, Y., & Hassan, H. (2017). Statistical twitter spam detection demystified: performance, stability and scalability. IEEE access, 5, (pp.11142-11154).
[18] Hai, Q. T., & Hwang, S. O. (2018). An efficient classification of malware behavior using deep neural network. Journal of Intelligent & Fuzzy Systems, 35(6), (pp. 5801-5814).
[19] Kaur, J., &Sabharwal, M. (2018). Spam detection in online social networks using feed forward neural network. In RSRI conference on recent trends in science and engineering 2, (pp. 69-78.
[20] Jain, G., Sharma, M., & Agarwal, B. (2019). Spam detection in social media using convolutional and long short term memory neural network. Annals of Mathematics and Artificial Intelligence, 85(1), 21-44.
[21] https://www.kaggle.com/uciml/sms-spam-collection-dataset. Accessed on 22.02.2020.
[22] https://gist.github.com/sebleier/554280 Accessed on 22.02.2020.
[23] Wilbur, W. J., &Sirotkin, K. (1992). The automatic identification of stop words. Journal of information science, 18(1), 45-55.
[24] Anger, I., &Kittl, C. (2011, September). Measuring influence on Twitter. In Proceedings of the 11th international conference on knowledge management and knowledge technologies (pp. 1-4).
[25] Yang, X., Macdonald, C., &Ounis, I. (2018). Using word embeddings in twitter election classification. Information Retrieval Journal, 21(2-3), 183-207.
[26] Sidorov, G., Gelbukh, A., Gómez-Adorno, H., & Pinto, D. (2014). Soft similarity and soft cosine measure: Similarity of features in vector space model. Computación y Sistemas, 18(3), 491-504.
[27] Salehi, S., Selamat, A., &Bostanian, M. (2011, July). Enhanced genetic algorithm for spam detection in email. In 2011 IEEE 2nd international conference on software engineering and service science (pp. 594-597). IEEE.
[28] Sivanandam, S. N., &Deepa, S. N. (2008). Genetic algorithm optimization problems. In Introduction to genetic algorithms (pp. 165-209). Springer, Berlin, Heidelberg.
[29] Feng, W., Sun, J., Zhang, L., Cao, C., & Yang, Q. (2016, December). A support vector machine based naive Bayes algorithm for spam filtering. In 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC) (pp. 1-8). IEEE.
[30] Diale, M., Van Der Walt, C., Celik, T., &Modupe, A. (2016, November). Feature selection and support vector machine hyper-parameter optimisation for spam detection. In 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech) (pp. 1-7). IEEE.
[31] Madisetty, S., &Desarkar, M. S. (2018). A neural network-based ensemble approach for spam detection in Twitter. IEEE Transactions on Computational Social Systems, 5(4), (pp. 973-984).
[32] Murugan, N. S., & Devi, G. U. (2018). Detecting streaming of Twitter spam using hybrid method. Wireless Personal Communications, 103(2), (pp. 1353-1374).

About Authors

Dr. Savita Kumari Sheoran is presently an Associate Professor in Department of Computer Science & Engineering, Indira Gandhi University Meerpur, Rewari – INDIA. She had graduated her Ph.D. in Computer Science from Banasthali Vidhyapeeth (Rajasthan) – INDIA and posses more than fifteen years of experience in teaching and research supervision in various reputed Institutes and Universities in India and abroad. Dr. Sheoran has authored various books / chapter and published about 65 research papers in international and national journals conferences / seminars / workshops. She is an active researcher having interest in research domains of Mobile Computing, Social Media Computing, Big Data Analytics and Crime Prediction.

Ms. Partibha Yadav presently pursuing her Ph.D. in Computer Science at Indira Gandhi University Meerpur, Rewari (India) in the field of Security Threat Detection in Social Media Networks. She holds M. Tech. in Computer Engineering and poses teaching experience in reputed College/University. She has about a dozen of published research papers/attended conference.