JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Improved and Dynamic Distance Measure Algorithm to detect the Fake and Clone Social Networking Accounts

Penmatsa Hemalatha[1], Mr.Ch. Dileep Chakravarthy[2],

Student, Department of Information Technology, Sagi Rama Krishna Raju Engineering College,
Bhimavaram, AP, India.

Assistant Professor, Department of Information Technology, Sagi Rama Krishna Raju Engineering College,
Bhimavaram, AP, India.

Abstract: Social media is a fast growing field in present days and more data is generating day by day. Social media is a platform for users to communicate with each other from anywhere in the world. Millions of new people are joining in the social media platforms. Online social media sites (OSMS) such as Face book, Twitter are used by the users to store and share their personal information. With the generation of huge data everyday many fake users are creating fake or cloned profiles to damage the social networking platforms with these profiles. Fake or cloned profiles are detected based on the set of rules that can classify fake or genuine profiles. Many existing approaches are used to find the fake profiles such as C4.5 and Cloned detection indexes. With these systems there is a lack of accuracy in result analysis. To overcome this we have proposed a new approach called as Linear Support Vector Machine (SVM) which is a dynamic and improved approach to find the fake profiles in OSMS. To improve the performance of fake profile detection, a robust preprocessing is integrated to the Linear SVM. The dataset is collected from the kaggle website which consists of 5000 fake profiles. Results show the performance of proposed system.

Keywords: C4.5, Fake and Clone profiles, Linear SVM, Online Social Media Sites(OSMS).

1 INTRODUCTION

People on social networking sites sharing their feelings, daily news, comments, opinions, events and trying to post everyday activities such as travelling, drinking, eating etc. Malicious users or clone users check every profile and analyze the activities by checking their profiles, timeline messages, and tweets and place the hateful messages about the original users. Fake users try to spread the fake news, links that are fake photos etc. Many Online Social Network (OSN) users don’t know about this fake profiles and accounts by accepting their requests and creating problem to the original profile.

From the last few years, OSN's such as facebook, twitter and instagram have improved the millions of users to use their platforms that are used to communicate with friends, family and missing persons to share their interests, opinions and other information relating to society, politics etc. Some OSN platforms provide the messages to share with other users with limited number of characters which is seen in twitter. Twitter limited the tweets with 160 characters. At present, twitters having 340 million users.

Nowadays, many spam persons these people are also called as malicious users or fake users creating lot of miscommunication between the users by spreading the fake news, bullying, personal abuse, hacking the bank accounts by using the malicious links. It is very important to overcome all these fake user activities and a powerful and dynamic tool is required to detect these fake profiles. Many machine learning algorithms are developed to detect the clone and fake profiles to detect and predict. Cloned profiles are created by the hackers with same name and profile pictures. In this paper, the new dynamic distance measure algorithm is developed to detect the fake or clones profiles. The proposed algorithm uses the linear SVC that can improve the accuracy and decrease the error rate.

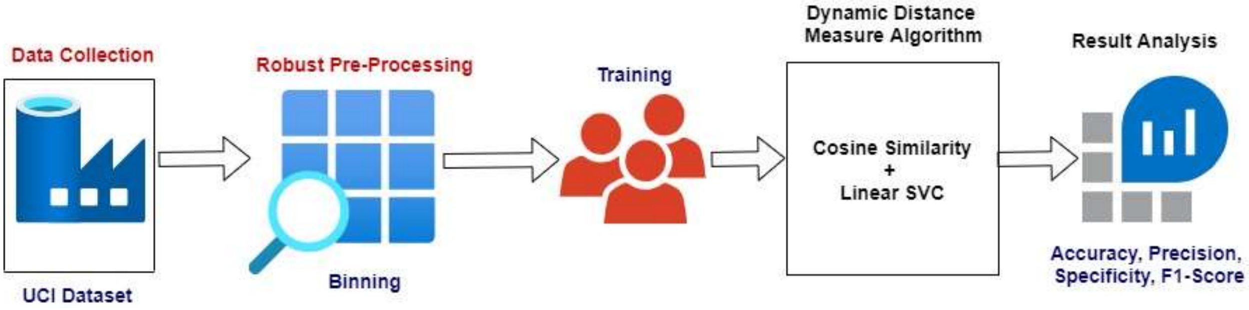


Figure: 1 Architecture of proposed model

2 LITERATURE SURVEY

Georgios Kontaxis et al., [2] proposed a model to check whether the clients have become casualty to cloning assault or not. Data is extricated from client profile and a hunt is made in OSN to discover profiles which match to that of client profile and a closeness score is determined dependent on shared characteristic of property estimations. In the event that the closeness score is over the limit esteem, the specific profile is named as clone.

Brodka, et al., [3] proposed two novel techniques for distinguishing cloned profiles. The main strategy depends on the similitude of trait esteems from unique and cloned profiles and the subsequent technique depends on the organization connections. An individual who questions that his profile has been cloned will be picked as a casualty. Then, at that point regarding name as essential key, a hunt is made for profiles with the very name as that of casualty, utilizing inquiry search. Likely clone (Pc) and the Victim profile (Pv) are thought about and comparability S is determined. In the event that S(Pc, Pv) >Threshold, profile is suspected to be a clone. In the check step, the client does it physically as he probably is aware which his unique profile is and which one is a copy.

Cresci S et al., [4] proposed about the audited probably the most pertinent existing highlights and rules (proposed by Academia and Media) for counterfeit Twitter accounts discovery. They have utilized these standards and highlights to prepare a bunch of AI classifiers. Then, at that point they have thought of Class A classifier which can viably arrange unique and phony records.

Ahmed El Azab et al., [5], have proposed a characterization technique for distinguishing counterfeit records on Twitter. They have gathered some compelling highlights for the recognition interaction from various research and have sifted and weighted them in first stage. Different investigations are directed to get least arrangement of traits which gives precise outcomes. From 22 ascribes, just seven credits were chosen which can viably identify counterfeit records and have applied these components on characterization procedures. An examination of the order procedures dependent on outcomes is made and the one which gives most exact outcome is chosen.

Counterfeit characters made by people or bots are recognized utilizing AI models which are subject to designed highlights. It was assessed whether promptly accessible and designed highlights that are utilized for the fruitful discovery, utilizing AI models, of phony personalities made by bots or PCs can be utilized to identify counterfeit characters made by people. Managed AI calculations require a dataset of highlights with a mark grouping each column or result. Highlights are accordingly the information utilized by directed AI models to anticipate a result. These highlights can be the properties found by means of APIs that depicts a solitary snippet of data about a SMP account, similar to the quantity of companions. The prescient outcomes from the prepared AI models just yielded a best F1 score of 49.75%. The AI models were prepared to utilize designed highlights without depending on conduct information [6].

Content polluters, or bots that commandeer a discussion for political or promoting objects are a known issue for occasion expectation, political decision anticipating and while recognizing genuine news from counterfeit news in web-based media information. Distinguishing this sort of bot is especially difficult. Content polluters are bots that endeavor to undercut an authentic conversation by commandeering it for political or promoting purposes. Techniques were created to recognize social bots in information utilizing just fractional data about the client and their tweet history, progressively. They researched two qualities of tweets for example worldly data and message variety. It was tracked down that content polluters in this dataset regularly coordinated their tweets together. By investigating the fleeting examples one could construe the presence of bot accounts. It was likewise discovered that bots utilized a little arrangement of URLs in their tweets [7].

In K. Patel et al., [8] several machine learning algorithms are discussed to detect the fake profiles in social media and also in social networking sites (SNS). Reinforcement learning is proposed and shows the huge accuracy when compared SVM and adaboost.

Venkatesan et al. [9] proposed the new reinforcement learning which is used to detect the bot i,e malicious profiles. Based on the feedback platform this model detects fake accounts in SNS. Arif et al. [10] proposed the unique rules based on the feature extraction technique utilized to detect spam on SNS.

S. D. Munoz et al., [11] proposed the new fake profiles detection system by extracting the features of profiles and analyze the accurate fake profiles with 96.5% detection rate. The dataset is collected from instagram with 16 metedata features from real and fake profiles.

Goswami et al., [12] discussed about the challenges that are obtained in the SNS analysis. The author proposed the new mapping analysis to detect the fake profiles in the SNS with clear understanding.

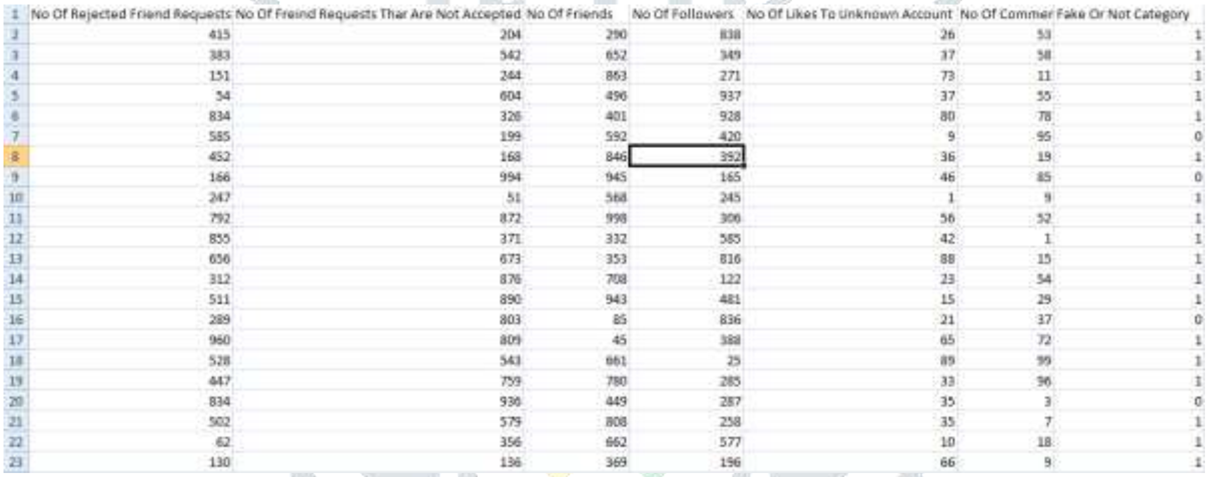
M. Smruthi et al., [13] proposed the new hybrid model which is the combination of machine learning and skin detection algorithms to detect the fake accounts in the SNS with huge accuracy.

P. Tehlan et al., [14] proposed the model which is used to detect the spam using fuzzy logic and analyze through neural network multilayer perceptron. This approach is combination of ML algorithms, fuzzy logic (FL).

F. Ahmed et al., [15] introduced the Markov Clustering (MCL) based approach for the detection of spam profiles on OSNs. The MCL is applied on Facebook profiles dataset, which includes both benign and spam profiles. This system uses the weighted graph in which profiles are represented as nodes and their interactions as edges. The weight of an edge, connecting a pair of user profiles, is calculated as a function of their real social interactions in terms of active friends, page likes and shared URLs within the network. MCL is applied on the weighted graph to generate different clusters containing different categories of profiles. Majority voting is applied to handle the cases in which a cluster contains both spam and normal profiles.

3 DATASET DESCRIPTION

The twitter profile data is collected from kaggle.com. This data consists of 5000 profiles and 9 attributes that we considered here are User id, No of Abuse Report, No of Rejected friend requests, No of Friend Requests that are not accepted, No of Friends, No of Followers, No of likes to Unknown Account, No of comments. These attributes are suitable for detecting fake profiles and these are having more relevant features.



1	No Of Rejected Friend Requests	No Of Freind Requests Thar Are Not Accepted	No Of Friends	No Of Followers	No Of Likes To Unknown Account	No Of Commer	Fake Or Not Category
2	415	204	290	838	26	53	1
3	383	542	652	349	37	58	1
4	151	244	863	271	73	11	1
5	54	604	496	937	37	55	1
6	834	326	401	928	80	78	1
7	585	199	592	420	9	95	0
8	452	168	846	392	36	19	1
9	166	994	945	165	46	85	0
10	247	51	568	245	1	9	1
11	792	872	998	306	56	52	1
12	855	371	332	585	42	1	1
13	656	673	353	816	88	15	1
14	312	876	708	122	23	54	1
15	511	890	943	481	15	29	1
16	289	803	85	836	21	37	0
17	960	809	45	388	65	72	1
18	528	543	661	25	89	99	1
19	447	759	780	285	33	96	1
20	834	936	449	287	35	3	0
21	502	579	808	258	35	7	1
22	62	356	662	577	10	18	1
23	130	136	369	196	66	9	1

Figure 2: Twitter profile data

The algorithm follows the several steps to improve the performance of fake profile detection**.**

4 ROBUST DATA PREPROCESSING

This is very important step in machine learning that helps to process the dataset by removing the missing values, irrelevant data and extract the accurate meaningful data from the dataset. In twitter fake profile dataset which is collected from kaggle, the pre-processing technique cleans the raw data which is creates the better platform for training models. By using this step, the data is converted to understandable and better format that can be readable by the algorithms.

Some transformation algorithms applying to original data can be useful for binning. Standardization method is a widely-used technique for numerous machine learning algorithms to resolve the problem of different data distributions. Quantile Transformation (QTF), MinMaxScaler (MMS), and logarithmic computations scalers are considered to convert data before binning. Quantile Transformation is implemented to combine with EQW in these experiments. QTF is considered as a robust pre-processing technique because it can reduce the effect of the outliers in fake profile dataset. Samples in test and validation sets which are smaller or larger than the fitted range then will be assigned to the bounds of the output distribution. Another algorithm illustrated in this study is MinMaxScaler, to make a comparison with QTF and logarithmic computations. MinMaxScaler converts each feature to a given range by (1) and (2) formulas:

$$X_{std} = \frac{X - \min(X)}{\max(X) - \min(X)} \quad - - - (1)$$

$$X_{scaled} = X_{std} * (\max - \min) \quad - - - (2)$$

Functions which perform the transformation as above are now available in scikit-learn library.

5 TRAINING

After undergoing the preprocessing step, 80% of both profiles (fake and clone) are used to prepare a training dataset and 20% of both profiles are used to prepare a testing dataset. In this training step the data is analyzed and observed the fake and non-fake profile patterns which are input and output variables. We find the efficiency of the classification algorithm using the training and testing datasets.

6 ALGORITHM

6.1 Linear Support Vector Machine (Linear SVM)

Linear SVM is a supervised machine learning technique used to classify the data. The basic idea of linear SVM is to maximize the margin of data by discovering the best possible separating hyper plane which is linear. One side of data belongs to one class and the other side of data belongs to another class. Here the data is simply separable and there is no complexity while the separation of data into classes. Linear SVM provides higher accuracy than the other classification techniques.

In our proposed work, we use Linear SVM method that applies a linear kernel function to perform the classification of dataset classes into normal and fake profiles using a hyper plane. The Linear Kernal Function is defined as follows

$$F(x) = w^T x + b - - - (3)$$

w- Represents the weight vector which is used to minimize,

x- Represents the data selected for classification.

b- Represents the linear coefficient estimated from the training data

T- Represents training.

The above equation is used to initialize the decision border of the data.

6.2 Profile Similarity Measures

In order to improve the efficiency and accuracy of our work, we then calculate the cosine similarity of the profiles. This module detects clones based on Attribute and Network similarity. User profile is taken as input. User identifying information is extracted from the profile. Profiles which are having attributes matching to that of user’s profile are searched. Similarity index is calculated and if the similarity index is greater than the threshold, then the profile is termed as clone, else normal.

This similarity function is used to measure the k number of profiles. Given k vectors of attributes, $X_1, X_2, X_3 \ldots X_n$, the cosine similarity, n represents the number based on the attributes, cos(θ), is represented using a dot product and magnitude as

$$\text{Similarity} = \cos(\theta) = \frac{X_1 * X_2 * X_3 * X_n}{||X_1|||X_2|||X_3|||X_n||}$$

$$= \frac{\sum_{i=1}^{n} X_i B_i}{\sqrt{\sum_{i=1}^{n} {X_1}_i^{\,2}}\sqrt{\sum_{i=1}^{n} {X_2}_i^{\,2}\sqrt{\sum_{i=1}^{n} {X_3}_i^{\,2}\sqrt{\sum_{i=1}^{n} {X_2}_i^{\,2}}}}} ---(4)$$

Where, X_i and Y_i are components of vector X and Y respectively.

6.3 Steps for Linear SVM Algorithm

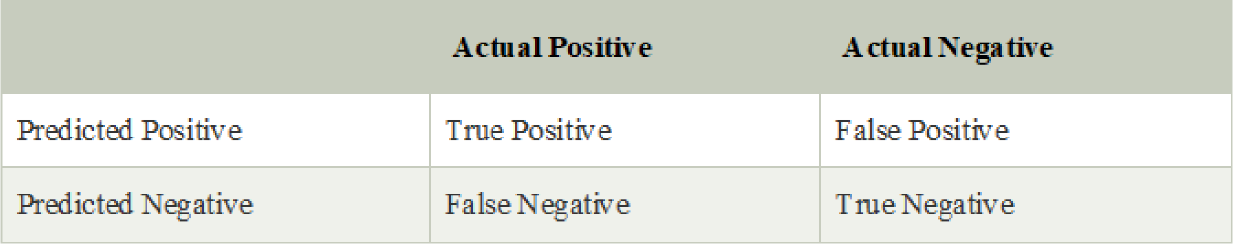
```
Input: training dataset $T_d$.
        K- Applied model.
        F(X) - linear kernel function.
        C for tuning margin and errors of SVM
Output: classification results based on given dataset $T_d$.
Begin
Creating each profile as p which is denoted by $P_1, P_2, P_3 \ldots .. P_n$ and their centers $c_1, c_2 \ldots c_k$.
For i←1 to K do
$lSVMi = SVM(Td, F(X), C)$
End
Return $LSVM - model = \{(c_1 SVM_1), (c_2 SVM_2), \ldots \ldots ., (c_k SVM_k)$
Apply equ: (3)
Apply equ: (4)
End
```

7 EVALUATION METRICS

7.1 Performance Evaluation using Confusion Matrix

- The confusion matrix provides us a matrix/table as output and describes the performance of the model.
- It is also known as the error matrix.

- The matrix consists of predictions result in a summarized form, which has a total number of correct predictions and incorrect predictions. The matrix looks like as below table:



	Actual Positive	Actual Negative
Predicted Positive	True Positive	False Positive
Predicted Negative	False Negative	True Negative

7.2 Precision

The proportion of actual positives which are correctly identified is the measure of the precision. It relates to the ability of the test to identify positive results.

$$\mathbf{Precision} = \frac{\text{No. of TP}}{\text{No. of TP} + \text{No. of TN}} - - - (5)$$

7.3 F1 Measure

This is a measure of a model's accuracy on a dataset. It is used to evaluate binary classification systems, which classify examples into 'positive' or 'negative'.

$$\mathbf{F1\ Measure} = 2 \times \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} - - - (6)$$

7.4 Accuracy: This will calculate the overall accuracy of the result.

$$\mathbf{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} - - - (7)$$

7.5 Recall: Appropriate when **minimizing false negatives** is the focus.

$$\mathbf{Recall} = \frac{\text{TP}}{\text{No. of TP} + \text{No. of FN}} - - - (8)$$

Table 1: These are the measures calculated based on the given datasets. From these measures the performance is analyzed. These values are obtained from applying algorithms on twitter profile dataset.

Algorithm	TP	FP	TN	FN
CDSim	140	110	650	65
C4.5	132	99	622	56
Linear SVC	120	80	598	42

Table 2: Performance of Classifiers

Algorithm	F1- Measure	Accuracy	Recall	Precision
CDSim	61.54	81.87	68.29	17.72
C 4.5	63.01	82.95	70.21	17.45
Linear SVM	66.30	85.48	74.07	16.71

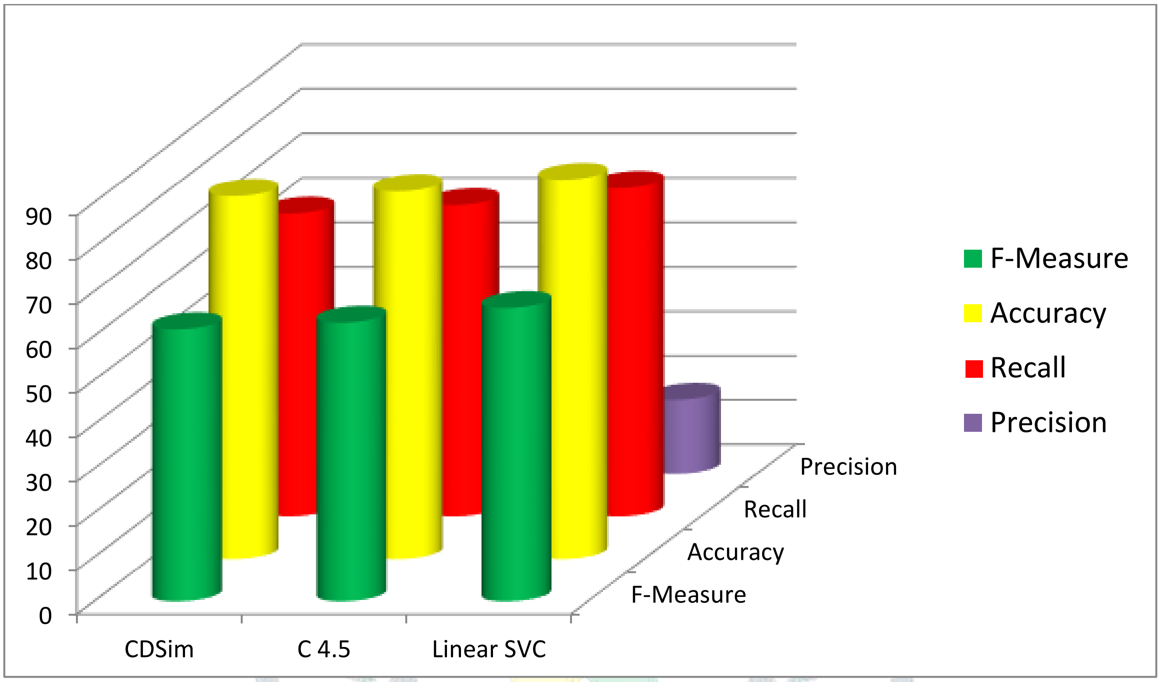


Figure 5: Performance of Classifier

8 CONCLUSION

In this paper, Linear SVM is applied on twitter profile data which overcome the fake account detection problem on Twitter with using linear SVM, and comprehensive experiments are done with cosine similarity functions and their combinations. According to the experimental results, the use of Linear SVM in detecting fake accounts yields successful results. Another strong reason to use Linear SVM is, this will find the very complex relationships among the data without taking huge transformations. This algorithm can find more accurate results and have more ability to work on small and complex datasets.

REFERENCES

[1] Sowmya P and Madhumita Chatterjee, "Detection of Fake and Cloned Profiles in Online Social Networks", Proceedings 2019: Conference on Technologies for Future Cities (CTFC)

[2] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", 2013.

[3] Piotr Brodka, Mateusz Sobas and Henric Johnson, "Profile Cloning Detection in Social Networks", 2014 European Network Intelligence Conference

[4] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angello Spognardi, Maurizio Tesconi, "Fame for sale: Efficient detection of fake Twitter followers", 2015 Elsevier's journal Decision Support Systems,Volume 80.

[5] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set", World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering Vol:10, 2016.

[6] Van Der Walt, Estee, and Jan Eloff. "Using machine learning to detect fake identities: bots vs humans." IEEE Access 6 (2018): 6540-6549.

[7] Sever Nasim, Mehwish, Andrew Nguyen, Nick Lothian, Robert Cope, and Lewis Mitchell. "Real-time detection of content polluters in partially observable Twitter networks." arXiv preprint arXiv:1804.01235 (2018).

[8] K. Patel, S. Agrahari and S. Srivastava, "Survey on Fake Profile Detection on Social Sites by Using Machine Learning Algorithm," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 1236-1240.

[9] S. Venkatesan, M. Albanese, A. Shah, R. Ganesan, and S. Jajodia, "Detecting stealthy botnets in a resource-constrained environment using reinforcement learning," in Proc. Workshop Moving Target Defence, 2017, pp. 75_85.

[10] M. H. Arif, J. Li, M. Iqbal,and K. Liu, "Sentiment analysis and spam detection in short informal text using learning classifier systems," in Soft Computing. Berlin, Germany: Springer, 2017, pp. 1_11.

[11] S. D. Munoz and E. Paul Guillen Pinto, "A dataset for the detection of fake profiles on social networking services," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 230-237.

[12] Goswami, A., Kumar, A. Challenges in the Analysis of Online Social Networks: A Data Collection Tool Perspective. Wireless Pers Commun 97, 4015–4061 (2017).

[13] M. Smruthi and N. Harini, "A Hybrid Scheme for Detecting Fake Accounts in Facebook", International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 5S3, February 2019.

[14] P. Tehlan, R. Madaan and K. K. Bhatia, "A Spam Detection Mechamism in Social Media using Soft Computing," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 950-955.

[15] F. Ahmed and M. Abulaish, "An MCL-Based Approach for Spam Profile Detection in Online Social Networks," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 602-608.