Suspicious Account Detection Using Machine Learning Techniques

Afshan Anjum[1] | B.Anvesh kumar[2] |Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College of Engineering, Karimnagar,
[2] Assistant Professor,Department of MCA,Vaageswari College of Engineering, Karimnagar,
[3] Professor & HoD,Department of MCA, Vaageswari College of Engineering, Karimnagar,

To Cite this Article
. Afshan Anjum, B.Anvesh kumar, Dr.V.Bapuji, **"Suspicious Account Detection Using Machine Learning Techniques"** *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp124-132*
Article Info
Received: 04-06-2023 Revised: 09-07-2023 Accepted: 17-07-2023 Published: 27-07-2023

ABSTRACT

In the current generation, social networking sites have become an integral part of life for most people. On social networking sites such as Facebook, Instagram, and Twitter, thousands of people create their profiles daily, interacting with each based on the classification for detecting Suspicious accounts on social networks. Here the traditionally way has been used for different classification methods in this paper.

The implementation of machine learning and natural language processor (NLP) techniques are done to enhance the accuracy of others regardless of location and time. Our goal is to understand who encourages threats in social networking profiles. To determine which social network profiles are genuine and which ones are Suspicious profiles, The support vector machine (SVM) and Naves bays algorithm technique can also be applied to achieve this strategy.

KEYWORDS: *Online Social network, Classification, Natural language processing (NLP), Facebook, Support vector machine (SVM).*

INTRODUCTION

Millions of participants and billions of minutes of usage make social networking a well-liked online network. However, there are many security issues and protection concerns, particularly with the threat of identity theft. The privacy regulations imposed by social networking service providers tend to be inadequate, making them vulnerable to manipulation and misuse. The advance in technology has led to an evolution of knowledge. Machine learning algorithms have emerged, emphasizing analyzing obstacles as well as data. Although handheld devices and social media outlets revolutionize communication and improve decision-making, they tend to be prone to violation of privacy. To identify users who conceal their identities. Research has focused on trained and untrained machine learning algorithms, with the vast majority accomplishing a precision of 50%- 96%. The techniques in use have become effective at ensuring personal information about users from harmful behavior.

In addition to the impact of the increasing popularity of social networking sites on the web, individuals are becoming more susceptible to increasing security dangers and weaknesses including being subjected to violations of privacy, fraud identities, unsafe programs, suspicious profiles, and harassment based on gender. To resolve those problems, security providers provide protective systems and surveillance technologies. Online interaction monitoring tools like those offered by monitoring make it easy to identify users and address security issues. as open social network (OSN) usage increases, it will become critical to address such problems by developing feasible solutions.

I. RELATED WORK

Social media platforms have gotten progressively More widespread since users upload data as well as personal data on websites. Multiple techniques have been employed by hackers and cybercriminals to obtain user account credentials and private data Researchers and organizations are working on tools to spot suspicious accounts and malicious activities to protect users, researchers have used semantic analysis and spectacular temporal analytics to organize, detrimental Poster and compare them with real profiles.

Websites like Facebook[8] offer their users a range of privacy setting to safeguard their personal information and their immune system guarantees users identity. With the use of features like friend request frequency, link information time stamps, and reflective policy assignments tools. Yang et all were able to spot Profiles Ahmed and Frappe[10] have detected suspicious accounts.

Online social network privacy and security have been increasing scrutiny in recent years to increase user security and privacy in social networks. Operator security firms and researchers have suggested several solutions, including adding authentication procedures, providing customization privacy settings, and providing security against hackers, spammers, social bots, identity cloning, phishing, and other threats.

Examples include the Immune System from Facebook. Graph centrality metrics, honey profiles, the Pox extension, Yang et al.'s method to identify false profiles, the Reflective Policy Assessment tool, and the Gamekeeper Facebook application are just a few examples of the remedies that academic studies have suggested for various social network concerns.

As social networks grow in popularity, researchers are employing machine-learning techniques to identify suspicious accounts. The proposed framework in figure1, which demonstrates an order of actions that must be understood to be different depending on the location of phony profiles with dynamic gain from the input of the result provided by the arrangement calculation.

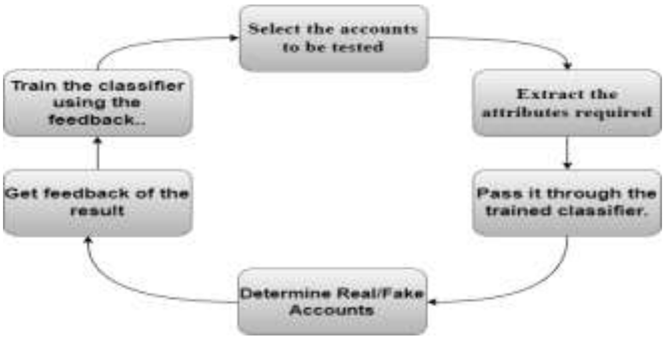

Select the accounts to be tested
Extract the attributes required
Pass it through the trained classifier.
Determine Real/Fake Accounts
Get feedback of the result
Train the classifier using the feedback..

Fig 1. Cycle for Detection

The cycle for the detection of suspicious accounts step-by-step procedure as follows.

1.The selection of the profiles to be characterized prepares the framework for the rest of the process.

2.When the accounts are chosen the highlights

3.The highlights from the accounts are encouraged to prepare to train, and classifiers are taken from them.

4.The highlights are sustained as the input into the classifiers which turns out to be more increasingly precisely showing the result of suspicious accounts.

III. METHODOLOGIES

Several methods exist to stop people from engaging in malicious activity on social media. Specific approaches are employed to identify suspicious accounts to stop customers from using dangerous apps in this section. Different techniques to recognize suspicious accounts are examined. Payable One illustrates multiple approaches to suspicious accounts on social media platforms can be found.

A hybrid approach is used for experiments with some machine learning techniques such as logistic regression, Random Forest, and k-nearest Neighbours (K-NN) to find optimal solutions. For fine-tuning, further support vector machine and Natural language processing (NLP) is also taken into consideration.

Logistic regression and neural networks have also been used, but the most efficient way is Natural Language Processing and Support Vector Machine, which, trains the data by applying a support vector machine independently and on natural language processing methods used to analyze the result of classification techniques to find the accuracy rate. Iteratively the dataset is applied to the model to cross-validate the technique to avoid situations or overfitting as in the validation technique dataset.

3.1 SVM ALGORITHM:

Support Vector Machine is one of the most popular machine learning algorithms, which is used for classification as well as regression problems. However, here primarily classification problems in machine learning are used for finding out the fraud accounts in social media network Support Vector Machine (SVM) algorithm is to create the best decision for finding out the profiles which are being used in social networking. It is easy to put the new data point in the correct category in the future. The best decision boundary is called a hyperplane Support Vector Machine (SVM) chooses the extreme points and the vectors that help in creating the hyperplane. These extreme cases are called support web tasks, and hence algorithm is shrunk as support, but consider the below figure in which two different categories are classified using the decision boundary and hyperplane.

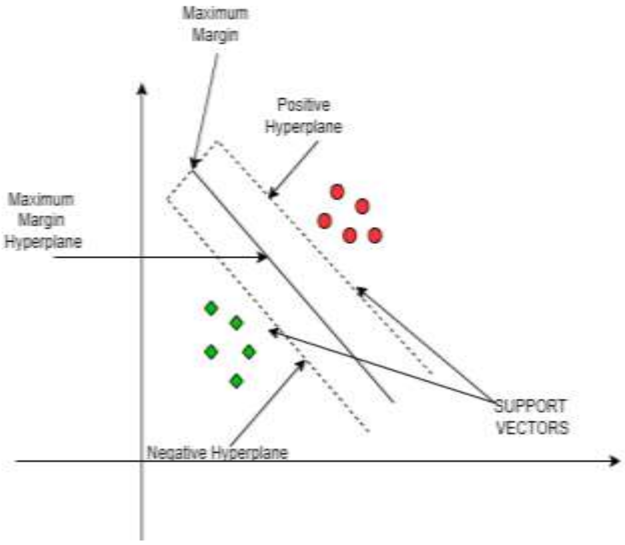


Fig 2. Positive hyperplane and negative hyperplane

There are four steps in support Vector Machine.

1.labeled data

2.Model training prediction

3.New data

4.output

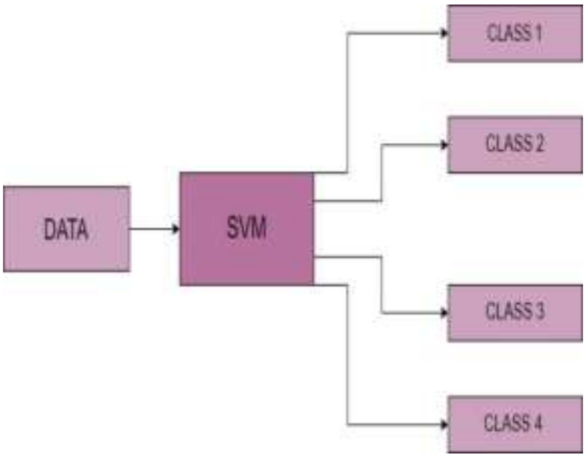


Fig 3.Data flow in Support Vector Machine (SVM)

The step-by-step procedure which is used in natural language processing to find out the suspicious profile.

3.2 NLP TASKS:

Human language is filled with ambiguity, making it incredibly difficult to write software that accurately data mindset meaning of text or voice data. Homophones, sarcasm, idioms, metaphors, grammar, and uses exceptional variations in sentence structure that take human ears to learn. NLP drives applications to recognize and understand the accuracy from the start of the application, if those applications are going to be useful the task is to break down human text data in ways that help the computer make sense out of it.

Statistical machine learning and deep learning applications were used but couldn't easily accommodate Seamless accurate results. So Natural language processing uses models automatically to extract the data and classify the label elements of text data.

3.3 Social media network sentiment analysis:

Natural language processing has become essential for uncovering hidden data and insights from social media network sites. sentiment analysis can analyse language using social media post responses, reviews, and more to extract the attitudes and emotions in response to the events, information which is very useful for finding out the fake and real accounts in social networking.

Here, text recognition is done, and summarisation of applications of fraud and real accounts using semantic reasoning of natural language processing (NLP).

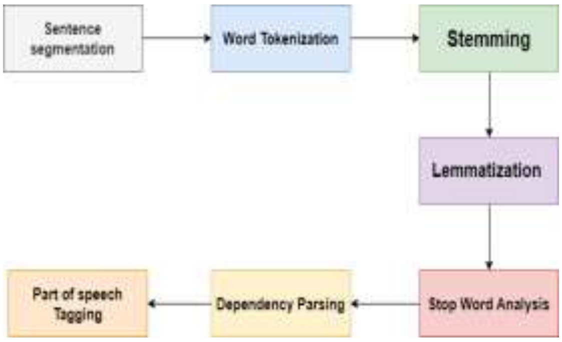


Fig 4. Natural language processing pipeline

Some possible characteristics that could be used as input features for suspicious account detection in an online social network model include:

1. The number of followers the account has

2. The ratio of followers to following

3. The age of the account

4. The amount of activity on the account

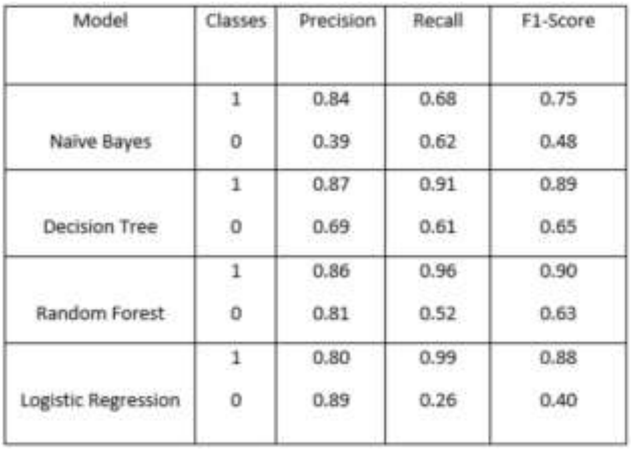
(number of posts, comments, likes)

5. The type of content that is posted

6. The use of hashtags

7. The presence of a profile picture and biography

8. The use of third-party apps to boost the account's activity



Model	Classes	Precision	Recall	F1-Score
Naive Bayes	1	0.84	0.68	0.75
	0	0.39	0.62	0.48
Decision Tree	1	0.87	0.91	0.89
	0	0.69	0.61	0.65
Random Forest	1	0.86	0.96	0.90
	0	0.81	0.52	0.63
Logistic Regression	1	0.80	0.99	0.88
	0	0.89	0.26	0.40

Table.1 Comparison of accuracy for different Algorithm

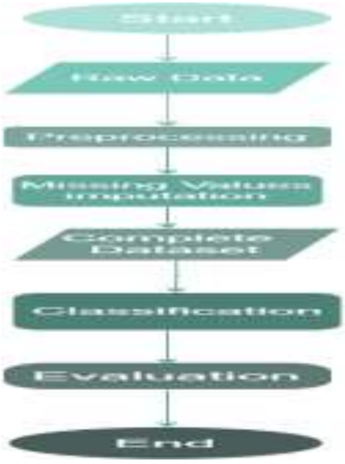
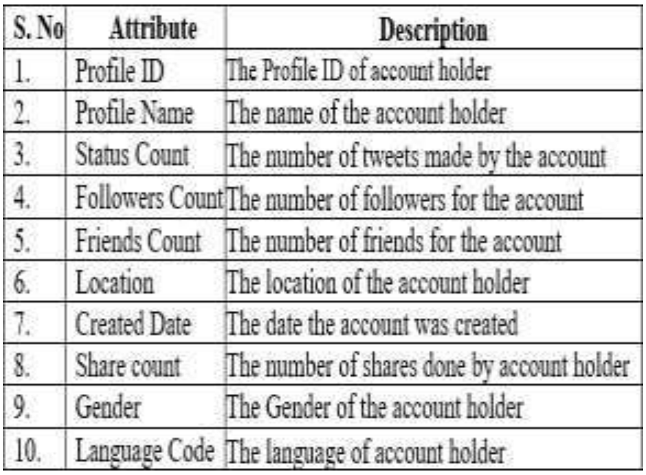


Fig - 5: Process of extracting data

IV. IMPLEMENTATION

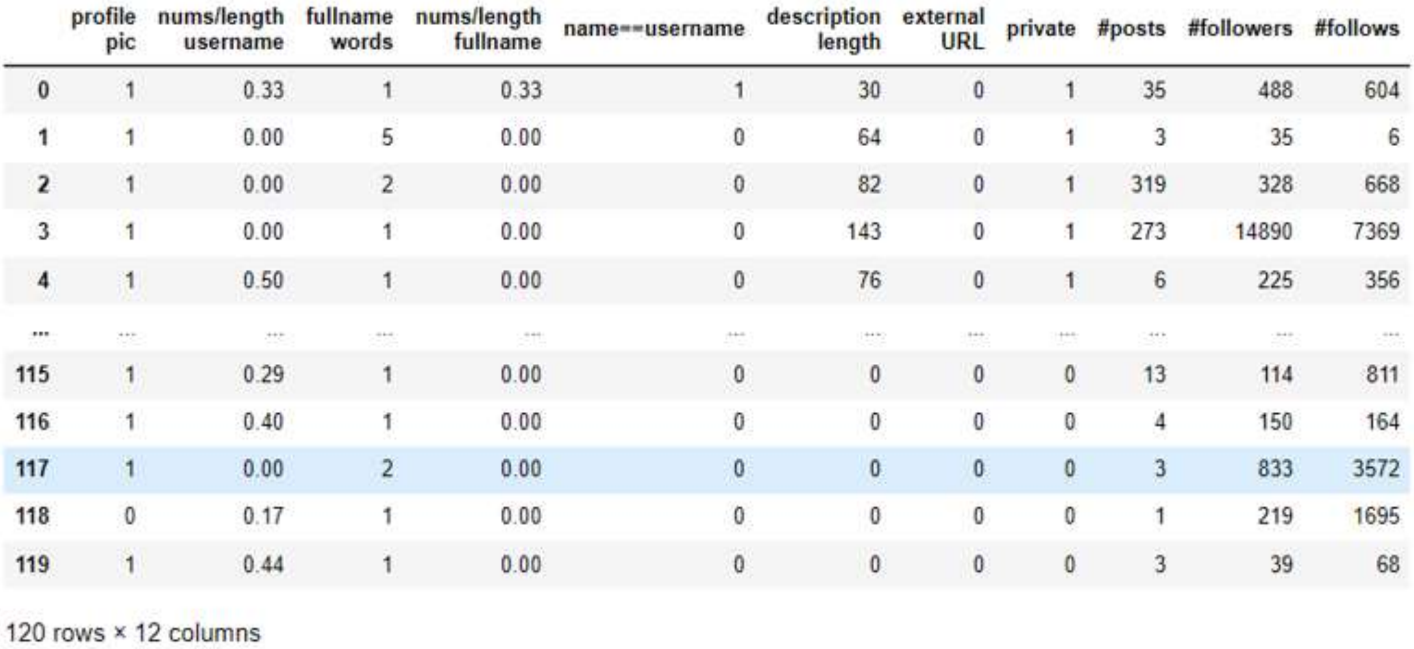
The dataset of fake and genuine accounts, Various attributes that include in the dataset are the number of friends, followers, status count location, and tagged post, created resulting in this data set to the training and testing data Then the classification of the algorithms are done to determine the efficiency of the algorithm from the data set used. More than 80% of accounts are used to train the data and 20% of accounts to test the data.



S. No	Attribute	Description
1.	Profile ID	The Profile ID of account holder
2.	Profile Name	The name of the account holder
3.	Status Count	The number of tweets made by the account
4.	Followers Count	The number of followers for the account
5.	Friends Count	The number of friends for the account
6.	Location	The location of the account holder
7.	Created Date	The date the account was created
8.	Share count	The number of shares done by account holder
9.	Gender	The Gender of the account holder
10.	Language Code	The language of account holder

Table 2.Attributes considered for the suspicious account identification

4.1. Dataset



	profile pic	nums/length username	fullname words	nums/length fullname	name==username	description length	external URL	private	#posts	#followers	#follows
0	1	0.33	1	0.33	1	30	0	1	35	488	604
1	1	0.00	5	0.00	0	64	0	1	3	35	6
2	1	0.00	2	0.00	0	82	0	1	319	328	668
3	1	0.00	1	0.00	0	143	0	1	273	14890	7369
4	1	0.50	1	0.00	0	76	0	1	6	225	356
...	...	...	...	...	...	...	...	...	...	...	...
115	1	0.29	1	0.00	0	0	0	0	13	114	811
116	1	0.40	1	0.00	0	0	0	0	4	150	164
117	1	0.00	2	0.00	0	0	0	0	3	833	3572
118	0	0.17	1	0.00	0	0	0	0	1	219	1695
119	1	0.44	1	0.00	0	0	0	0	3	39	68

120 rows × 12 columns

Table 2. CSV file of dataset

4.2 Evaluation Parameters

Efficiency/Accuracy = Number of predictions/Total

Number of Predictions Percent Error = (1-Accuracy)*100

Confusion Matrix - Confusion Matrix is a technique for

Figure 5. Sample of CSV file

4.3 Training of the Dataset

summarizing the performance of a classification algorithm.

Calculating a confusion matrix can give you a better idea of

what your classification model is getting right and what

types of errors it is making.

TPR- True Positive Rate TPR=TP/(TP+FN)

FPR- False Positive Rate FPR=FP/(FP+TN)

TNR- True Negative Rate TNR=TN/(FP+TN)

FNR- False Negative Rate FNR=1-TPR

Recall- How many of the true positives were recalled (found), i.e. how many of the correct hits were also found.

Recall = TP / (TP+FN)

Precision- Precision is how many of the returned hits were

true positive i.e. how many of the found were correct hits.

Precision = TP / (TP + FP)

F1 score- F1 score is a measure of a considers both the precision p and the recall r of the test to compute the score.

ROC Curve- The Receiver Operating Characteristic is the plot

of TPR versus FPR. ROC can be used to

compare the performances of different classifiers. training the dataset with different hybrid approach classification algorithms. The results show an increase in the accuracy results of the different classification algorithms.

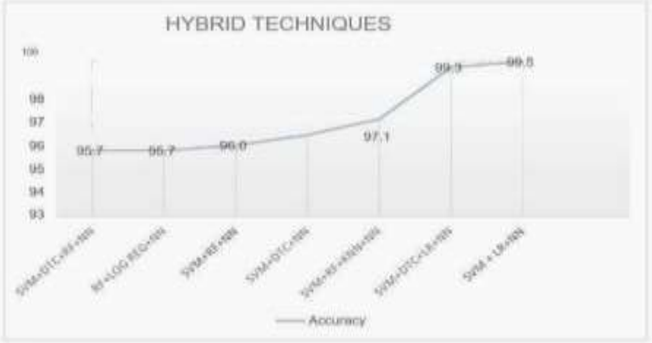


Figure 6. Accuracy of models in ascending order

Shows the accuracy of each of

our experimental model in ascending order

and the model with highest accuracy being our trained system.

A confusion matrix is a matrix that summarizes the performance of a machine learning model on a set of test data. It is often used to measure the performance of classification models, which aim to predict a categorical label for each input instance. The matrix displays the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) produced by the model on the test data.

For binary classification, the matrix will be of a 2X2 table, For multi-class classification, the matrix shape will be equal to the number of classes i.e for n classes it will be nXn.

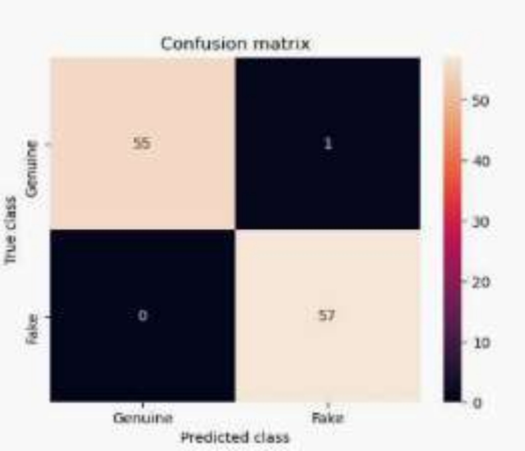


Figure 8: Confusion matrix of proposed hybrid

model

The fig 8, shows the confusion matrices for our proposed hybrid model which gives us the summary of true positive, true negative, false positive and false negative without normalization.

V. CONCLUSION

While designing a system, the majority of implementation of fake accounts detection is either graph-based or feature-based, and they may be used as graph analysis techniques or machine learning techniques to identify the data. Here, the conclusion is that we are going to use the Support Vector Machine and Natural language processing (NLP) to find the accuracy rate. By testing and training the dataset with different hybrid approach classification algorithms. The results show an increase in the accuracy results of the different classification algorithms.

While designing a system, the majority of implementation of fake accounts detection is either graph-based or feature-based, and they may be used as graph analysis techniques or machine learning techniques to identify the data. Here, the conclusion is that we are going to use the Support Vector Machine and Natural language processing (NLP) to find the accuracy rate.

VI. REFERENCE

[1]. L. P, S. V, V. Sasikala, J. Arunarasi, A. R. Rajini and N. Nithiya, "Fake Profile Identification in Social Network using Machine Learning and NLP," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2022, pp. 1-4, doi: 10.1109/IC3IOT53935.2022.9767958. Learning and NLP) pp. 4133-4136

[2]. Dhawan, Sanjeev. (2016). Implications of Various Fake Profile Detection Techniques in Social Networks. IOSR Journal of Computer Engineering. 02. 49-55. 10.9790/0661-15010020249-55.V . Ramakrishna and K Kanaka Durga.

[3]. Gupta, Aditi & Kaushal, Rishabh. (2017). Towards detecting fake user accounts in facebook. 1-6. 10.1109/ISEASP.2017.7976996.

[4]. C. Perez, M. Lemercier and B. Birregah, "A dynamic approach to detecting suspicious profiles on social platforms," 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, 2013, pp. 174-178, doi: 10.1109/ICCW.2013.6649223.

[5]. Joshi, S., Nagariya, H.G., Dhanotiya, N., Jain, S. (2020). Identifying Fake Profile in Online Social Network: An Overview and Survey. In: Bhattacharjee, A., Borgohain, S., Soni, B., Verma, G., Gao, XZ. (eds) Machine Learning, Image Processing, Network Security and Data Sciences. MIND 2020. Communications in Computer and Information Science, vol 1240. Springer, Singapore. https://doi.org/10.1007/978-981-15-6315-7_2

[6]. Chakraborty, P. , Shazan, M. , Nahid, M. , Ahmed, M. and Talukder, P. (2022) Fake Profile Detection Using Machine Learning Techniques. Journal of Computer and Communications, 10, 74-87. doi: 10.4236/jcc.2022.1010006.

[7]. David Savage, Xiuzhen Zhang, Xinghuo Yu, Pauline Chou, Qingmai Wang,Anomaly detection in online social networks,Social Networks,https://doi.org/10.1016/j.socnet.2014.05.0.

[8]. C. Perez, M. Lemercier and B. Birregah, "A dynamic approach to detecting suspicious profiles on social platforms," 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, 2013, pp. 174-178, doi: 10.1109/ICCW.2013.6649223.

[9]. M. Fire, R. Goldschmidt and Y. Elovici, "Online Social Networks: Threats and Solutions," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019-2036, Fourthquarter 2014, doi: 10.1109/COMST.2014.2321628.

[10]. arXiv:1303.3751 [cs.SI]
(or arXiv:1303.3751v1 [cs.SI] for this version)https://doi.org/10.48550/arXiv.1303.3751.