ISSN 2224-087X. Електроніка та інформаційні технології. 2023. Випуск 22. С. 46–56
Electronics and information technologies. 2023. Issue 22. P. 46–56

UDC 004.89 DOI: https://doi.org/10.30970/eli.22.5

DETECTION OF UNNATURAL USER BEHAVIOR IN SOCIAL MEDIA USING MACHINE LEARNING TECHNOLOGIES

Iryna Mysiuk, Roman Shuvar

Ivan Franko National University of Lviv
50 Drahomanova St., UA-79005 Lviv, Ukraine
iruna.musyk8a@gmail.com

Information from social media influence public sentiment, the spread of opinions and reactions to events. The spread of often false information and the incitement of people in sensitive topics are often influenced by artificially created users for certain events. In other words, such users are called bots, which should be quickly detected and blocked in order to stop the promotion of certain profitable questions to customers. The detection process can be automated with the help of trained models based on the collected data and clustering of users according to the features inherent in bots. Among the mentioned differences are information about the number of subscribers and followers, activity of publishing posts, photo, date of profile creation and others. For training and testing models, a method of automated data collection using the Selenium framework from user pages is described. Correlation of various attributes is shown, and classification results are shown for identifying users with unnatural behavior in social media.

Keywords: bot, machine learning, social media, data classification, collecting data.

Overview

Social media are actively developing and taking more and more of our free time. Users receive and exchange information instantly from the moment of its publication, which leads to such popularity of such communication systems. As a result, there is a lot of manipulation, false information and the picking up and rapid spread of a certain topic or news in the social media. The dissemination of such information often turns out to be fake or not completely true. Users with unnatural behavior (bots) increase the spread of panic and activity in the social media. A large number of such fake users are created to spread and comment on the information the customer needs. Such bot groups are often activated precisely when the necessary information is included in a post on a social media and spread across the Internet. The topic of analysis of user-bots, which have certain anomalous indicators of being subscribed to someone among all users of social networks, is considered in works [1, 2]

Popular social media Youtube, Twitter, Facebook, Instagram have different specifics and features. However, the formation of communications between users, in the same way, is the connection of a subscriber or a friend and a following someone on your account. In the accounts of real users and bots, there are certain differences in their activity and the difference in filling out information [3, 4].

The purpose of this work is to identify the main features of bots in social media from collected user data for profile classification using machine learning methods.

© Mysiuk I., Shuvar R. 2023

The main tasks in this work are the collection of data about potential bots and regular users from social media (Twitter, Facebook, Instagram), filtering and forming datasets for training and learning using various classification methods in machine learning.

Data collection and formation of data sets

Data about users can be collected using various application programming interfaces (APIs) or directly from the user interface (UI). Unlike working with data from the API, the process of working with UI requires time delays for reading the values of elements. However, the process simulates the user experience on web pages.

The data collection process is lengthy considering the chosen method of collection from the UI. The amount of data for further training using machine learning methods can reach thousands of records from one social media. Most of the main attributes are similar and transform to the dataset template. The process of reading data took place from several accounts and in several stages, considering the impossibility of long-term work. Extracting information about the number of posts on a page in the feed is a difficult task, given the prohibition of page scrolling from a non-logged-in user.

Data is collected by searching for keywords and names (for example: Ivan, Peter, Simon) and more specific for bots (joke, bot, others). By logging into each account, the necessary data was collected to form data sets. The process of data collection and accumulation is iterative. Some fields are missing, the "null" value was recorded in the data set.

At the collection stage, it is difficult to detect bots visually, given the large number of user profiles. However, at the stage of forming datasets for training such users, it is revealed by the presence of photos, the date of profile creation, the number of subscribers and followers, the number of profile mentions, filling in general information, the number of publications and subscriptions to users with status.

The data collection process takes place with the help of a program for reading data from the Document Object Model (DOM) web page of social media and saves it to a file for further processing. The program is written in the Java programming language with the connection of the Selenium library for automating the testing of web pages in browsers [1, 2].

Fig. 1. Graphical visualization of the steps of data collection and formation of data sets

As shown in Fig. 1, the collection of data from social media Twitter, Instagram and Facebook takes place using a program with the integration of the Selenium framework. The received data has a slightly different structure and redundant characters due to different web pages, to clean the data, the data is standardized into the same format for further training. The data processing process takes place already with the formed training and test data set at the next stage before working with the analysis.

For the collected data from several social networks, it is possible to summarize and analyze the data for the presence of bots according to certain attributes [3]. In addition, it is worth taking into account a larger number of parameters for training and classification.

At the stage of formation of data sets, all data are written into a comma separated values (CSV) file, which is parsed through commas and can be separated into arrays of data for use for training with machine learning methods.

The file contains columns with the following data:

- serial number of the record in the file
- username, if present
- description of general information (profile description, etc.)
- number of subscribers (per user account)
- number of following someone (on the account of other users)
- the number of posts on the user's page
- the date of the first post in the feed on the user's page
- the number of liked, followed, favorite pages
- availability of the user's picture
- the number of mentions of the account
- other technical details (link on the page such as URL, bot or non-bot labeling for model training).

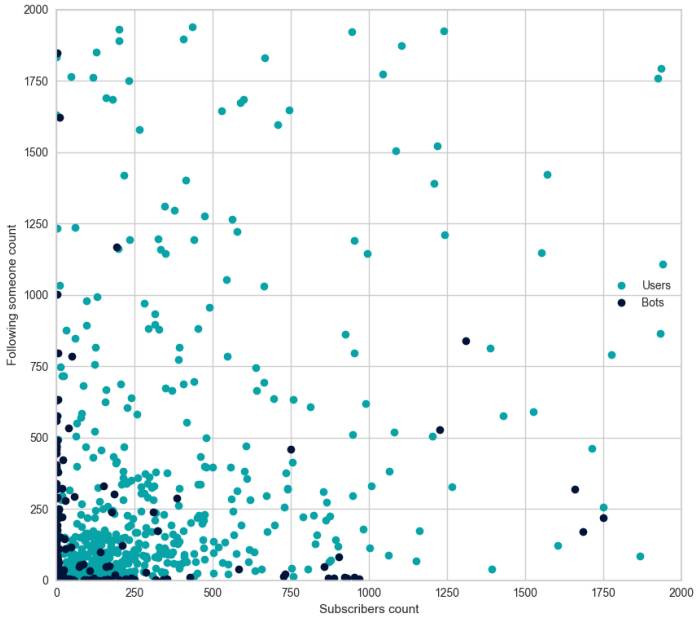


Fig. 2. Visualization of changes in the number of subscribers and following from users and bots

Collecting about 1600 entries in a file of about 550 from three social media. A training set of 1000 records with potential marked bots and a test set of about 600 records with various users were formed. A larger data array of 6000 records from various social networks has also been formed.

In addition to analyzing values and sorting through data with certain conditions-restrictions, you can use visualization in the form of graphs to better represent the differences between users and bots. The dependence of the number of following users on the number of subscribers for users and potential bots as it is shown in Fig. 2.

Bots have a small number of subscribers relative to following, because they do not have connections with other users. This is the trend of bots in the proportion of 1 to 2 and more percentages of following.

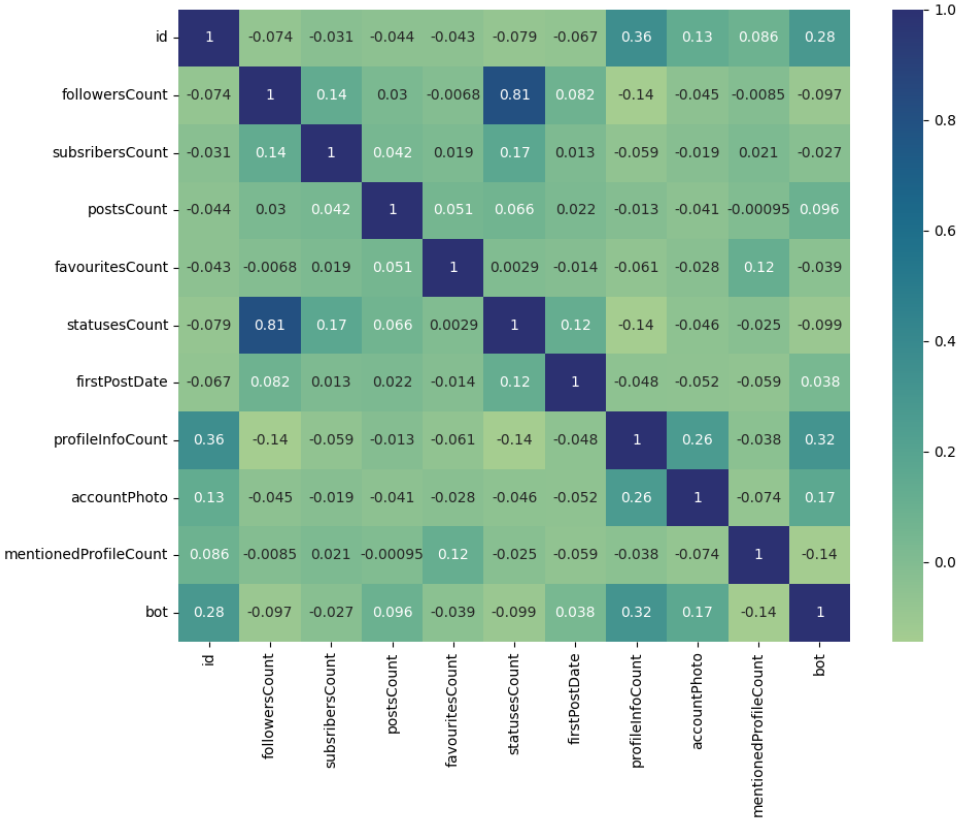


Fig. 3. Correlation matrix from data sets

Fig. 3 shows a heatmap with correlation values of values of linear dependence of attributes among themselves. Coefficients presented in the range from -1 to 1 indicate the linearity and dependence of the increase or decrease of values, respectively, among themselves [3]. This data represents the dependency for the entire data set with bots and is the result common to all collected data.

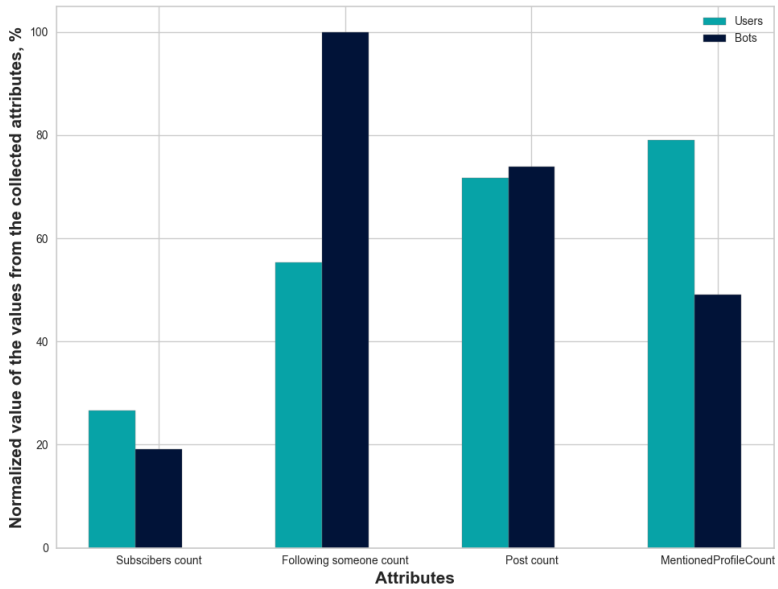


Fig. 4. Normalized values of the number of subscribers, posts, mentions, the number of following of a user or a bot for a general comparison of attributes

For a general presentation, the quantitative ratio of values among themselves is shown in Fig. 4. To present the graph, the average value of the quantity was taken and divided by the maximum value. In order to present as a percentage, the ratio is divided by the maximum value and multiplied by 100. According to the collected data, bots have a small number of followers, and many follow someone. This trend may be due to the fact that bots are designed to comment and share information. At the same time, the number of mentions of the user profile is more among ordinary users, but the number of posts in the feed is more among bots.

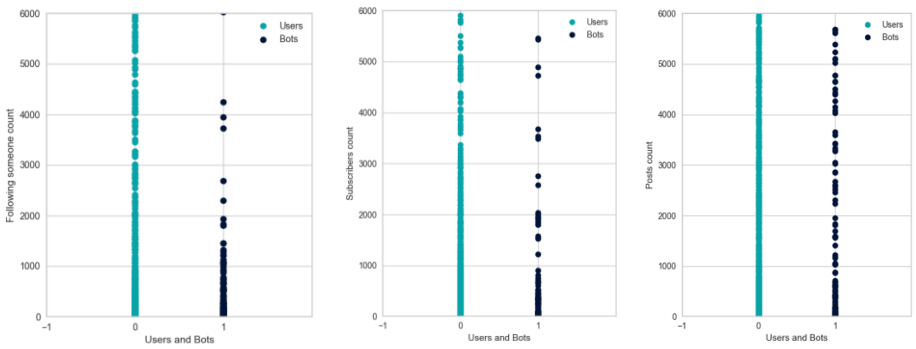


Fig. 5. Following someone, subscribers, posts count change visualization for users and bots

In Fig. 5 shows the number of following someone, subscribers and posts for users and bots from the training dataset. The number of following someone for bots is quite large considering the density of points for a value of 1, which shows the value for bots. The number of subscribers for users and bots from the training dataset. Obviously that all organic users have a more followers than bots. Currently, the amount of information from bots is less than from regular users. The number of posts for users indicates its authenticity compared to a bot.

Comparison of user and bot classification methods based on communication data

For the training process, only data on the number of subscribers, following someone, posts and the date of the first post, the number of mentioned profiles, the presence of a description of general information and the presence of a profile photo are used. We reserve all other information for statistical analysis and other research. Among the classifiers used are Random Forest, Decision Tree, Gaussian Naive Bayes, K-Nearest Neighbors, Support Vector Classification [5]. The accuracy of the classification result was calculated for each classifier separately for comparison. The obtained training results can be determined by the selection of setting parameters. The Decision Tree and Random Forest Classifiers from the mentioned classifiers showed the best classification accuracy based on the training data set as it is shown in Fig. 6.

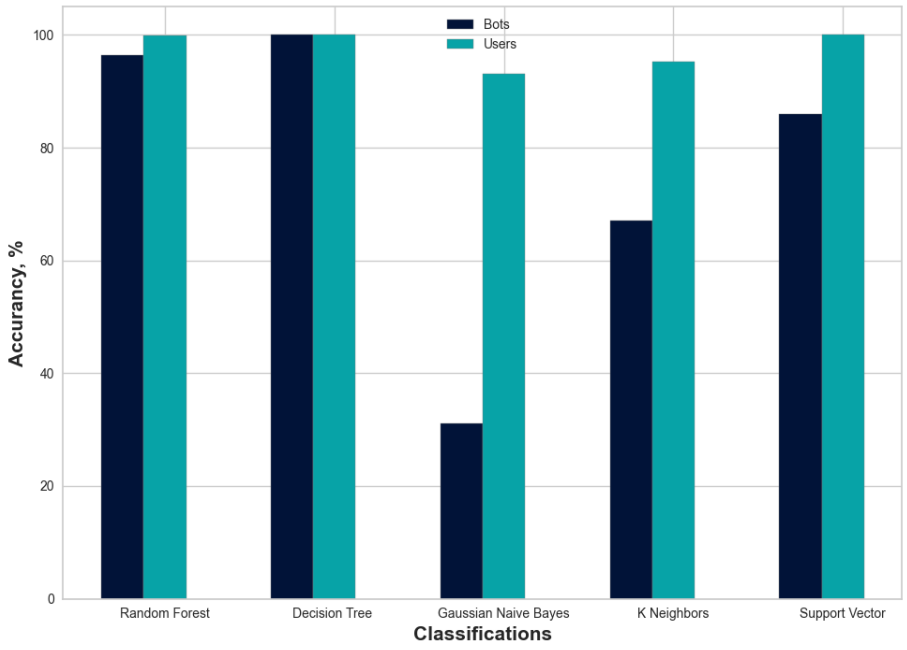
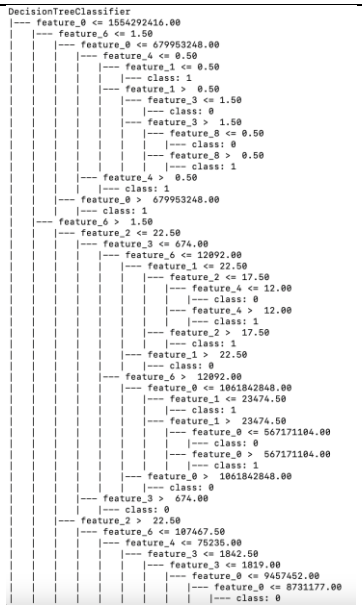


Fig. 6. Comparison of the accuracy of classification methods based on training data for bots and users

Methods from the sklearn library were used to train the model using machine learning methods. As shown in Fig. 7, it is feasible to export the formed decision tree for the data set. After training, to clearly infer the training result, a portion of the actual and expected user classification results into bots is presented for visual comparison [6].



Users

	Actual	Predicted
276	0	0
277	0	0
278	0	0
279	0	0
280	0	0
...	...	...
6682	0	0
6683	0	0
6684	0	0
6685	0	0
6686	0	0

[5859 rows x 2 columns]

Bots

	Actual	Predicted
0	1	1
1	1	1
2	1	1
3	1	1
4	1	1
...	...	...
3773	1	1
3774	1	1
3775	1	1
3776	1	1
3777	1	1

Fig. 7. A decision tree in the form of branching and the training result in the format of the actual and expected value

To visualize the learning process, a graph of the learning curve for the Decision tree and Random forest classifiers is presented. In contrast to the results shown in Fig. 6, the learning process was performed on the trained combined values from all records. For the reduced data set, the results of training the value of the accuracy of the score in the Random forest classifier.

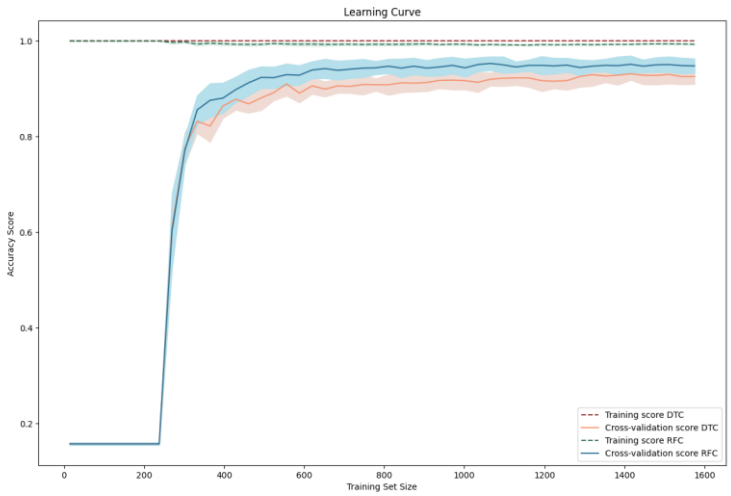


Fig. 8. Learning curve for Decision Tree Classifier (DTC) and Random Forest Classifier (RFC) for short training data set (approximately 1600 records)

For a data set of larger results, the learning curve reaches the mark of 1 accurancy rate. More accurate results are obtained faster for the Random forest classifier than for the Decision tree, as shown in Fig. 9. The highlighted area near the curve shows the difference between the mean value and the standard deviation. Considering the absence of sharp changes in the curve, it can be assumed that the trained model is sufficiently resistant to unpredictable data [7].

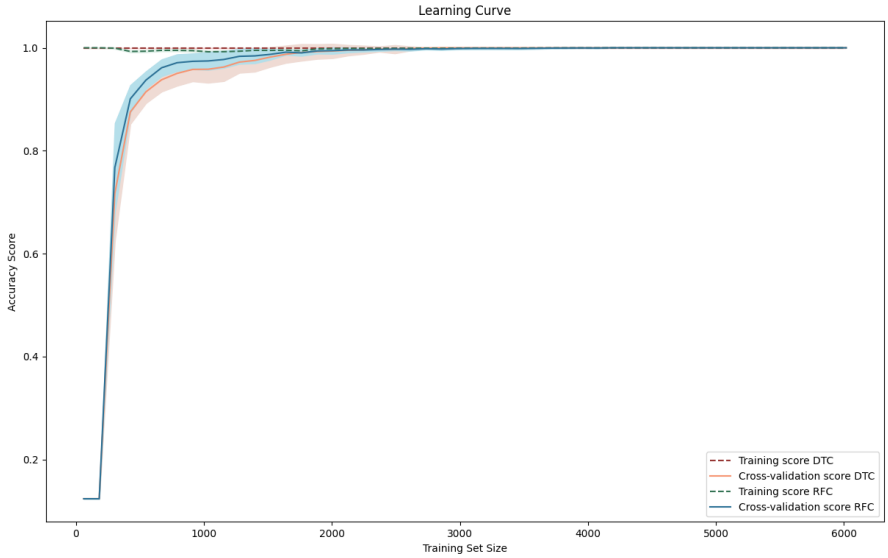


Fig. 9. Learning curve for Decision Tree Classifier (DTC) and Random Forest Classifier (RFC) for extended training data set (approximately 6000 records)

There is used a validation curve to show the influence of the maximum depth hyperparameter on the training and cross validation scores to learn. In Fig. 10 and Fig. 11 show validation curves for Random Forest and Decision tree classifiers, respectively. The model can be validated to avoid of underfitting or overfitting process using such curve. The maximum depth value means the best validation accuracy at that value. In the course of training, fitting takes place on the basis of existing and expected values, and a confusion matrix is formed. This matrix is used to evaluate the classification accuracy.

According to the obtained results, bots are less experienced and contain fewer connections than ordinary users. Although, as you know, bots flood social networks intensively already today. The behavior of bots is artificial and is not based on the quality of content, but on their quantity and mass. The main task of bots is to supplant real news, pages to replace real ones to create the information they need. Given the definition of some parameters, it can be argued that these bots have unnatural behavior and are significantly different from other network users.

When setting up bots, research is carried out on its areas of operation and the functions it will perform. When validating the curve, there will be a check of the learning success process. The validation curves will show the increase or decrease in speed and their difference in deviation when the values change. Usually, such dependencies grow, which indicates the possibility of conducting their training. Under the condition of sharp changes in values or reaching smaller or unchanged values, this means that the peak of their use has been reached.

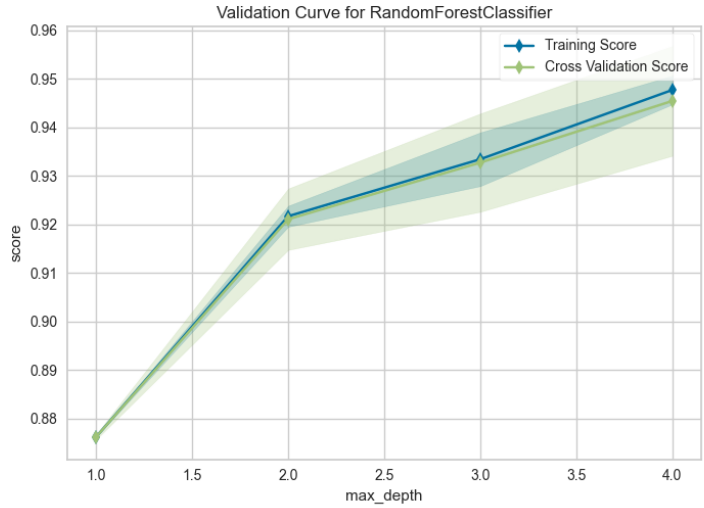


Fig. 10. Validation curve for Random Forest Classifier

Fig. 10 and Fig. 11 show the growth of score with increasing maximum depth for Random Forest and Decision tree classifiers. The dynamics of the value change is almost the same, at the maximum depth value of 3, the validation curve for the Decision tree has a higher score.

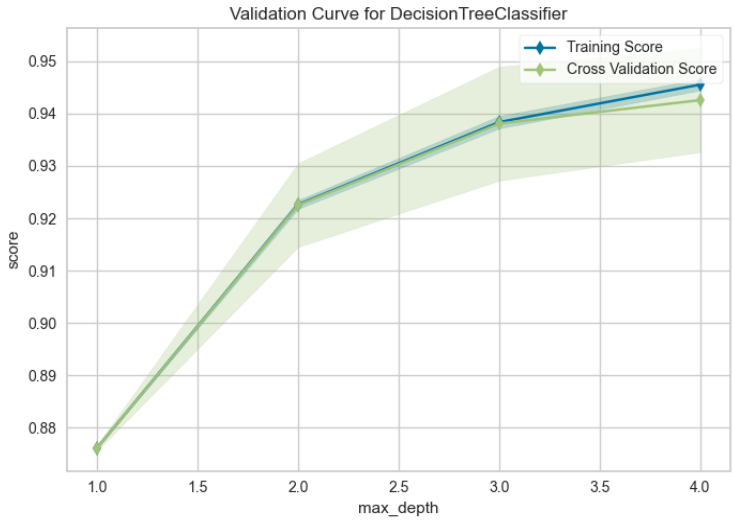


Fig. 11. Validation curve for Decision Tree Classifier

In general, such an analysis of learning results, in addition to understanding the obtained results, makes it possible to assess the quality of the process and choose the best parameters.

Conclusion

Social media are created for communication and exchange of ideas and information on the Internet. Active users publish a lot of information, have many connections. Unnatural behavior in social networks is characterized by excessive activity of unrelated events or actions with certain unique ratios of the amount of information on the page with the dates of their creation, etc. Bots are created for some events to spread false information for the benefit of the customer. As a result, you can highlight several criteria, such as the number of followers, those you follow, the date of publication of the first post, the number of mentions and other set of attributes.

The data is compiled into datasets using a written program. Dependencies between a bot and a regular user based on a set of defined attributes are described.

Having formed a data set for training and testing models, a comparison of data classification methods by means of machine learning was performed. The results of the application of the trained model were tested on the test data set and verified using learning and validation curves.

Analyzing the obtained results, the quality of the received information, the selection and classification of bots among ordinary users by machine learning algorithms, and the size and presence of bots in social networks were investigated.

References

[1] *Mysiuk I., Mysiuk R., Shuvar R.* Collecting and analyzing news from newspaper posts in Facebook using machine learning / Stuc. intelekt. // 2023; 28(1):147-154 DOI: https://doi.org/10.15407/jai2023.01.147

[2] *I. Mysiuk, R. Mysiuk, R. Shuvar, V. Yuzevych*. Methods of analytics of big data of popular electronic newspapers on Facebook // Electronics and information technologies 2022 – Vol. 19. – P. 66–74, DOI: http://dx.doi.org/10.30970/eli.19.6

[3] *Agarwal, Isha & Rana, Dipti & Bhatia, Devanshi & Rathod, Jay & Gandhi, Kaneesha & Sodagar, Harshit. (2021*). Detection of Bot Accounts on Social Media Considering Its Imbalanced Nature. Data Preprocessing, Active Learning, and Cost Perceptive Approaches for Resolving Data Imbalance. DOI: https://doi.org/10.4018/978-1-7998-7371-6.ch009

[4] *Mariam Orabi, Djedjiga Mouheb, Zaher Al Aghbari, Ibrahim Kamel*. Detection of Bots in Social Media: A Systematic Review, Information Processing & Management, Vol. 57, Issue 4, 2020, 102250, ISSN 0306-4573, DOI: https://doi.org/10.1016/j.ipm.2020.102250.

[5] *Aljabri, M., Zagrouba, R., Shaahid, A. et al.* Machine learning-based social media bot detection: a comprehensive literature review. Soc. Netw. Anal. Min. 13, 20 (2023). DOI: https://doi.org/10.1007/s13278-022-01020-5.

[6] [scikit-learn Machine Learning in Python – Retrieved from: https://scikit-learn.org/stable/

[7] Machine Learning Visualization with Yellowbrick – Retrieved from: https://medium.com/akava/machine-learning-visualization-with-yellowbrick-42e3142c41b9

ISSN 2224-087X. Electronics and information technologies. 2023. Issue 22

ВИЯВЛЕННЯ НЕПРИРОДНЬОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ У СОЦІАЛЬНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ

Ірина Мисюк, Роман Шувар

Львівський національний університет імені Івана Франка,
вул. Драгоманова, 50, м. Львів, 79005, Україна
iruna.musyk8a@gmail.com

Інформація з соціальних мереж впливають на суспільні настрої, поширення думок та реакцій на події. На поширення часто підставної інформації та підбурювання людей в чутливій тематиці часто впливають штучно створенні користувачі для певних подій. Іншими словами такі користувачі називаються боти, яких варто швидко виявляти та блокувати для зупинки просування певних вигідних питань замовникам. Процес виявлення може бути автоматизований за допомогою натренованих моделей на основі зібраних даних та кластеризації користувачів за ознаками притаманним ботам. Серед згаданих відмінностей є інформація про кількість підписників та друзів, активність публікації постів, наявність фото, дата створення акаунта та інше.

Більшість часу для аналітичних етапів витрачається для формування наборів даних. У роботі використано метод збору з вмісту веб елементів веб сторінок у браузері. Враховуючи використання комплексного підходу зі збору даних про користувачів з кількох соціальних мереж Instagram, Facebook та Twitter, великий об'єм даних різного формату та структури стандартизовано під однаковий шаблон. Для тренування та тестування моделей описаний спосіб автоматизованого збору даних з допомогою фреймворку Selenium зі сторінок користувачів в набори даних. Показано кореляцію різних атрибутів та показано результати класифікації для визначення користувачів з неприродньою поведінкою у соціальних мережах.

Для класифікації користувачів за ознакою боту з відмінними від користувачів рисами використано для порівняння кілька методів машинного навчання Random Forest, Decision Tree, Gaussian Naive Bayes, K-Nearest Neighbors, Support Vector Classification. Серед яких найкращим по точності виявився Decision Tree. На основі тестового набору даних виконано класифікацію даних про користувачів на основі навченої моделі. Отже, у роботі показано можливості реалізації операцій збору, опрацювання, проміжного аналізу та класифікації користувачів на наявність ботів у соціальних мережах.

Ключові слова: бот, машинне навчання, соціальна мережа, класифікація даних, збір даних.

Стаття надійшла до редакції 19.06.2023
Прийнята до друку 26.06.2023