iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: 59085

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Detecting Malicious Twitter Bots using Machine Learning

B. Sneha[1], M. Venusri[2], M. Jithin[3], Dr. S. Kirubakaran[4]
UG Student, Department of Computer Science & Engineering, CMR College of Engineering & Technology, Hyderabad, India

Abstract: ***Twitter play a significant role in our daily lives, offering a wide range of opportunities to their users. However, Twitter and online social networks (OSNs) in general are increasingly being utilized by automated accounts, commonly known as bots, as they continue to gain immense popularity across various user demographics. Malicious twitter Bots detection is required to detect real users from fraudulent users because it leads to spreading of spam messages and engage in fraudulent activities. To overcome this, we are going to differentiate bots from legitimate users using feature extraction techniques and find malicious bots and tweets using machine learning algorithm and deep learning architecture known as VGG19 which is combined with the convolutional neural network (CNN) in order to identify whether the tweets are posted by bots or real users and also identifying malicious twitter bots along with malicious URLs. By following these techniques, we can identify the account as bots or real user and prevent spreading of malicious content in the society. The deep learning architecture combined with convolutional neural network to evaluate over a series of experiments using two large real Twitter datasets and compare the experimental results with other machine learning algorithms and provide advantages over other existing techniques like logistic regression targeting the identification of malicious users in social media.***

Keywords: Deep Learning, Machine learning, Twitter bot detection.

I. INTRODUCTION

Twitter is one of the fastest-growing social media stages. It empowers clients to trade news, express themselves, and wrangle about current occasions. Clients may take after people who share their interface or have comparable perspectives. Clients may send tweets to their adherents right absent. Re-tweeting permits the substance to reach a more extensive group of onlookers. Amid live occasions such as sports or grant ceremonies, the number of tweets spikes. Smartphones and PCs can both get to Twitter. Paid advancements may result in critical salary creation as well as an increment in item deals. Understudies may utilize Twitter to memorize more almost the subjects that are secured in class. The message that's shared with devotees is alluded to as a tweet. The tweet ought to be brief and to the point, with a most extreme of 140 characters. The hashtag (#) is utilized to find and take after a certain subject. When a hashtag gets well known, it is alluded to as a trending theme. Twitter associations are bidirectional, meaning that a individual may have both adherents and followers.

Van Der Walt, E., & Eloff, J [1] Personality duplicity on enormous information stages (like social media) is an expanding issue, due to the proceeded development and exponential evolvement of these stages. Nasim, M., Nguyen, A., Lothian, N., Cope, R., & Mitchell, L [2] Substance polluters, or bots that capture a discussion for political or promoting purposes are a known issue for occasion forecast, race determining and when recognizing genuine news from fake news in social media information. Khalil, A., Hajjdiab, H., & Al-Qirim, N [3] The positioning of tweets in this look motor depends on numerous components, one of which is the user‟s number of adherents.Twitter's ubiquity has made it an appealing put for spam and spammers of all sorts. Spammers have different objectives: spreading publicizing to produce deals, phishing or essentially fair compromising the system's notoriety. Wetstone, J. H., & Nayyar, S. R [4] Twitter has gotten to be a well known media center where individuals can share news, jokes and conversation approximately their temperaments and talk about news occasions. In Twitter clients can send Tweets immediately to his/her supporters. Moreover, Tweets can be recovered utilizing Twitter'sgenuine time look motor . The positioning of tweets in this look motor depends on numerous components, one of which is the user's number of devotees.

II. LITERATURE SURVEY

Karataş, A., & Şahin, S [5] The rise of web administrations and notoriety of online social systems (OSN) like Facebook, Twitter, LinkedIn etc. have driven to the rise of unwelcome social bots as mechanized social on-screen characters. Those performing artists can play numerous malevolent parts counting infiltrators of human discussions, scammers, impersonators, deception disseminators, stock showcase controllers, astroturfers, and any substance polluter (spammers, malware spreaders) and so on.

It is evident that social bots have major significance on social systems. Subsequently, this paper uncovers the potential risks of noxious social bots, audits the location strategies inside a methodological categorization and proposes roads for future investigate.

Chavoshi, N., Hamooni, H., & Mueen, A [6] In this paper they discussed about a strategy to distinguish strangely related client accounts in Twitter, which are exceptionally improbable to be human worked. This modern approach of bot discovery considers cross-correlating client exercises and requires no labeled information, as contradicted to existing bot discovery strategies that consider clients freely, and require expansive sum of as of late labeled information. Our framework employments a lag-sensitive hashing method and a warping-invariant relationship degree to rapidly organize the client accounts in clusters of strangely connected accounts. Our strategy is 94 % exact and identifies one of a kind bots that other strategies cannot distinguish. Our framework produces day by day reports on bots at a rate of a few hundred bots per day. The reports are accessible online for assist investigation.

Perdana, R. S., Muliawati, T. H., & Alexandro, R [7] The reputation of Twitter has pulled in spammers to spread broad entirety of spam messages. Preliminary considers had showed up that most spam messages were conveyed subsequently by bot. Along these lines bot spammer revelation can lessen the number of spam messages in Twitter basically. In any case, to the foremost amazing of our data, few asks almost have centered in distinguishing Twitter bot spammer. Hence, this paper proposes a novel approach to recognize between bot spammer and bona fide client accounts utilizing time between times entropy and tweet closeness. Timestamp collections are utilized to calculate the time intervals entropy of each client. Uni-gram matching-based likeness will be utilized to calculate tweet resemblance.

Datasets are crawled from Twitter containing both ordinary and spammer accounts. Test comes almost showed up that bona fide client may show standard behavior in posting tweet as bot spammer. A number of genuine blue clients are additionally recognized to post comparative tweets.

In this way it is less ideal to recognize bot spammer utilizing one of those highlights because it were. Be that because it may, combination of both highlights gives predominant classification result. Precision, survey, and f-measure of the proposed technique come to 85,71%, 94,74% and 90% separately. It outflanks precision, audit, and f-measure of procedure which because it were livelihoods either time between times entropy or tweet likeness.

III. METHODOLOGY

A. Algorithms

The algorithms used are logistic regression a machine learning algorithm and VGG19 a deep learning algorithm. These two are used to detect the bots and malicious URLs.

B. Logistic Regression

It is a machine learning algorithm. It belongs to supervised machine algorithm group. It is mainly used for classification. Here the goal is to predict whether the given input/instance belongs to the class or not. It can handle large datasets. It is a statistical algorithm which analyzes the relationship between two data factors. To predict the binary classification i.e; 0 and 1 it uses sigmoid function.

C. VGG19

It is a deep learning algorithm. It is 19 layers deep Convolutional Neural Network algorithm. It is an extension of VGG16. VGG19 (Visual Geometric Group) is used for classifying images. To use it, we have to import Keras function and TensorFlow function. Because, it can easily assign weights with other frameworks.

D. Implementation of Block Diagram

Firstly, we have created modules for each phase. The modules include uploading the dataset and extracting them. And also it includes bot detection, URLs detection, and both URL and bot detection modules, and comparison module. Each module is tested separately because to find and rectify errors without affecting the other modules. The modules are executed sequentially, and each module is dependent on previous module because if previous modules are not executed correctly then we cannot perform further operations.

The modules are executed one by one and the results are compared for each module and plot it in a graph. As a result of comparison module, it shows that the proposed method performs better and shown best results than the existing solution.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

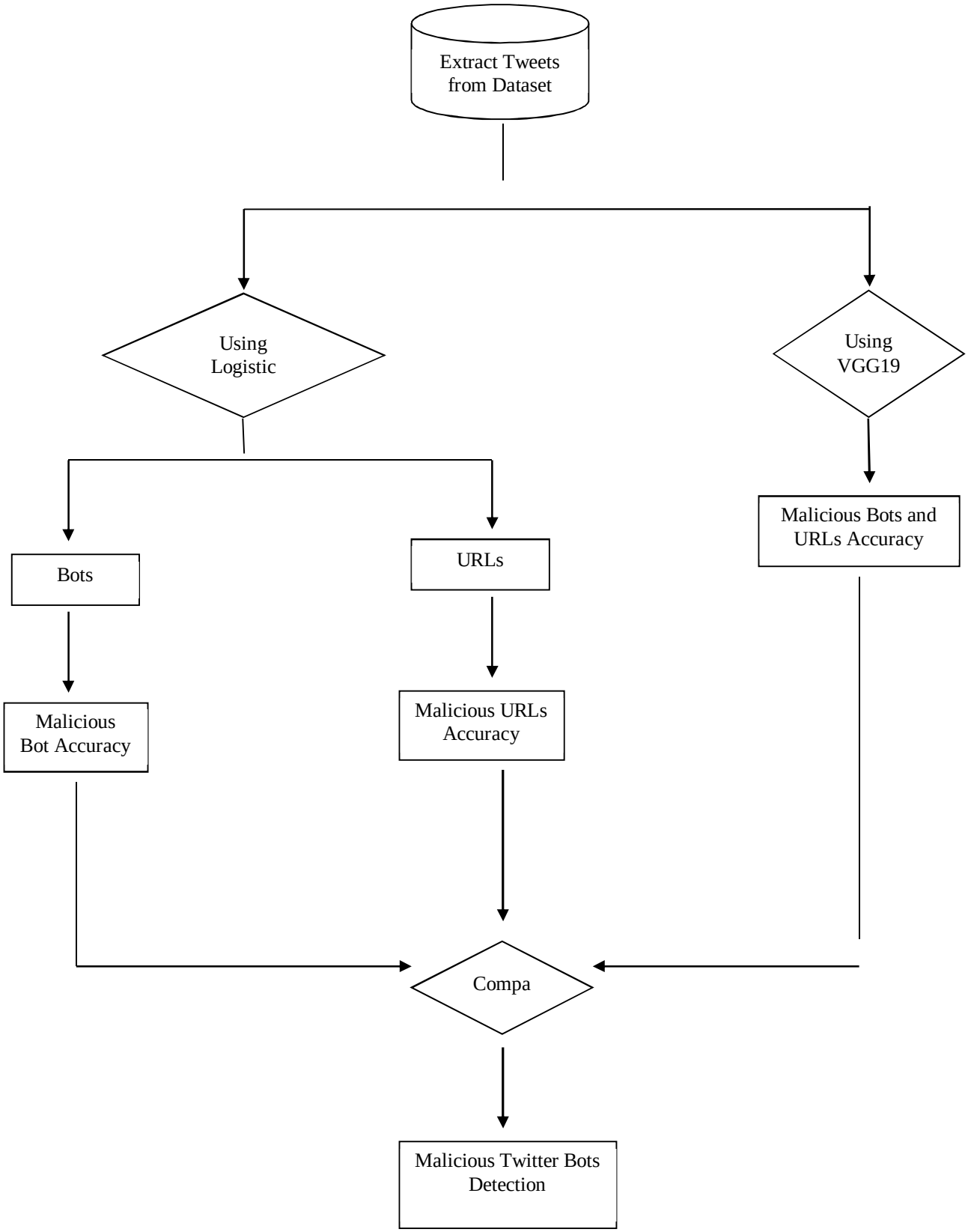


Fig 1: Model Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

IV. RESULTS AND DISCUSSION

A. Figures

To run the modules for execution and get output screen a bat file is created. When we click on it the execution starts and we get the below screen

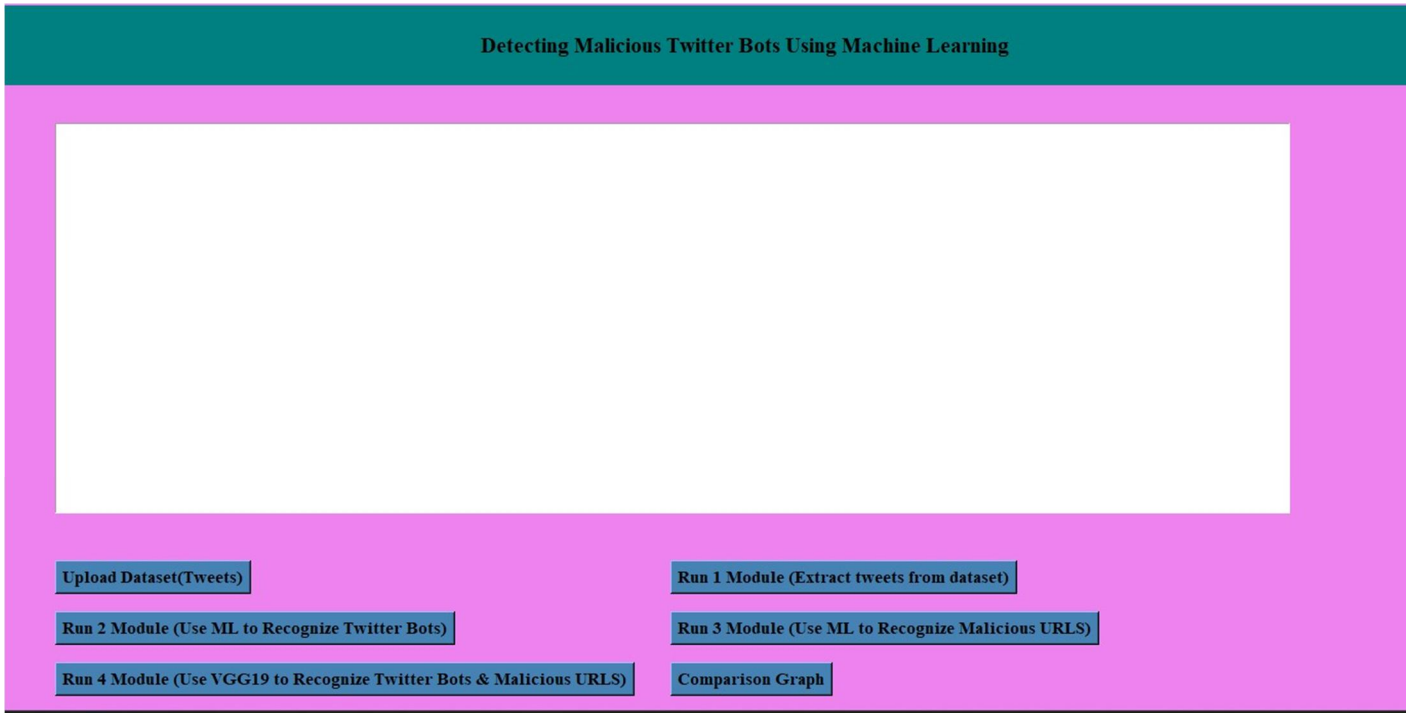


Fig 2: It represents the output screen

To upload the dataset we click the button named Upload Dataset (Tweets). The dataset is uploaded successfully.

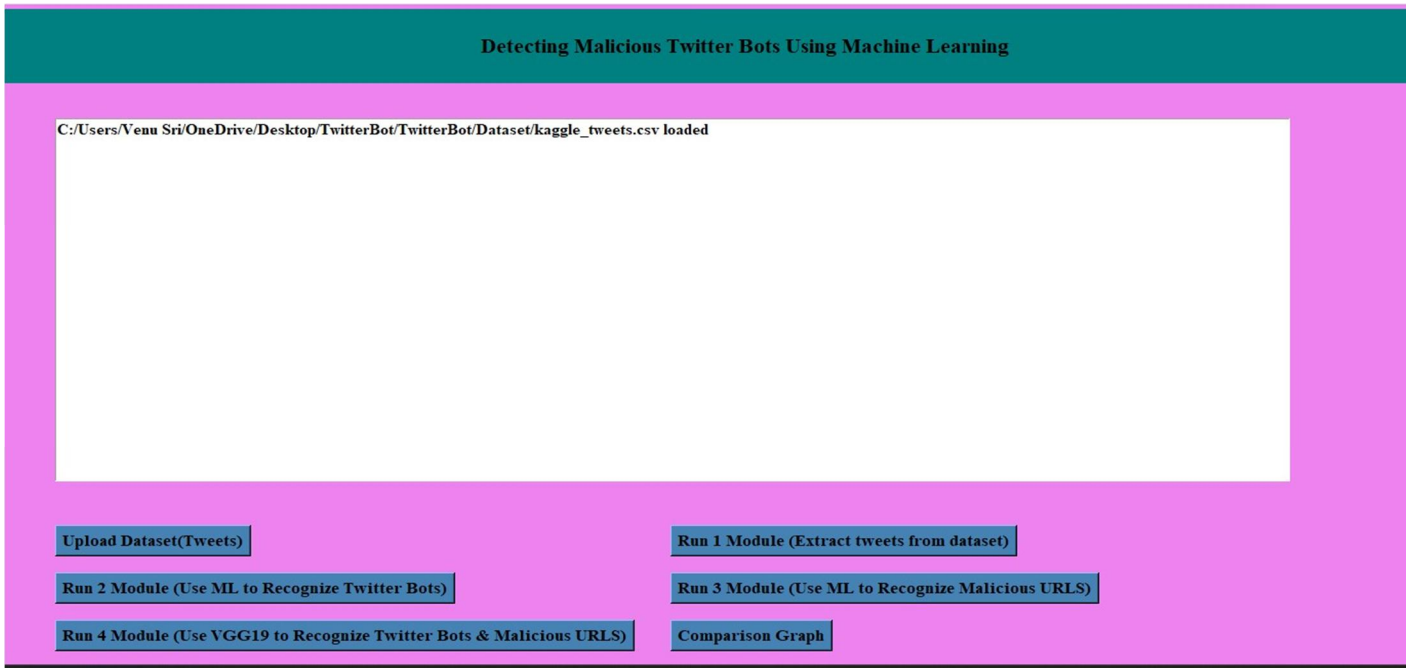


Fig 3: It represents the image when dataset is uploaded

When the dataset is uploaded successfully, we run first module to extract tweets from the dataset and read them.

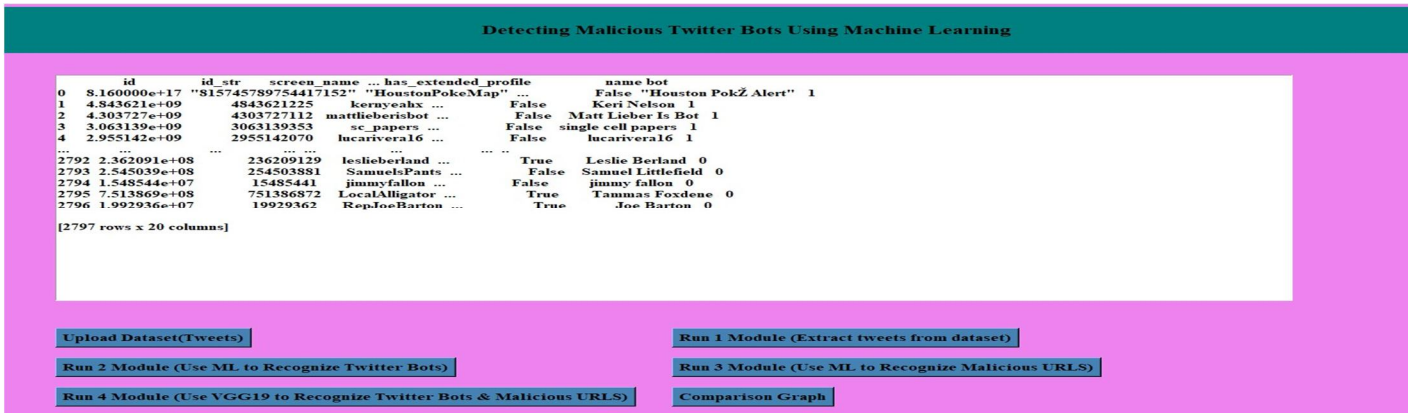


Fig 4: It represents the extraction of tweets from dataset

"Run 2 Module" to recognize the bots from real users using machine learning algorithm i.e; logistic regression. Using this, we got 71% accuracy.

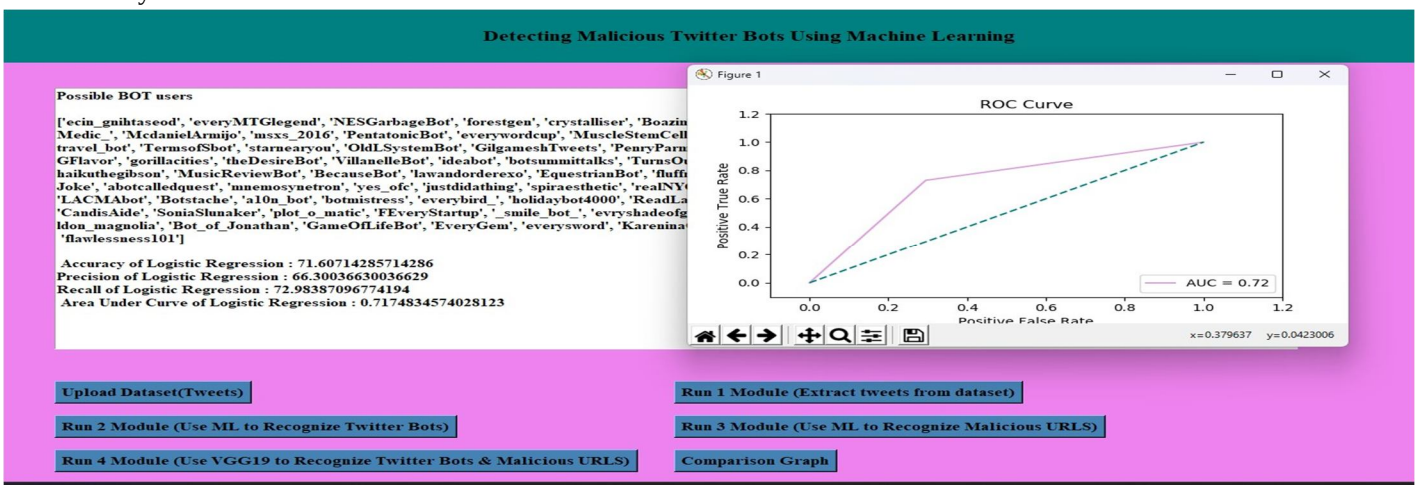


Fig 5: It presents the ROC for recognition of twitter bots

"Run 3 Module" to recognize malicious URLS using logistic machine learning algorithm. Using this we got accuracy of 73%.

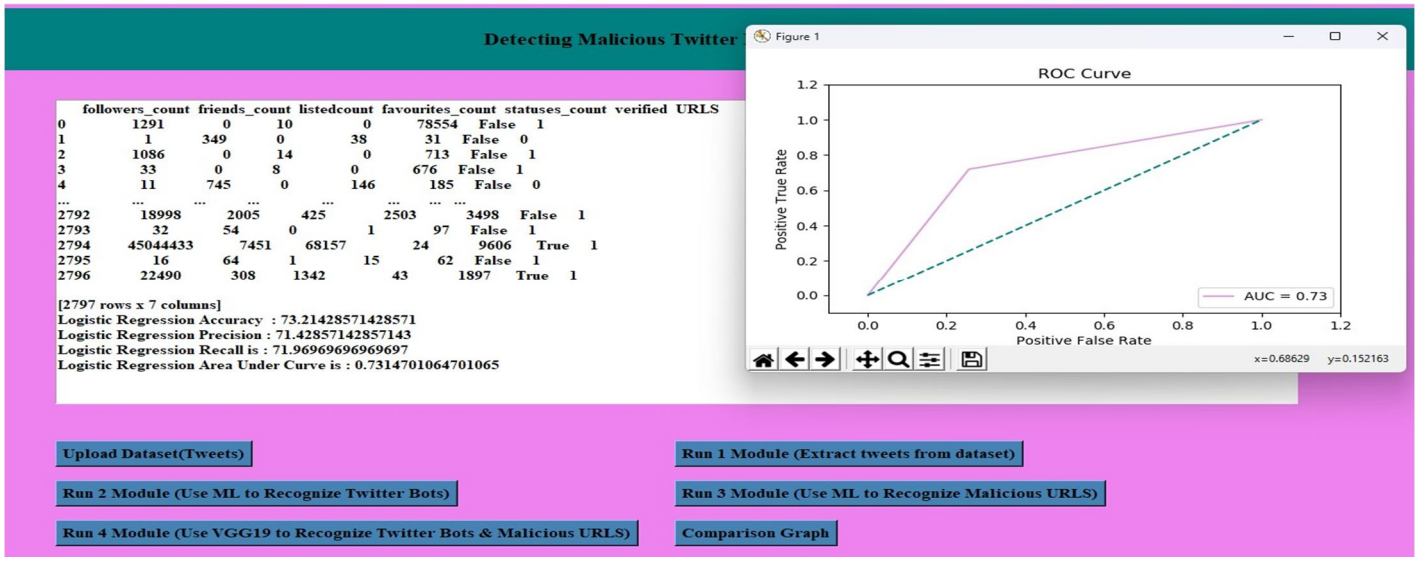


Fig 6: It represents the ROC of recognition of malicious URLS

"Run 4 Module" to detect bots and URLS at a time using deep learning algorithm VGG19.Using this we got accuracy of 87.5%.

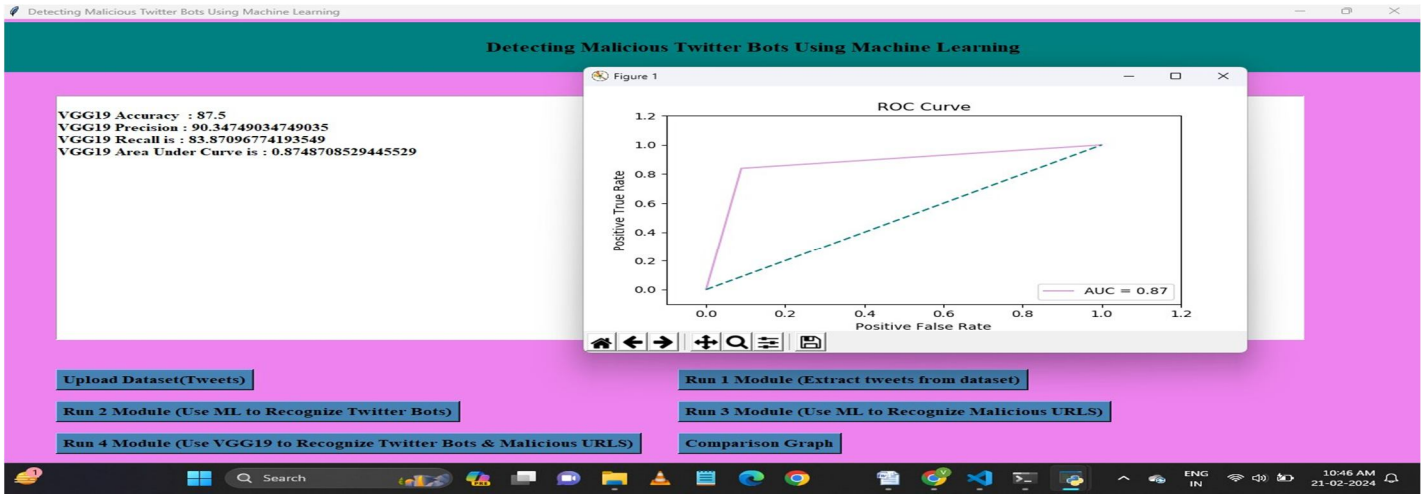


Fig 7: It represents the ROC for recognition of both malicious twitter bots and malicious URLS

To compare the results obtained by each module, we use "Comparison Graph" button and check which algorithm is best suited for detecting malicious twitter bots. By comparing it in a graph we got VGG19 with 87.5%.

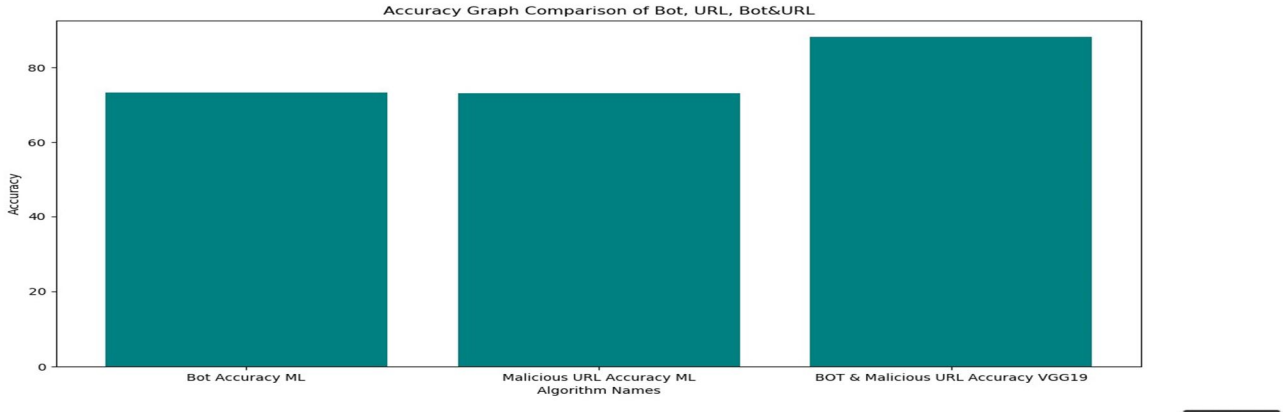


Fig 8: It represents the Accuracy comparison graphs

B. Comparison of Algorithms

Table 1 shows the graphical representation of the accuracy, precision, recall, AUC of the algorithms.

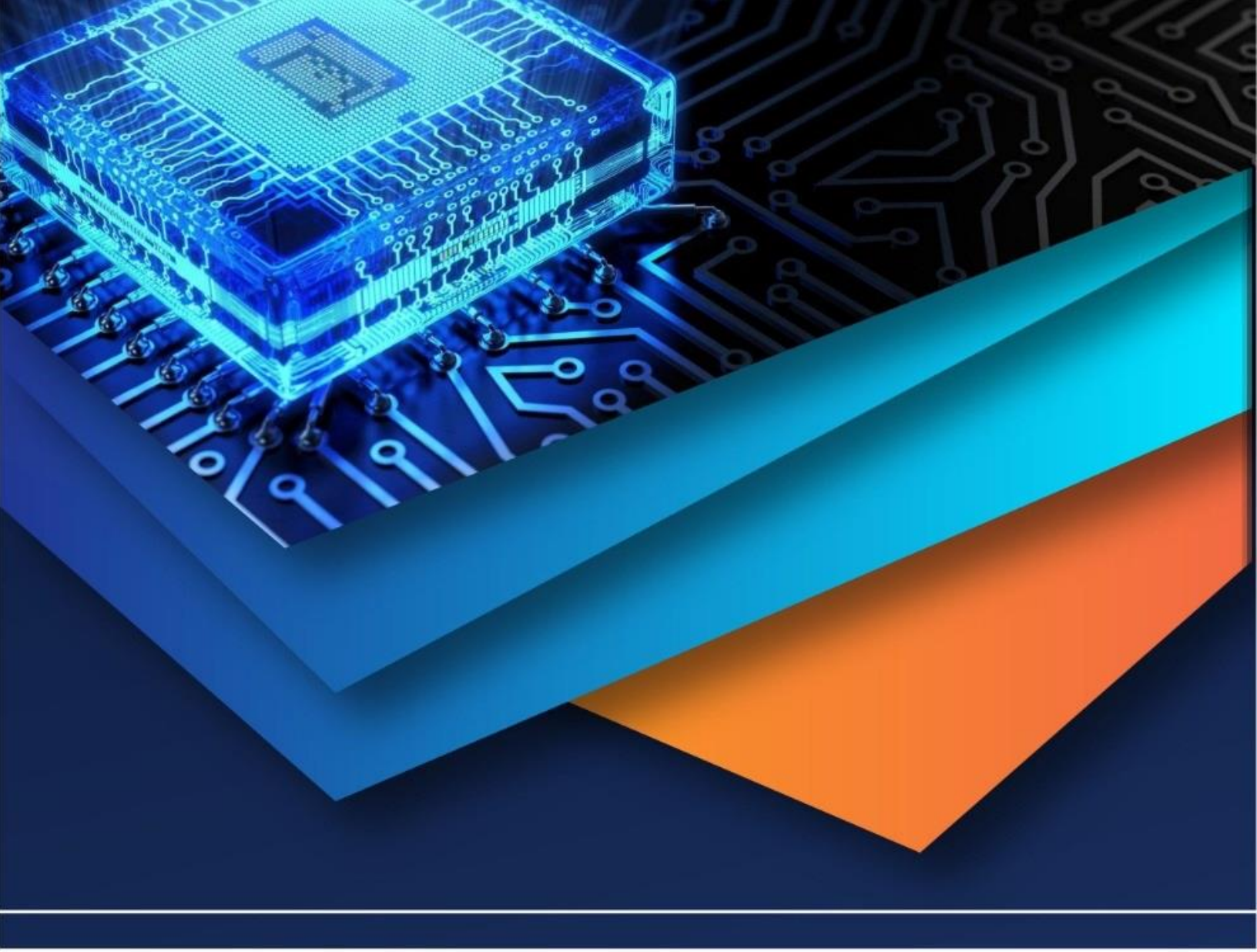
Algorithms	Bot Using ML	URL Using ML	Bot and URL using VGG19
Accuracy	71.60	73.21	87.5
Precision	66.30	71.42	90.34
Recall	72.98	71.96	83.87
AUC	0.71	0.73	0.83

V. CONCLUSION

We created a calculation in our investigate that distinguishes Twitter bots. Pack of words strategy for prepare information was the leading show VGG19 having tall precision compared to calculated relapse. Hence, word calculations were utilized to real-time information and the Twitter bots have been identified successfully. By using VGG19 along with convolutional neural network architecture we got a high accuracy when compared toLogistic regression machine learning algorithm.

REFERENCES

[1] VanDerWalt,E.,&Eloff,J.(2018).Using machine learning to detect fake identities:botsvshumans.IEEEaccess,6,6540-6549
[2] Nasim, M., Nguyen, A., Lothian, N., Cope, R., & Mitchell, L. (2018, April). Real-time detection of content polluters in partially observable Twitter networks. In Companion Proceedings of the The Web Conference 2018 (pp. 1331-1339).
[3] Khalil, A., Hajjdiab, H., & Al-Qirim, N. (2017). Detecting fake followers in twitter: A machine learning approach. International Journal of Machine Learning and Computing, 7(6), 198-202.
[4] Wetstone, J. H.,& Nayyar, S. R.(2017). I Spot a Bot: Building a binary classifier to detect bots on Twitter. CS 229Final Project Report.
[5] Karataş,A.,&Şahin,S. (2017).A review on social bot detection techniques and research directions.
[6] Chavoshi, N., Hamooni, H., & Mueen, A. (2016). Identifying correlated bots in twitter. In Social Informatics: 8th International Conference, SocInfo 2016, Bellevue, WA, USA, November 11-14, 2016, Proceedings, Part II 8 (pp. 14-21). Springer International Publishing.
[7] Perdana,R.S.,Muliawati,T.H.,&Alexandro,R.(2015).BotspammerdetectioninTwitterusingtweetsimilarityandtimeinterval entropy. JurnalIlmuKomputer dan Informasi, 8(1), 19-25.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY