Exposing Pernicious Bots in Twitter Utilizing User Profile Attributes and Machine Learning

KATTOJU SHIRISHA
M.Tech Student, Malla Reddy College of Engineering and Technology, Hyderabad,T.S, India.

Dr. M JAYAPAL
Associate Professor CSE, Malla Reddy College of Engineering and Technology, Hyderabad,T.S, India.

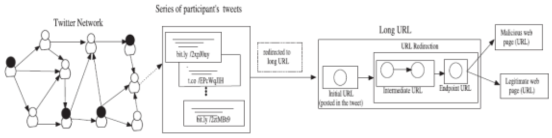
Dr. S SHANTHI
Professor & HOD Department of CSE, Malla Reddy College of Engineering and Technology, Hyderabad,T.S, India.

Abstract: - **With the rampant usage of social media, fraudsters try to employ malevolent social bots that tend to generate counterfeit tweets and try to establish relationships with other users on the social media by acting like followers or try to generate multiple counterfeit accounts that get involved in malevolent activities. They also tend to post malevolent URLs that are used to navigate genuine users to malevolent web servers. Thus it is very essential to differentiate the bot accounts from genuine accounts. It is observed that bots can be identified by analyzing the profile based featured and URL features that they post such as redirected URL, spam data, frequency of URL sharing etc than social features. In this project, we suggest a novel approach using Deep Learning techniques that uses profile based features for exposing pernicious bots on social networks. We feed the Twitter data set to the above-mentioned model and observe that it gives better performance than other algorithms. we also tried to build a web application that can show that the above approach gives better performance when compared to other existing models.**

Keywords:- **Recommendation Algorithm; Emotional Polarity Classification; Recommender System; Collaborative Filtering;**

I INTRODUCTION

Social media platforms have lots of accounts in which users post and share content with each other. However, since there are millions of profiles but is not able to manually check it's an account is agenda not a fake account. In due course of time many fake accounts have been created like malevolent bots get may cause harm to genuine users in the form of spamming, posting and sharing URLs that redirect the users to malevolent servers etc. so that users may share their personal information unknowingly and it could be misused for other illegal transactions [1]. Hence it is very much essential. One must be able to predict whether a Twitter account is a bot or not So that all bot accounts may be monitored and deactivated if necessary. Most of the existing techniques make use of attributes related to social activity but it has been observed that profile based features and URL features plays an important rolein identifying malevolent bots. Hence in this project, we come up with a novel approach that can identify a bot using profile based features. We have used the Twitter data set and fed it to the proposed model that is built using advanced machine learning techniques and observe that it gives better performance when compared to the existing systems. An example of such spamming technique is shown below:



AIM OF THE PROJECT

The main of the project is to identify pernicious bots in twitter accounts based on profile based features. We have used the Twitter data set and fed it to the proposed model that is built using advanced machine learning techniques

SCOPE OF THE PROJECT

The scope of the project is limited to the compute the accuracy of the proposed model and identify pernicious bots. The admin of the system trains the proposed model with training data and tests the model with test data. The results of the test data are saved in "results.csv" file. Maintenance of user accounts, Monitoring the accounts or de-activating the bots does not fall under the scope of the project [2]. Pernicious bots can be exposed using URL based features but it has not been used in the project as the we are able to achieve an accuracy of about 93% for the given dataset with the BOT Prediction algorithm.

II LITERATURE SURVEY

2.1 "Detecting Malicious Social Bots Based on Clickstream Sequences"

With the rampant usage of social media and maintaining millions of accounts, one cannot verify if an account is genuine or counterfeit. many fake accounts Have been created by fraudsters to spam other users and other illegal activities. Hence it is very important that the fake accounts are detected and deactivated or removed. Many existing techniques identify bots using quantitative analysis of their account behavior.

2.2“Adaptive deepQ-learning model for detecting social bots and influential users inonline social networks”

Many social platforms in networks like Twitter, Facebook have fake accounts called botswhich try to establish relationships with genuine followers and post spammed content to the users so that they can get some personal information and misuse it [4]. They also have the capabilities of manipulating or modifying public opinion. It is not possible to manually figure out which account is a bot and which account is not. In this paper a novel technique called deep Q learning model has been proposed which will be able to detect a bot based on the social parameters or attributes such as profile features etc. It also proposes and approach that can identify the most influential users on a network and observe their activity. Experimental results show that the deep learning model Is successful in both the cases.

III SYSTEM ANALYSIS

Existing system:

With the extensive use of social networks like Facebook, Twitter etc, Malicious users try to create fake accounts with the help of bots and manipulate users opinions find redirect them to malicious sites using spamming. Traditional techniques to identify search bots are not helpful as they rely on features that the bots use to establish relationships with genuine users [3]. One cannot make out if the account is a bot or not manually. Many techniques have come up based on social features but they're not really helpful.

Disadvantages:

- low accuracy
- not helpful to identify bots in real time environments

Proposed System:

The proposed system implements a novel technique to identify bots using URL features and relationship features called “BOT PREDICTION ALGORITHM”. The profile based features mentioned in the below table would help in identifying pernicious social bots and check if the users are being redirected to fake websites where they may input their personal data [5][6]. The below features have helped in identifying bots with high accuracy.

Advantages:

- High accuracy
- Can be extended to real time environments.

IV IMPLEMENTATION

Below is the proposed modular implementation of the project. It consists of modules:

1. Admin

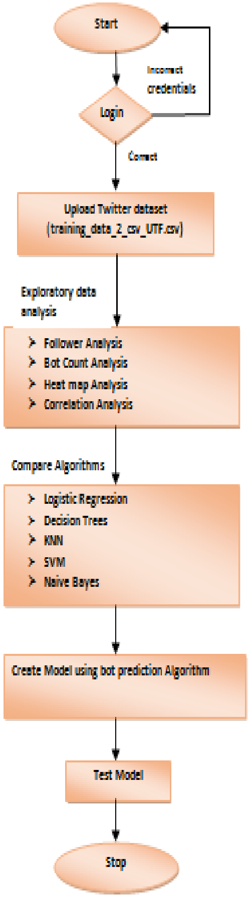
Admin Module:

The admin of the system is responsible for the activities like:

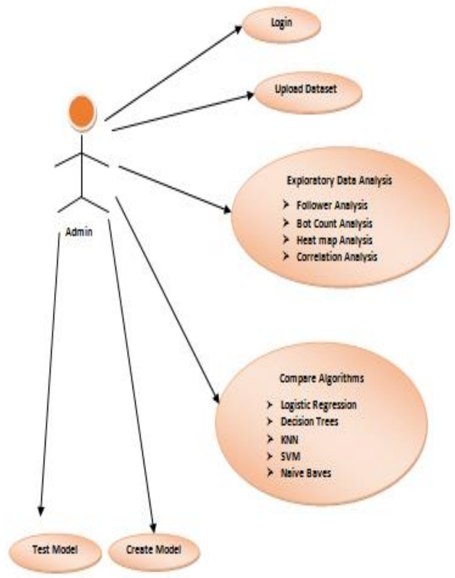
1. Uploading the dataset
2. Analysis of user Twitter data.
3. Comparison of various machine learning algorithms on the twitter bot dataset.
4. Build model for Pernicious Bot Detection.
5. Review the performance of the algorithms on the given dataset
6. Test the model for pernicious bot prediction using test data.

V. SYSTEM DESIGN

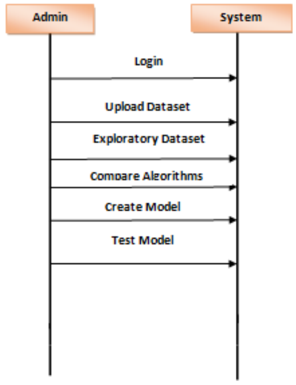
Data Flow Diagram: Admin



Use Case Diagram: Admin

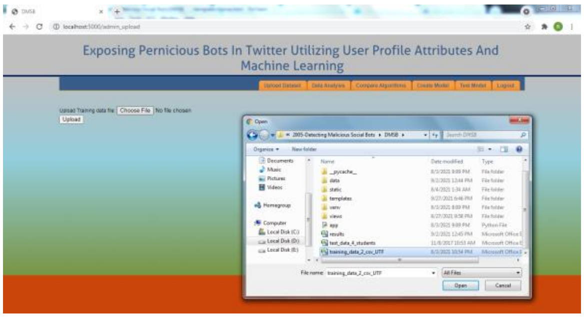


Sequence Diagram:



VI PROJECT EXECUTION

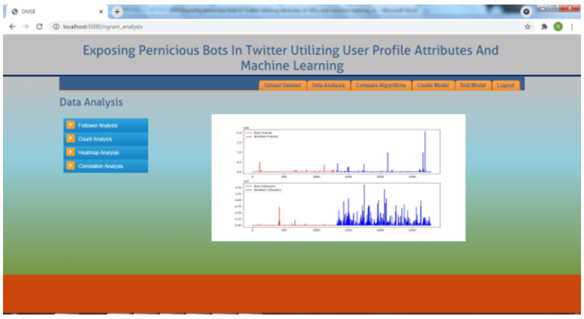
Upload Dataset:



Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

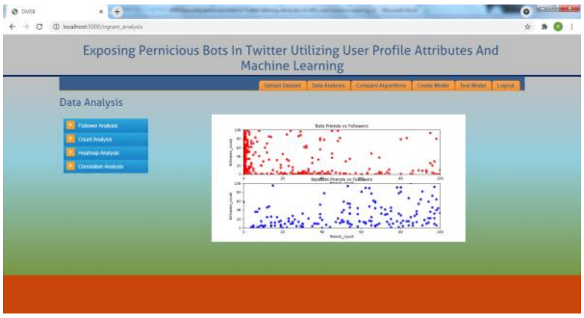
Data Analysis:

- **Follower Analysis:**



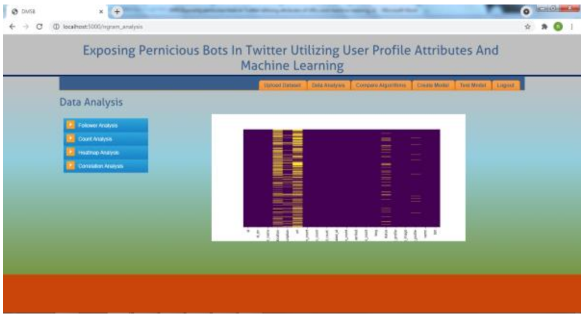
Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

- **Count Analysis:**



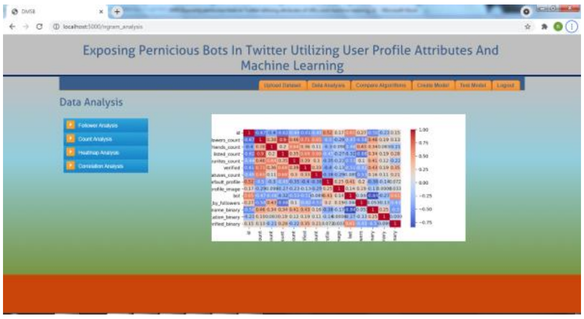
Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

- **Heatmap Analysis:**



Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

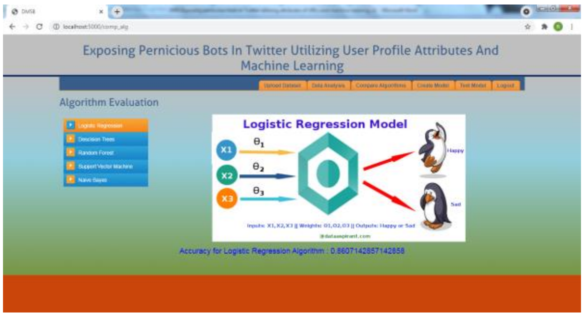
- **Correlation Analysis:**



Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Compare Algorithms:

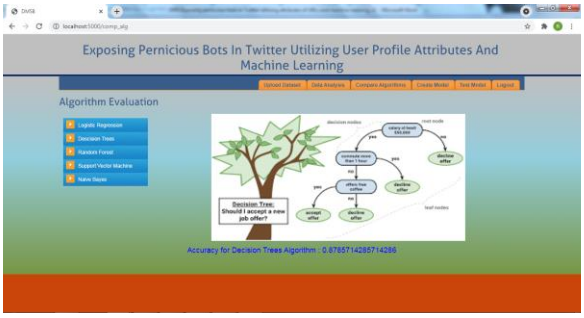
- **Logistic Regression:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Algorithm Evaluation

Accuracy for Logistic Regression Algorithm : 0.8607142857142858

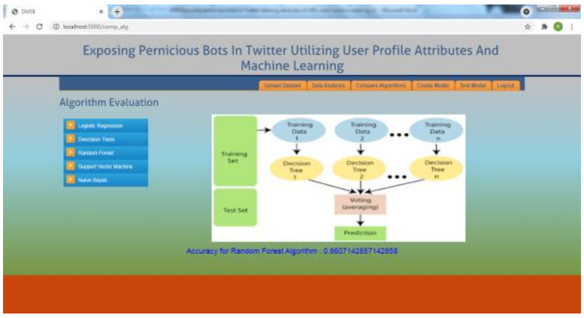
- **Decision Trees:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Algorithm Evaluation

Accuracy for Decision Trees Algorithm : 0.8785714285714286

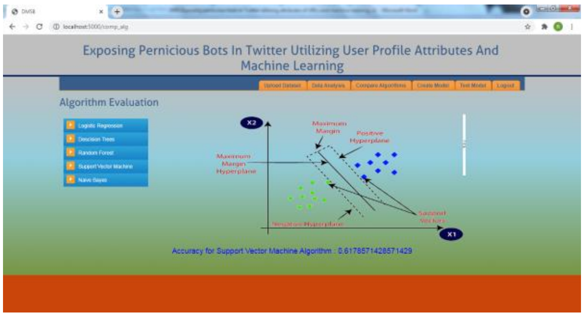
- **Random Forest:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Algorithm Evaluation

Accuracy for Random Forest Algorithm : 0.8607142857142858

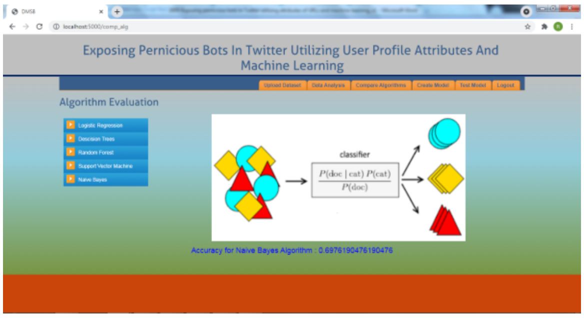
- **Support Vector Machine:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Algorithm Evaluation

Accuracy for Support Vector Machine Algorithm : 0.6178571428571429

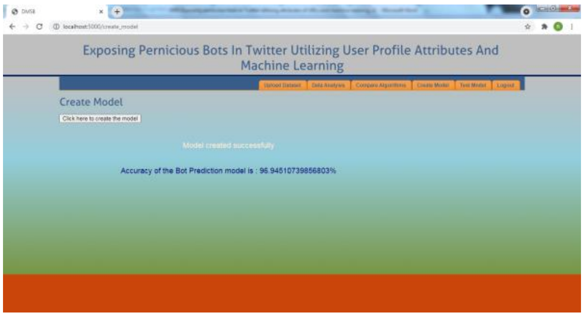
- **Naive Bayes Algorithm:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Algorithm Evaluation

Accuracy for Naive Bayes Algorithm : 0.6976190476190476

- **Create Model:**

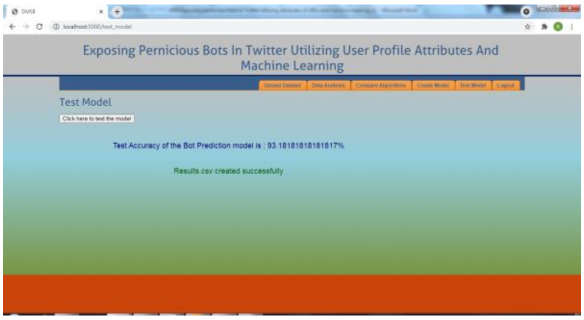

Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Create Model

Model created successfully

Accuracy of the Bot Prediction model is : 96.94510739856803%

- **Test Model:**


Exposing Pernicious Bots In Twitter Utilizing User Profile Attributes And Machine Learning

Test Model

Test Accuracy of the Bot Prediction model is : 93.18181818181817%

Results.csv created successfully

VII CONCLUSION

In this project we have proposed a novel mechanism in which the virtual machines and their data on the cloud server can be safeguarded for data privacy and confidentiality with the help of hypervisors to encrypt the virtual machines and decrypt them for the authorized people. We demonstrated this using medical scenario in which a patient can upload his health information in encrypted format to the cloud server. The doctor can view this health information and suggest required medicines. An insider such as an untrusted cloud service administrator can try to modify or steal this information but that gets recorded and would be available for the cloud service provider for stringent actions.

FUTURE ENHANCEMENT:

In future, an add-on to a novel mechanism in which the virtual machines and their data on the cloud server can be safeguarded for data privacy and confidentiality with the help of hypervisors to encrypt the virtual machines and decrypt them for the authorized people and scale the system for larger environments in public clouds.

REFERENCES

[1] I. Khan, Z. Anwar, B. Bordbar, E. Ritter and H. Rehman, "A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds", IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 942-954, Oct.-Dec. 2018.

[2] T. Gunasekhar and K. Thirupathi Rao, "Framework for Prevention of Insider attacks in Cloud Infrastructure through Hardware Security", Journal of Adv Research in Dynamical & Control Systems, vol. 9, no. 4, 2017.

[3] J.M. McCune, B.J. Parno, A. Perrig, M.K. Reiter and H Isozaki, "Flicker: An execution infrastructure for TCB minimization", ACM SIGOPS Operating Systems Review, vol. 42, pp. 4, 2008.

[4] J.M. McCune, Y. Li, N. Qu, Z. Zhou, A. Datta, V. Gligor, et al., "Trust Visor: Efficient TCB reduction and attestation", IEEE Symposium on Security and Privacy (SP), 2010.

[5] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, et al., "The eucalyptus open source cloud computing system", Proc. 9th IEEE/ACM Int. Symp. Cluster Comput. Grid, 2009.

[6] AMD64 virtualization: Secure virtual machine architecture reference manual, AMD Publication, no. 33047, May. 2005.

[7] R. Sailer, X. Zhang, T. Jaeger and L. van Doorn, "Design and implementation of a TCG-based integrity measurement architecture", Proc. 13th USENIX Security Symp., 2004.

[8] Adrian J Duncan, Sadie Creese and Michael Goldsmith, "Insider Attacks in Cloud Computing", IEEE 11th International Conference on Trust Security and Privacy in Computing and Communications, 2016.

[9] F. Rocha and M. Correia, "Lucy in the sky without diamonds: “Stealing confidential data in the cloud", IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), 2011.

[10] “Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing”, IEEE Transactions on Cloud Computing, 2020.