Journal
of the
Oriental Institute
M.S. University of Baroda
ISSN: 0030-5324

FAKE NEWS DETECTION USING DEEP LEARNING

I.Venu[1],Dr.I .Satyanarayana[2], K.Jalaja[3],K.Vaishnavi[4] ,K. Ravikiran[5] ,K.Poojitha[6]
[1]Assistant Professor, Dept. of ECE, Sri Indu Institute of Engineering & Technology, Hyderabad.
[2] Principal and Professor, Dept. of ME, Sri Indu Institute of Engineering & Technology, Hyderabad.
[3-6] Student, Dept. of ECE, Sri Indu Institute of Engineering & Technology, Hyderabad.

ABSTRACT: Social networking websites have become an integral part of the day-to- day lives of people. People turn to social media for interacting with other people, sharing ideas, gaining knowledge, for entertainment, and staying informed about the events happening in the rest of the world. Among these sites, YouTube has emerged as the most popular website for sharing and viewing video content. This popularity of YouTube has also attracted scammers, who upload video Swith the sole purpose of polluting the system content and causing dissatisfaction among other viewers. These spam videos may be unrelated to their title or may contain pornographic content. Therefore,it is very important to find a way to detect these videos and report them before they are viewed byinnocent users. In this paper, we propose a Markov Decision Process[4] approach to model the problem of YouTube video spam detection. We analyze the accuracy of the policy returned by the model and compare it with the accuracy of other data mining[2] algorithms that have been proposed for video spam detection.

Index Terms—Markov Decision Process, spam detection, optimal policy, YouTube.

Algorithms:- Keras, Sklearn, LSTM, Tokeniz

1. INTRODUCTION

In the recent past, social media has emerged to be the most dominant medium for communication and information sharing. Various social networking platforms such as Facebook, You tube, Twitter, and Instagram have gained widespread popularity among users. These websites offer not only text-based interaction services but also allow the sharing of multimedia content such as photos, videos, and GIFs.The ease of uploading, viewing, and sharing videos is the main reason for the rapid growth of the popularity of You tube in the last few years. To upload a video, a user merely has to create an account, choose the video source and privacy settings and then upload the video. There is a wide range of categories under which videos can beuploaded Neural Network A number of techniques for spam detection have been proposed in the literature. In this paper, we model the problem of YouTube video spam detection[1-2] using a MDP such as Entertainment, Sports, Education, Travel and Events, Science and Technology, News, and Politics to name a few. While the ease of video sharing

on You tube has enabled different forms of video communication and exchange of information and ideas among people from different parts of the world, it has also encouraged the system by actions such as self- promotion, video aliasing, and video Spamming.. The main purpose is to demonstrate an alternative scheme, with the use of Neural Network A number of techniques for spam detection have been proposed in the literature. In this paper, we model the problem of YouTube video[1-2] spam detection using a Markov Decision Process (MDP).

Algorithms

Keras:- Keras is a high-level, deep learning API developed by google for implementing neural network It is written in Python and is used **t**o make the implementation of neural networks easy. It also supports multiple backend neural network computations.

Sklearn:- What is Scikit-learn or Sklearn? Scikit- learn is probably the most useful library for machine learning in Python. The Sklearn library contains a lot of efficient tools for machine learning and statistical modeling including classification, regression, clustering and dimensionality reduction.

LSTM:- LSTM stands for Long-Short Term Memory. LSTM is a type of recurrent neural network but is better than traditional recurrent neural networks in terms of memory.

Tokenize:- Tokenization is the act of breaking up a sequence of strings into pieces such as words, keywords, phrases, symbols and other elements called tokens. Tokens can be individual words, phrases or even whole sentences. In the process of tokenization, some characters like punctuation marks are discarded.

2.LITERATURE SURVEY

Spam Detection:-

Social media has become a hub for broadcasting and receiving information on relevant topics from various areas of interest. Information uploaded online can be in the form of editorial posts, or audio or video files. Recent years have seen an increase in the spamming of social media through videos. Classification of spam is done with the help of attributes such as duration, comment count, like count, etc. It works with algorithms such as Naive Bayes, Decision tree, and Many spam detection techniques are being used now-adays. The rate 82%, 6% positive rate and 91% accuracy An approach using random forest algorithm approach is proposed by Akinyelu.

Methodology:-

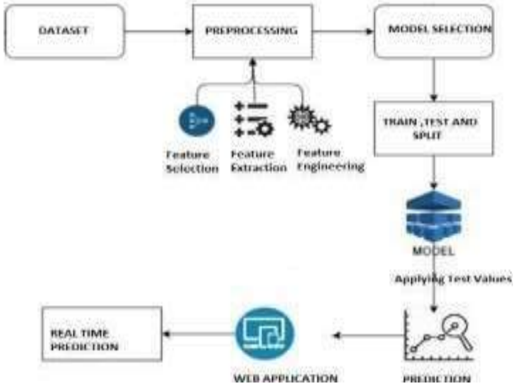


Fig.1: System Diagram

Pre-processing: This is the first stage that is executed whenever an incoming video is received. This step consists of tokenization.

Tokenization: This is a process that removes the words in the body of anemail. It also transforms a message to its meaningful parts. It takes the you tube and divides it into a sequence of representative symbols called tokens. Subramaniam, Jalab and Taqa emphasised that these representative symbolsare extracted from the body of the you tube, the header and subject.

Feature selection: The technique is beneficial when the size of the message is large and a condensed feature representation is needed to make the taskof text orimage matching snappy . big money through “work-from-home” jobs, online shopping, pleading and gift requests, business proposals and others. Some of the most important features for spam filtering include: Adult content and Bag of words from the **message content**

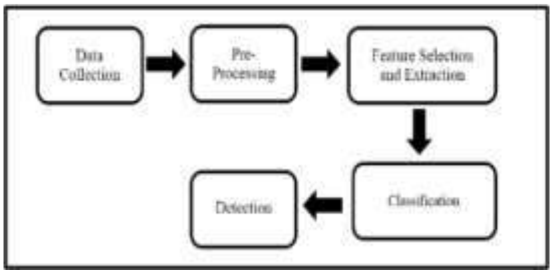
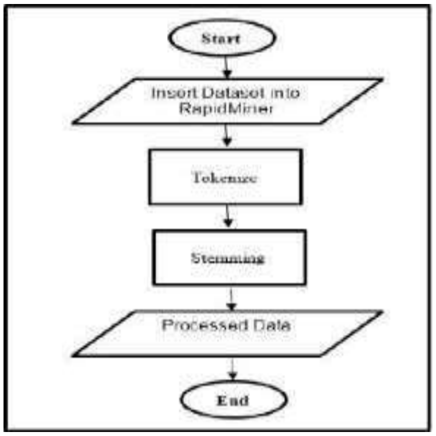


Fig.2: Flowchart of YouTube Spam Detection

Algorithm:-



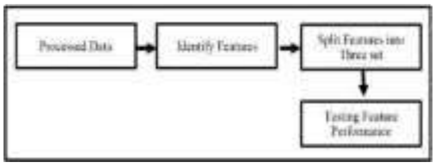


Fig.3: Flowchart of video detection

The spam detection system presented in the paper by Yuhanis Yusof et al. employs the EdgeRank algorithm used by Facebook to extract certain new features to aid in the determination of online video spammers Markov Decision Process model[4-8] to select the best action to be taken based on the optimal policy such that the system’s security. Resource consumption is kept at a minimum level.Njilla[7] et al. describe the problem of allocating finitecyber security resources among the two defense layers of agility and recovery. The states of the MDP are the coordinates of a grid with actions indicating the directions that the aircraft can take. The reward function for this model is based on theposition of intruders and threats and targets.

3..EXISTING SYSTEMS

Due to the increase in the number of YouTube users, the amount of spam videos have also risen innumber in the past years. It has now become even more challenging to handle a wide range of emails for data mining and machine learning. Hence, it isimportant to find an algorithm that gives the best possible outcome for any particular metric for correct classification of videos and spam or ham. The present systems of spam detection are reliant on three major methods:-

A. Linguistic Based Methods: Unlike humans, who can grasp linguistic constructs along with their exposition, machines cannot and hence it is necessary to teach machines some languages to help them understand these constructs.Since this technique requires that every expression be remembered, this method is not feasible and also time intensive.

B. Behavior-Based Methods: This technique is Metadata-based. This approach requires that users generate a set of rules, and the users must have a thorough understanding of these rules. Since the attributes of spam change over time so the rulesalso need to be reformed from time to time. As a result, it still requires a human to scrutinise the details and is majorly user-dependent.

C. Graph-Based Methods: This technique uses a single graphical representationby incorporating numerous, heterogeneous particulars. Graph-based anomaly recognition algorithms are executed which detect abnormalforms in the data showing behaviours of spammers.

4.DATA SET GENERATION

For data generation, we used publicly available APIs[1-2] to crawl YouTube and extract the required attributes of a given video. The first API is you tube. Search .the list takes a searchquery as an input parameter and returns the video IDs corresponding to 50 videos relevant to the search query. This API was run for each of the 50 videos obtained as output from the first API. The attributes collected for each video include Video Title, Video ID, ViewCount, Like Count, Dislike Count, Comment Count, Duration, and Category ID. This datasetwas used to create the MDP to classify a video as legitimate or spam. As no such dataset is publicly available, we aim to publish this dataset online so that it can be used by other researchers in this field.

5.CONSTRUCTION OFMARKOV DECISIONPROCESS MODEL

: Definition

A Markov Decision Process (MDP) is a mathematical model that is used to make decisions in a stochastic environment. A stochasticenvironment is one where outcomes are partially random and partially under the decision maker's control . In an MDP, the environment is modeled as a discrete-time state-transition system witha setof states and actions. The states represent the outcomes of the decision-making process, and action represents a decision that can be taken from a particular state.

: Representation

A is a finite set of actions. • P is a state transition probability. function. P(s 0 |s, a) is the probability of going to state s 0 on taking the action a from state s. P(s 0
|s, a) = P r{St+1 = s 0 | St = s, At = a}

• R is a reward function . R(s, a, s0) is the expected reward on taking action a from states to go state s 0 . R(s, a, s0) =E[Rt+1|St = s, At = a, St+l = s 0 • γ is the discount factor, where γ is in [0,1] Discounting is taken into account because a reward earned in the future is not worth quite as much as a reward earned now. Markov Property This property states that the future is independent of the past given the present. In other words, a state St is Markov if and only if : P[St+1|St] = P[St+1|S1, ..., St] (3)The state captures all relevant information fromthe history and is a sufficient statistic of the future. For any process to be a Markov Decision Policy A policy π is a mapping from a state, s ∈ S, to action, a ∈ A(s), and is denoted as follows: π(s) = a (4) where a is the optimal action to be taken from state s according to the policy π. C. Spam Detection using Markov Decision Process As described earlier, a Markov Decision Process isrepresented[4] by a tuple (S, A, P, R, γ).

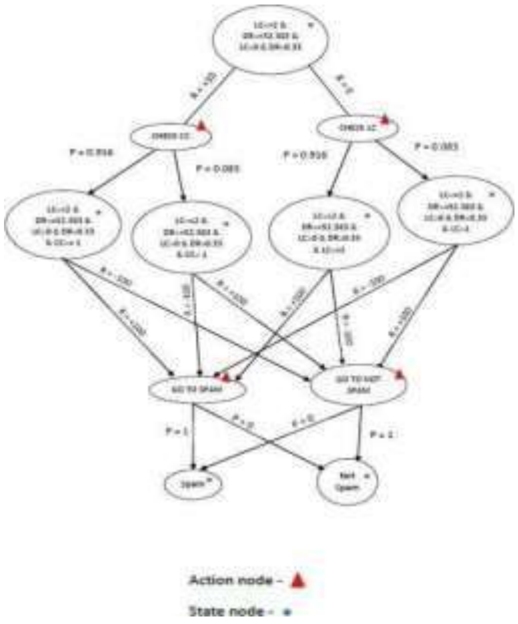


Fig.4: Representation of MDP

1) Reward = +80 (R1), if the state takes the right action to 'go to spam' or 'go to not spam. These actions are given a high reward because our ultimate aim is to classify the video into one of these categories.

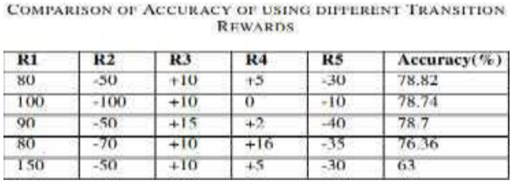
2) Reward = -50 (R2), if the state is supposed to take

the action ‘go to spam’ but instead takes the action ‘go to not spam’ and vice versa. A negative reward (cost) is associated with these actions because we do not want the video to be incorrectlyclassified.

3) Reward = +10 (R3), if the state takes the intended action from the state other than ‘go to spam’ and ‘go-to not spam. This reward is given to convey to the agent that it has taken the right step towards achieving the goal.

4) Reward = +5 (R4), if the state takes the next best action (i.e., the action that is better than all other actions except the optimal action from aparticular state).

5) Reward = -30 (R5), for all other state-action pairs. A negative reward is given to the agent if it chooses the incorrect action from a particular state.



COMPARISON OF ACCURACY OF USING DIFFERENT TRANSITION REWARDS

R1	R2	R3	R4	R5	Accuracy(%)
80	-50	+10	+5	-30	78.82
100	-100	+10	0	-10	78.74
90	-50	+15	+2	-40	78.7
80	-70	+10	+16	-35	76.36
150	-50	+10	+5	-30	63

Table .1: Comparison of Accuracy Using Different Transition Rewards

D. Markov Decision Process MDP By using the transition probabilities andsubsection, we constructed an (8 ∗ 211 ∗ 211) transition probability matrix which is of the form (A ∗S ∗S) and a (211 ∗8) reward matrix which is of the form (S ∗ A) where S is the number of states .

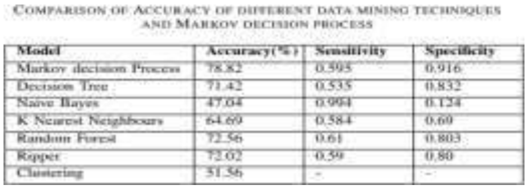
6.RESULTS

As described in the previous section, we utilized the map toolbox for python to generatethe ideal policy for video spam detection using the formulated MDP[6]. For this purpose, we executed three inbuilt algorithms in the toolbox, namely, Policy Iteration, Value Iteration, and Q-Learning. Each of these algorithms takes the transition probability matrix, the reward matrix, and the discount factor as input and returns a policy as the output. To evaluate the accuracy of the policy returned by each of these algorithms, we partitioned the dataset into a training set and a test set. The training set was used to build the MDP[4], and the test set was used for policy evaluation. The result so obtained was then compared with the actual results fromthe test set to check for the accuracy of the model. The transition probability matrix and reward matrix was given as input to each algorithm. On analyzing the accuracy of each algorithm, it was concluded that Value Iteration and Policy Iteration return the same optimal policy and they have better average accuracy than the Q Learning algorithm. Policy Iteration methods which are model-based reinforcement learning
Algorithms that utilize the transition probabilities given as input to the agent. The results have been recorded and documentedin Table 5 shown below.

Table2 : Comparison of Accuracy ofReinforcement Learning Algorithms

Comparison of Accuracy with other models Rashid et al. used a data mining based spam detection system for You Tube. The accuracy of Naive Bayes, K Nearest Neighbours (KNN) and Clustering techniques is inferior as compared to that of the MDP. A high sensitivity implies that the model correctly classifies majority of the videos belonging to the ‘spam’ category. This can beattributed to the stochastic nature of the MDP[4].

Table 3: Comparison of Accuracy of Different DataMining Techniques and MDV

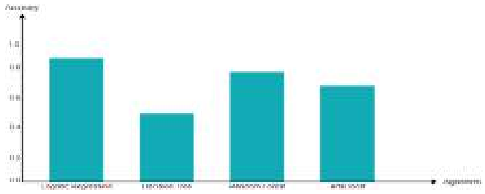


COMPARISON OF ACCURACY OF DIFFERENT DATA MINING TECHNIQUES AND MARKOV DECISION PROCESS

Model	Accuracy(%)	Sensitivity	Specificity
Markov decision Process	78.82	0.595	0.916
Decision Tree	71.42	0.535	0.832
Naive Bayes	47.64	0.994	0.124
K Nearest Neighbours	64.69	0.584	0.69
Random Forest	72.56	0.61	0.803
Ripper	72.02	0.59	0.80
Clustering	51.56	-	-

7.Conclusion &Future Work

In the past few years, social media has gained wide popularity among people and forms a major part of our day-to-day lives. Video sharing is emerging as the favored means of communication for conferences, educational activities, political propaganda, and marketing purposes to name a few. The ease of use of You Tube has attracted spammers who aim at circulating foul content or advertising a particular product etc. The existing systems for spam detection use data mining algorithms that do not have sufficient accuracy. In this paper, we proposed a Markov Decision Process approach[6-8] to model the problem We aim to make our dataset publicly available so that it can be used by other people who intend to conduct research in this field. The prospective future work can be aimed at improving the accuracy of the policy obtained. Twitter, the most famous web based life stages, gives a helpful method to individuals to impart what's more, speak with each other. It has beenall around perceived that impact exists during clients' co-operations. construing impact jobs.



COMPARISON OF ACCURACY OF REINFORCEMENT LEARNING ALGORITHMS

Algorithm	Average Accuracy(%)
Value Iteration	78.82
Policy Iteration	78.82
Q Learning	76.36

Fig 7.1.1: Analysis Graph

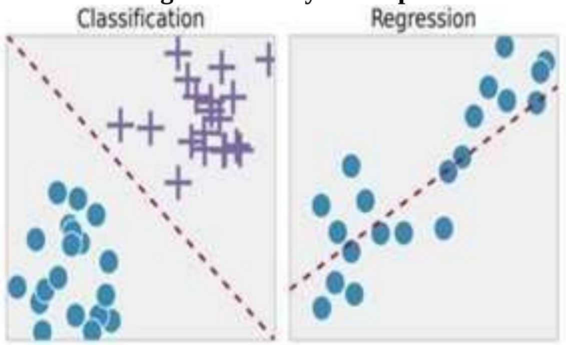


Figure 7.1.2: Difference betweenClassification and Regression

Figure 7.1.3: Home Page

8.REFERENCES

[1] A. D. Luz, E. Valle, and A. D. A. Araujo, "A Context-aware Description for Content Filtering on Video Sharing Social Networks," in Proceedings of IEEE InternationalConference on Multimedia and Expo, 2012

[2] R. Chowdury, M. N. M. Adnan, G. A. N. Mahmud, and R. M. Rahman, "A data mining based spam detection system forYouTube," in Proceedings of Eighth International Conference on Digital Information Management, 2013.

[3] P. S. Kiran, "Detecting spammers in YouTube: A study to find spam content in a video platform,"IOSR Journal of Engineering, vol. 05, no. 07, pp. 2630, 2015.

[4] O. Hayatle, H. Otrok, and A. Youssef, "A Markov Decision Process Model for High Interaction Honeypots," Information Security Journal: A Global Perspective, vol. 22, no. 4, pp. 159170, 2013

[5] M. M. Taibah, E. Al-Shaer, and R. Boutaba, "An Architecture for an Email- Worm Prevention System," in Proceedings of Securecomm and Workshops, 2006.

[6] Y. Fu, X. Yu, and Y. Zhang, "Sense and collision avoidance of Unmanned Aerial Vehicles using Markov Decision Process and flatness approach," in Proceedings of IEEE International Conference on Information andAutomation, 2015.

[7] L. L. Njilla, C. A. Kamhoua, K. A. Kwiat, P. Hurley, and N. Pissinou, "Cyber Security Resource Allocation: A Markov Decision Process Approach," in Proceedings of IEEE 18th International Symposium on High Assurance SystemsEngineering, 2017.

[8] W. Zong, F. Wu, and Z. Jiang, "A Markov-Based Update Policy for Constantly Changing Database Systems," IEEE Transactions on Engineering Management, vol. 64, no. 3,pp. 287300, 2017.