Phishing Detection System Using Dueling Network

MSc Internship

Cyber Security

Mohammed Afnan Ikram

Student ID: 18189725

School of Computing

National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Mohammed Afnan Ikram		
Student ID:	18189725		
Programme:	Cyber Security	**Year**	2019-20
Module:	MSc Internship		
Supervisor:	Ross Spelman		
Submission Due Date:	17 September, 2020		
Project Title:	Phishing Detection System using Dueling Network		
Word Count:	……………………………………… **Page Count**……………………………………………….……..		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:

Date: 17, September, 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Phishing Detection System Using Dueling Network

Mohammed Afnan Ikram

18189725

Abstract

Cyber attackers pull millions of dollars through phishing attack every year. Adding basics of social engineering in phishing makes the attack more effective. We can say, it is the modest way of cybercrime which has the aim of playing foul with people to steal their private sensitive information like bank details, passwords, credit/debit card details or other important personal identification details. The personal data or credentials stolen are used by the attacker to get illegal access of victim's personal accounts which could result in leak of private data or monetary loss. so, the first step taken to initiate the phishing attack is to send the infected messages and gather victims information, than on the basis of the information gathered through social engineering, attacker setup the deceptive copy of the original website, where the target is conned to enter its personal information or credentials.

In today's era of Artificial intelligence, machines are getting more advanced, Intellectual and smart enough to take decision on their own. It will not be wrong assuming that using these advancement, cyber criminals are also working hard finding loopholes in our system which can be undetected.

So, it is very important to develop a technology which is smart enough to evolve itself by leaning different pattern and function for detecting phishing websites. Many researches are done and various phishing detecting systems and tools are developed using different machine learning algorithms. taking inspiration from the vigorous approach and evolving nature of these phishing pages, in this paper, a novel approach is introduced using Random forest and dueling network of reinforcement learning model, where machine learns from training dataset and show improvement in accuracy results. The model in this research shows the capabilities of learning and adapting the unstable dynamic nature of the phishing websites and hence adopt the detected features related to the phishing website. The model also improves itself by learning from different data input. Dueling network is used in this research, where 2 Q-learning models are used to increase its efficiency and accuracy. The model also works on rewards-based system, where the model is awarded with the reward of 10 credits, if it performs well in detection, which thrives it to improve more. The proposed work showed high accuracy rate of 96%, and has further scope of increasing its accuracy with increase in model training.

Keywords: Reinforcement, heuristic, phisher, Random forest, dueling

1. INTRODUCTION

Phishing is the malicious actions taken by phisher on the internet to steal user confidential data. It is considered a very serious problem as phisher can badly harm the target by misusing stolen information like bank details, credit card number, social security number etc. To carry out these actions the phisher first creates a fake website that look identical to the actual target website, then they use bulk emails and text messages for broadcasting the fake URL (URL created are also very similar to the actual URL). Users who are unaware clicks the URL, which directs them to the malicious website. where, considering it a legitimate webpage, user input his personal information. The attacker on the other end captures the user input details and use them for his personal gain.

Now days, there are various methods and tools which are developed to detect phishing websites, these methods are mainly categories as heuristic-based or list based. List based techniques uses the prepared list (blacklist and whitelist) of phishing websites and non-phishing websites to identify the phishing page. Heuristic-based mechanisms uses different criteria to check if the webpage is phishing or not. Machine learning which is a part of AI is the most preferred in Heuristic-based phishing detection system. Tools and applications of different type of machine learning algorithms are used for problem classification and specially of malware and security detection, which have got a spotlight with huge increasing interest from researchers. As the computational power is growing and getting advanced, reinforcement learning which is a subset of machine learning have shown a great advancement in self-learning, pattern recognition and AI. Due to this, most of the decisions, classification and problems related to automations are now handled by these sophisticated statistical models and learning algorithms. These approaches are highly effective when the features which are used for computation are big. In today's time, when everything is getting advanced where machines are evolving itself. It will not be wrong saying, phishing attacks are also getting advanced, and it can easily be predicted, that, in future detecting phishing attack will become a challenge, unless an advanced phishing detection system is created which is good enough to learn and enhance itself with time.

This study presents random forest adding with dueling network where two Q-learning models of reinforcement learning are used for detecting phishing websites on the dataset. since the model is based on reinforcement learning it is self-adaptive. In this model, we have created two Q-learning models, where both the models work separately and give 2 different outputs, mean of both the output is calculated and used as final accuracy result. Few main steps used in this paper are as below:

1) Build model which identifies phishing using reinforcement learning, where the model learns function value from the given dataset for classification task.
2) A processes of decision making is mapped in a sequential manner for classification using dueling network model, implementing reinforcement learning.
3) Evaluating performance from both the Q-learning models. Calculating performance mean of both the Q-learning network and give rewards based on its performance to increase accuracy result.

The proposed noel approach is self-adaptive and robust as algorithm used in reinforcement learning can propose a solution (action) depending on training dataset, reward function and state conversations for deciding an action. This paper basically focusses on improving accuracy rate of detecting phishing sites using a self-evolving model of machine learning. dueling network with two Q-learning models is used where the model enhance itself from data fed and rewards earned, which helps the model in continuous improvement of its accuracy. The dataset being used in this is from kaggle.com and data.mendeley.com which are considered the most reliable phishing community-based verification system (descriptive information in section 5). Research question for this research work is "how to enhance phishing detection system with self-learning for enhancing its accuracy". many different machine learning models and algorithms are studied and researched in the literature review to understand the existing techniques with the chosen model, considering the problem complexity.

2. LITERATURE REVIEW

This section critically analyses the various past researches and studies, conducted using different techniques to enhance phishing detection system, and makes a comparative study of previously used techniques like CANTINA, mining based approach, blacklisting approach, Conventional machine-learning-based detection, CANTINA+ etc. It is categorized into: Established related work for phishing detection and the use of reinforcement learning of ML increase accuracy rate.

2.1. RELATED WORK

Detecting phishing attacks and preventing them is a huge step towards securing the internet and cyberworld. in most cases phishing attacks happen because of user ignorance or inability to identify the malicious pages. in today's advancement, machine learning open various ways of preventing users from getting phished. the better is the detection model, the better will be the protection. So now, focus is more on improving accuracy rate and self-learning models. There are numerous works related to phishing detection done previously, some relatable are mentioned below:

A technique introduced by Zhang et al. [1] where the phishing detection is done on content-based websites known as CANTINA. He proposed a method where each web page term is scored with tf-idf, and a lexical signature is created based on best five tf-tdf score which are used for further checking and classification. Generated signatures are given a search on some famous search engines like bing.com or google to search additional data. if the search engine result matches the same domain name than it is considered as legitimate website else it is marked as phishing page.

one more similar technique is proposed by Xiang et al. [2] known as CATINA+ which has fourteen features divided into different categories like HTML features, high level page feature, web-based feature. where they have used 6 different ML algorithms on a dataset and confirmed that the Bayesian network is the leading technique then others. But the disadvantage of this approach is that, that it is not resilient to famous XXS cyber-attack.

Famous data mining-based approach [7] which is used for classification of phishing URL. Algorithm used in this approach is MCAC i.e. multi-label Classifier based Associative classification, which works in 3 different stages. First is Rules discovery, in which algorithm recapitulate on training dataset and highlights the salient distinct features. Second is building classifier, in which all the rules are classified asper length, level of confidence and support for mentioning the classification directive. And the third is class assignment, where the page URLs are defined in an order with high confidence and support. In this, the researcher pulled 16 features from the test URL and check the mentioned algorithm on 1350 webpages with 601 actual sites and 754 fake sites.

Sahingoz et al [5] worked on phishing detection system by using seven ML classification algorithms. because of unavailability of large public dataset on phishing URLs, a balanced data set is created having phishing and malicious URLs. the main aim of their work is to identify the useful features from the URL. In data pre-processing phase hybrid-based features, word based, and NLP based features are extracted, and their classifier depicted 97.2% accuracy with NLP-based features.[6]

Conventional machine learning detection is a part of heuristic approach which faces many problems as it does not give enough flexibility to adapt changes made on phishing sites. Bypass could easily be done by making minor changes. so, machine learning technique are added later to increase its flexibility and ability to adopt changes. Dataset in this technique plays a major role in training the model, it also represents the feature value derived from this approach. The algorithm uses random forest, Principal component analysis random forest, vector machine decision tree etc. which are even capable of detecting phishing zero day attacks when are trained with these model features.[3] A survey is done to find the achievable accuracy rate of phishing site detection and found that 99% phishing detection can be achieved using machine learning algorithm, though the accuracy rate and the performance of the ML algorithm depends on the training data size, parameter values and extracted features quality to achieve the optimum accuracy.[4] Based on studies available online it is quite clear that use of machine learning for phishing detection is very trending topic which is highly supported by the community of cyber security and researchers. This research shows how adoptive and self-independent our system could be, where reinforcement learning helps the model to learn the task variables and enhance itself to improve future results. Random forest adding with dueling network is a novel idea which is never researched before on machine learning for phishing detection, in which we split our data into 3:7 ratio for training and testing purpose. We prepared two Q learning networks which run parallelly for phishing detection and give two separate results (output). It also adds reward function in which each Q network is awarded with 10 rewards points if their detection accuracy rate is more than 95%. Earning a reward by a Q network also helps the model to understand that the step taken is correct and can be taken again in future. No reward earned means that step taken is incorrect and should be avoided in future, which ultimately enhance the accuracy rate of detection.

2.2. REINFORCEMENT LEARNING: BACKGROUND

This section gives an overview on technical details and practical use of reinforcement learning of ML. This technique is widely used in many different domains [8] [9]

2.3. RL- PARADIGM

Reinforcement learning model is used to achieve optimal behavior proficiency. This paradigm is known as an 'agent' problem, to take steps based on 'trial & error' in a form of communication with 'environment' which is unknown and gives feedback through 'rewards'. The simple form of RL model consists of: Agent, Action, state, policy, Reward, Discount factor, probability of state transition, Episodes which are briefly explained below:

Agent:

- The model state (S_t) is learned by the agent trough input reading (X_t) where (t) shows transition of state at (t) time. In this research model, the input of an agent is the feature vector of a dataset. The interaction between the agent and the framework is established by the activities (U_t) which gives $R_{(t+1)}$ Reward, which aims to improve or enhance the policy π. Once the given reward is accepted then the Q-table (quality table) is updated. It is a table that is used as a reference table which stores the state q-value and action pairs. It is formatted to all 0 and post every learning process episode which is updated, making the agent understand the state best preferred action.

Action:

- In Action, it influences and reflect the updates made in an environment. the activity frequency changes which is based on no. of Q network layer, dataset used or feature vectors.

State:

- At every time step (t) the agent interacts with the environment which affect and change the action performed through the agent. The state in this model is determined through the input vector (x_t) [10]

Policy:

- The policy (π) depict the connection between optimum action and the state of environment which is actioned for that state. policy plays a critical role for the agent in reinforcement algorithm. as it is responsible for making the optimum decision.

Reward:

- It defines the current feedback received from the environment for agent. so that it can define the optimum action for that specific state.

Probability of state transition:

- It defines the probability of changing of one state to another (S_{t+1}).

Episodes:

- It defines the total no. of rounds required by an agent to select the best suited Q-value for action pairs, states.

2.4. CLASSIFIER

A classifier is termed as an algorithm which helps in sorting of data in labeled classes or different categories of information. The simplest example to understand classifier is an example of spam mail. spam mail detection added on a mailbox by a mail service provider is said to be a classification problem, though it is just a binary classification as it uses only 2 classes, mail or spam mail. Training data is basically used by classifier to sort the input variables to their class, in this example mail and spam mail will be used as a training data. [11]

Dueling network is trained so that it works as an agent 'A' of reinforcement learning which creates an interacting bridge with the environment, get the sample 's' for training and give the probability as per the policy 'π’. Which is shown as: $\pi(a|s) = Pr(at = a|st = s)$

The main aim of the agent here is to predict class labels by exploring and identifying the training samples. so that it can receive maximum rewards as: $Rc = \sum_{k=1}^{\infty} \gamma^{k}.r_{t+k}$

Where the reward received is 'r' and the total number of episodes is 'k'. state action combination is given a Q-value [s, a] and is known as Q-function, which can be used by adding expected 'E' rewards for the policy'π' followed. $Q^{\pi}(s, a) = E\pi[Rc|(st = s, at = a)]$

The agent in reinforcement learning can optimize the cumulative rewards "Rc" by resolving it to the closest possible Q function by applying greedy π (policy). In this policy it selects random action in a certain manner from the present action pool. this policy is basically applied so that it makes the agent optimal by learning, and gain rewards from the policy 'π' based environment and makes the Q* as the best used classifier model.

As per the policy the Q-function gives value for predicting label or performing action for that specific data vector. This quality-value is the maximum achievable Rc. Storing of Q-function is preferably done in a table because of limited actions and stringent state space for speculating the label of the class. whereas, Gradient decent π is used which works best for dueling network, which helps in optimizing the classification learning. It is implemented, so that Q-value can be approximated which is known as Q Network.[12] it uses its experience or stored event for learning. the stored value it uses is the information about rewards, state, or action for Q-learning. for storing the information 's' experience memory 'm' is used, this memory provides 'Bm' mini-batch to carry-out gradient decent according to L(θ) i.e. loss function. $L(\theta) = \sum_{(S_1, a_t, r_t, s_{t+1}) \in Bm} (y - Q(s, a, \theta_k))^2$

2.5. LEARNING MODEL

This part of the paper highlights the principles of the proposed algorithm for phishing detection using reinforcement learning model.

2.5.1. PROBLEM STATEMENT

problem statement for phishing detection can be formulated as problem related to classification of phishing websites where the classes are predicted as "phishing" or "no phishing". here, we assume the training dataset as D URL where the data along with class label are as follows:
$(\upsilon_1, x_1), (\upsilon_2, x_2), (\upsilon_3, x_2) .... (\upsilon_D, x_D)$
whereas:
υ_i for i =1,2,3...D which shows the URL in the provided training dataset D and
$x_i \in \{1, -1\}$ for i=1,2,3....D is aligned with the URL where x_i = -1 means phishing and x_i= 1 means no phishing.

- we have used Feature extraction method to classify the phishing website:

2.5.2. FEATURE EXTRACTION

To identify the phishing website from the legitimate website we check characteristics in the website, instance for such characteristics are URL length, IP address, domain registration length, such characteristics helps in identifying the phished pages from the legitimate pages. a similar type of process is used in a research [13] where researcher categorized the website label in four different features. first is based on address bar, second is based on Anomaly, third is domain based and fourth is based on Java script and HTML. we did a similar work and created a list of features which will help in identifying the phished page. some of them are mentioned and explained below:

HTTPS_token

"s" in HTTPS stands for "secure", information that is sensitive or confidential is travelled through HTTPS protocols, and using this protocol clearly give sign of that page being safe. though in this advanced time, attacker have found various ways of faking this secure protocol, so, it is important to check the protocol received from authentic issuer like Verizon that is why it is set to 1 else it would be -1.

having_IPhaving_IP_Address

Having an IP address mentioned in the website URL, gives a clear sign that the website could be phishing, for example having a URL as http://154.32.155.221/setup/processr.php indicates that someone is trying to acquire unwanted access. As we know writing IP address as a host name is no more a standard protocol, hex format in IP address is also used for hiding the actual address. Therefore, value given to this feature is -1 if IP address is mentioned in URL else it is 1.

URLURL_Length

value for long URL is set to 1 as longer URL increases the vulnerabilities, a value of 56 character is set, and it is considered as long URL if it exceed 56 character, else it is a short URL and its value is set to 1

having_At_Symbol

using "@" symbol in URL is also one way which is used by attacker, if we use this symbol in a browser, browser ignores the part which is written prior to this symbol and therefore gives a way to phisher to divert user to a phishing page. so, the feature value for this is set to -1 if it contains symbol

Prefix_Suffix

usually "_" is used as a prefix or suffix in domain name by attacker through which optimizing component of a search engine can be ignored. now search engines like yahoo search is using "_" for separating words. so, we set the value as -1 if it uses "_" else it is 1.

having_Sub_Domain

Attacker usually create a fake domain where he adds the sub domain name of a legitimate website which make it look authentic. so to authenticate it, count of dots are checked in the URL (,.:) which should be below 3. if true then the set value is 1 else value is -1.

URL_of_Anchor

as per the research on "assessment of feature on phishing website" [13] anchors above 20% creates vulnerability and is set to 1 as it gives alert of being a whishing page below 20% is given as -1.

on_mouseover

the attacker replaces the legitimate URL with the malicious one which is given on the address bar. and this can be detected through hovering mouse curser over it, if the actual URL does not appear on the mouseover then feature is marked to -1 else it is set to 1

Redirect

In phishing attack, phisher generally redirects the user from the legitimate URL to its fake URL, where he can steal the confidential information of the target. therefore, if the count of redirect is more than 1 then it raises an alarm for suspicious behavior.

age_of_domain

since phishing websites are made for short period of time, it is taken that website which are newly created have more chances of being a phish page.[14] WHOIS is for domain name registration for URL which is used to check the domain registration period. so, any domain created with in 1 year is set to value -1 in feature.

Abnormal_URL

we also check domain name existence in WHOIS [14], if the domain name fails to exist then it is marked as -1 in feature and it is flagged as suspicious website

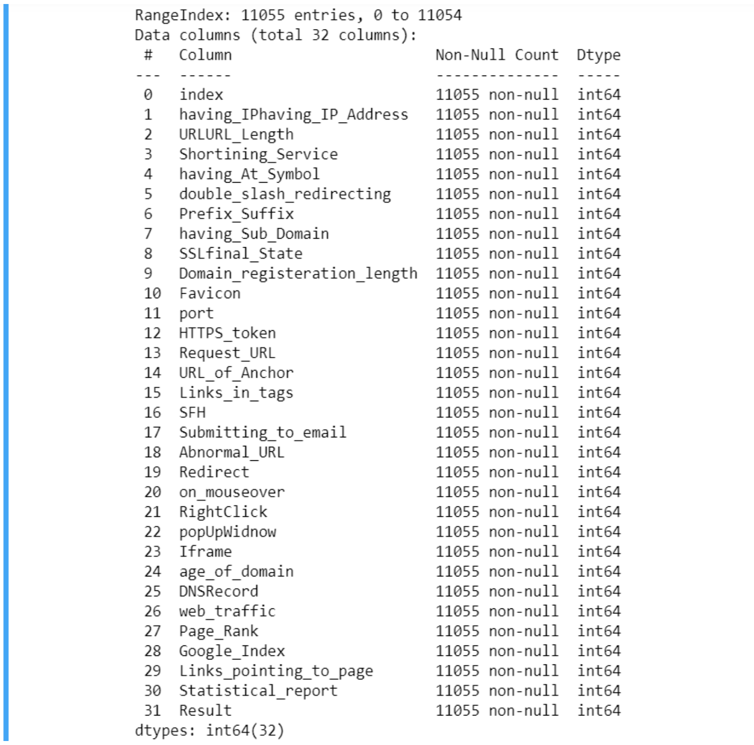
popUpWidnow

Too many popup windows indicate the sign of phishing attack, usually actual sites never request for login details on popups. Therefore, feature is set to -1 if a URL request to open more than 2 popup windows and raise a flag for suspicious behavior.

DNSRecord

DNS recorder basically carries the information of the currently active domain; hence, DNS recorder is not commonly used by attacker in their phishing website. As phishing websites are created for specific purpose and are for short/specific time and generally missing DNSrecorder

Given below in figure 1 is a list of features used for detecting phishing websites in this research.

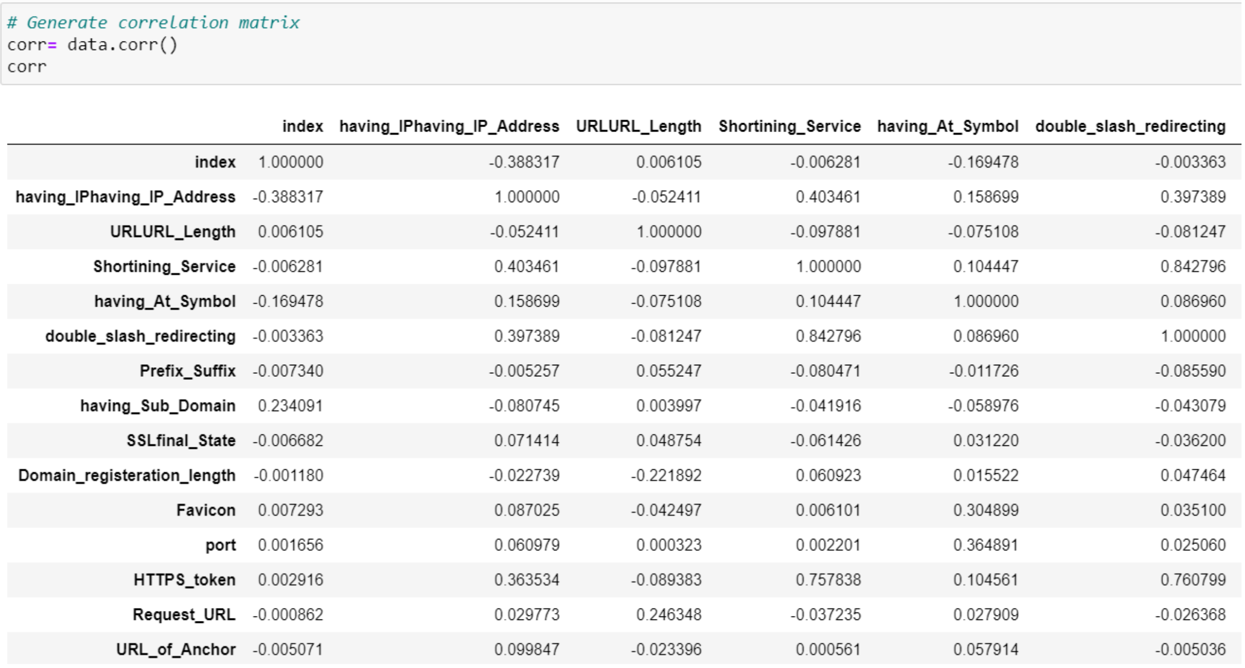


```
RangeIndex: 11055 entries, 0 to 11054
Data columns (total 32 columns):
 #   Column                       Non-Null Count  Dtype
---  ------                       --------------  -----
 0   index                        11055 non-null  int64
 1   having_IPhaving_IP_Address   11055 non-null  int64
 2   URLURL_Length                11055 non-null  int64
 3   Shortining_Service           11055 non-null  int64
 4   having_At_Symbol             11055 non-null  int64
 5   double_slash_redirecting     11055 non-null  int64
 6   Prefix_Suffix                11055 non-null  int64
 7   having_Sub_Domain            11055 non-null  int64
 8   SSLfinal_State               11055 non-null  int64
 9   Domain_registeration_length  11055 non-null  int64
 10  Favicon                      11055 non-null  int64
 11  port                         11055 non-null  int64
 12  HTTPS_token                  11055 non-null  int64
 13  Request_URL                  11055 non-null  int64
 14  URL_of_Anchor                11055 non-null  int64
 15  Links_in_tags                11055 non-null  int64
 16  SFH                          11055 non-null  int64
 17  Submitting_to_email          11055 non-null  int64
 18  Abnormal_URL                 11055 non-null  int64
 19  Redirect                     11055 non-null  int64
 20  on_mouseover                 11055 non-null  int64
 21  RightClick                   11055 non-null  int64
 22  popUpWidnow                  11055 non-null  int64
 23  Iframe                       11055 non-null  int64
 24  age_of_domain                11055 non-null  int64
 25  DNSRecord                    11055 non-null  int64
 26  web_traffic                  11055 non-null  int64
 27  Page_Rank                    11055 non-null  int64
 28  Google_Index                 11055 non-null  int64
 29  Links_pointing_to_page       11055 non-null  int64
 30  Statistical_report           11055 non-null  int64
 31  Result                       11055 non-null  int64
dtypes: int64(32)
```

Figure :1

2.6. NORMALIZATION

Features vectors which are used by our actor are normalized as mentioned above in binary of 1 and -1. Also, a correlation matrix is created mentioning the correlation between all the features in a dataset, and a table is created with all the sorted values in descending order. Given below in figure 2 is a screenshot of correlation matrix table created.



```
# Generate correlation matrix
corr= data.corr()
corr
```

	index	having_IPhaving_IP_Address	URLURL_Length	Shortining_Service	having_At_Symbol	double_slash_redirecting
index	1.000000	-0.388317	0.006105	-0.006281	-0.169478	-0.003363
having_IPhaving_IP_Address	-0.388317	1.000000	-0.052411	0.403461	0.158699	0.397389
URLURL_Length	0.006105	-0.052411	1.000000	-0.097881	-0.075108	-0.081247
Shortining_Service	-0.006281	0.403461	-0.097881	1.000000	0.104447	0.842796
having_At_Symbol	-0.169478	0.158699	-0.075108	0.104447	1.000000	0.086960
double_slash_redirecting	-0.003363	0.397389	-0.081247	0.842796	0.086960	1.000000
Prefix_Suffix	-0.007340	-0.005257	0.055247	-0.080471	-0.011726	-0.085590
having_Sub_Domain	0.234091	-0.080745	0.003997	-0.041916	-0.058976	-0.043079
SSLfinal_State	-0.006682	0.071414	0.048754	-0.061426	0.031220	-0.036200
Domain_registeration_length	-0.001180	-0.022739	-0.221892	0.060923	0.015522	0.047464
Favicon	0.007293	0.087025	-0.042497	0.006101	0.304899	0.035100
port	0.001656	0.060979	0.000323	0.002201	0.364891	0.025060
HTTPS_token	0.002916	0.363534	-0.089383	0.757838	0.104561	0.760799
Request_URL	-0.000862	0.029773	0.246348	-0.037235	0.027909	-0.026368
URL_of_Anchor	-0.005071	0.099847	-0.023396	0.000561	0.057914	-0.005036

Figure: 2

2.7. REINFORCEMENT LEARNING BASED CLASSIFICATION

Reinforcement learning is the most used algorithm of machine learning, its robust nature makes it the most preferred amongst others, it creates an interacting bridge between the agent and environment and makes decision on the bases of states obtained. The input dataset representation is accepted by the agent which are pointing to the target classes. Action and state have the dependency on function of reward and not on class. whenever an action is selected by the phishing class agent to increase the reward to its maximum, it would be tried to minimize the rewords by the no phishing class on the other hand. The agent carryout the action when it gets the input URL vector step by step while in training phase and receive rewards. in that case at every cycle the agent trained to earn more rewards. once the cycle is finished, the model can be used to test on unknown new data.

2.8. TRAINING THE NETWORK

The reinforcement model which is proposed here is basically get trained by gathering the uniformities present in the training URL vectors. which helps the agent responsible for learning, achieve maximum rewards. The training data set is fed continuously, which helps the agent to make the required prediction stats. Adding this model in environment helps in discouraging the problems regarding function approximation in binary classification for testing dataset.

In this research we have used dueling network, which helps the agent in learning from the vector space of phishing dataset, to improve the accuracy we run a two-fold cross validation. [15] The structure of dueling network is depicted in the Figure 3[15].

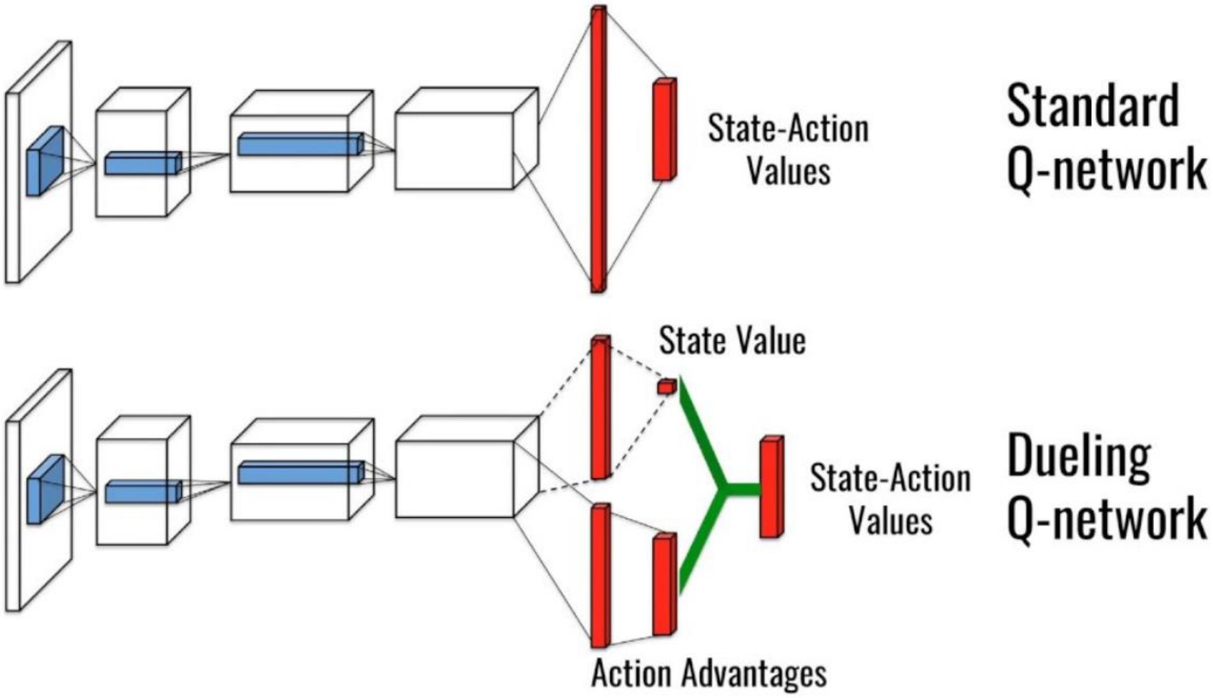


Figure3: Dueling Q-Network Architecture

for selecting an appropriate action, the agent uses a method which is similar to "greedy" for maximizing the earning of rewards within an environment. greedy algorithm uses the probability equation to earn the maximum rewards all together, in current learning phase.

3. METHODOLOGY

We are seeing technology getting advanced, things are getting more user friendly and compact; with that advancement, it is also noticed that, threat associated with it, are also getting advanced with equal pace. Attacks are getting more sophisticated, complex and difficult to detect. Cyber criminals are finding more advanced ways to have an upper hand. A study [16] says, there are approximately 777 phishing pages created every day and approximately 397 potential victims in a day. There are several studies done on phishing website some of them also gave some impressive results, but their workings are limited to some extent. Some of the methods used are : Spoof guard (SG), [17] it uses the scoring technique, where it check 3 tests on all the pages downloaded and sum-up the result by scoring mechanism, then comes the stateless and stateful method which tells if the downloaded pages are suspicious, it compare and evaluate the downloaded page with user previous activities using method that checks the html outgoing data. SG calculates spoof index and give a warning to the user if that is more than the limit selected. SG trigger false alarm when a new account is generated with the same ID and password or in case of redirection. Google and Microsoft integrated [18] the phishing blacklist into web browsers, where browsers raise alarm against the listed URLs. But blacklisting never proved to be a complete solution and is susceptible because of the efforts between anti-phishing org and phishers. phish guard [19], it maintains a whitelist consisting of trusted domains and related IP addresses and checks the similarity between the URL with the whitelist URL. It triggers the alarm if the similarity is more than the threshold. Antiphish [20], it saves mapping of confidential information with the mapping domain corresponding to it, it is never preferable to save confidential information. Antiphish cannot completely save user from phishing attack and storing their confidential information could be vulnerable for user. ItrustPage [21] it creates a repository and checks the URLs from it. but users are vulnerable if the system is hacked, also, it cannot detect phishing site if the site is hosted on an authentic domain. As seen, some of the good methods also have limitations. The biggest problem is phisher can easily bypass the security by making some desired changes in the URL.

So, to overcome this problem, a system is needed which is future read, which can learn and understand the phishing websites and can enhance its accuracy. So, to achieve this, machine learning model is used. Though several machine learning technologies are used by many researchers for phishing detection, but here, I have used dueling network of reinforcement learning model of ML, which makes the system self-independent, self-learning and two Q-network makes the study unique and help in improving the accuracy rate of detection.

The research is carried out following the linear-sequential model which is also called the waterfall model. In this model, we divide our project into different sequential phases, which includes manual coding and frameworks, which helps in smooth project transition considering each phase requirements are achieved. the components included are machine learning, database(dataset), User interface platform, which are used together for successful results. Figure4 depicting waterfall model.

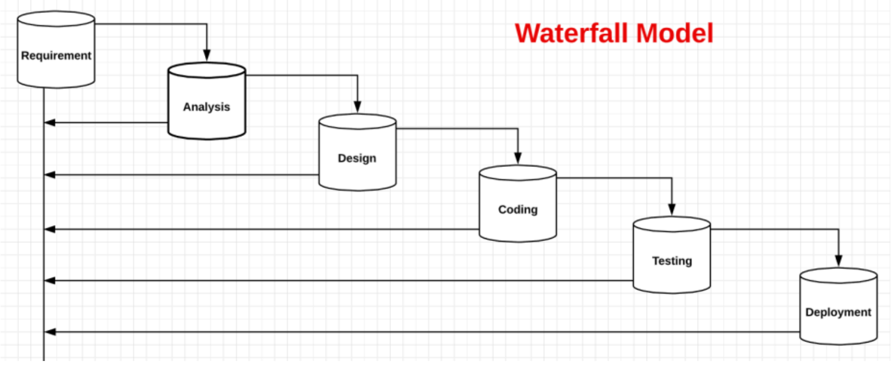


Figure4: Waterfall Model

The data used in this model is split into training and testing (X and Y) , in 3:7 as x_train,x_test, y_train, y_test. Two separate models are created for Q-network random classifier where the number of estimators is set to 10. Since we are using Q learning here, it works on reward basis, so the model is rewarded based on its accuracy.so, if the model accuracy score is above 95%, a reward of 10 is given. Getting a reword on any result will tell that the model that the step taken is preferred in future, and it will avoid the steps where the reward is not received. So, this will help the model in improving its learning, and increase its accuracy.

4. DESIGN SPECIFICATION

This prototype is built on the concept of reinforcement learning of machine learning concept, which has multiple features, it has data collection and data analysis feature, where the data is received, analyzed and sorted. Sorted data is also shown in histogram for better understanding. Next feature is “feature extraction”, where co-relation matrix is generated which shows the correlation between the data and the results are also shown on a heat map for clearer view of co-related data. Then the data features that are not required, (features scored between +/- 0.03 in co-relation matrix) are removed.

Next feature is Dueling Q network where variables are set which are used for training; then comes Training model feature, where model is trained by feeding data and Using reward function. In reward function, if the result accuracy score is more than 95% then the reward of 10 will be given to the model, which implies that the same step can be preferred again, but, if the accuracy score is less than 95%, then no reward is given, and the model will avoid taking the same step in future. Another feature is, use of “two Q networks”. Dual Q network help in refining the accuracy of the result. Both the network works separately and give 2 separate results. Result of both the networks are used to calculate mean, which is the final result. The system process and architecture are shown in below flow chart(figure5):

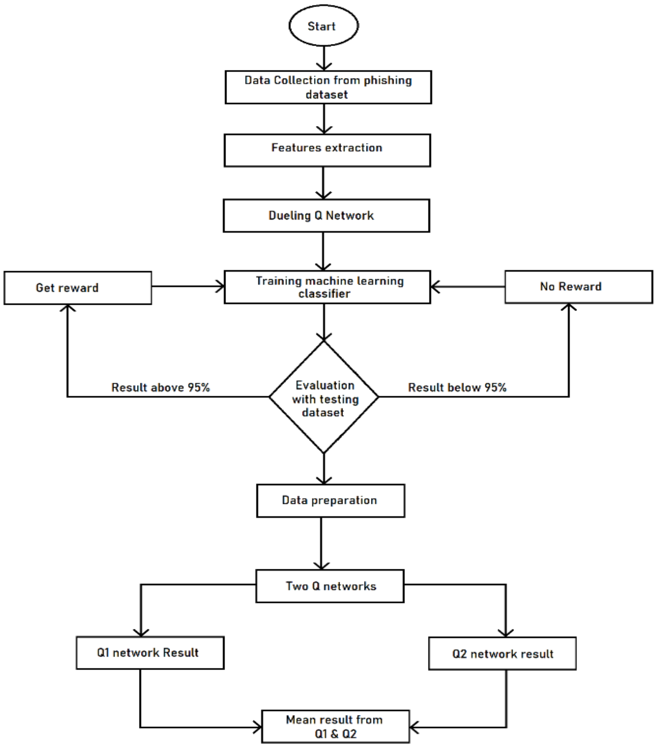


Figure5: Architecture flow diagram

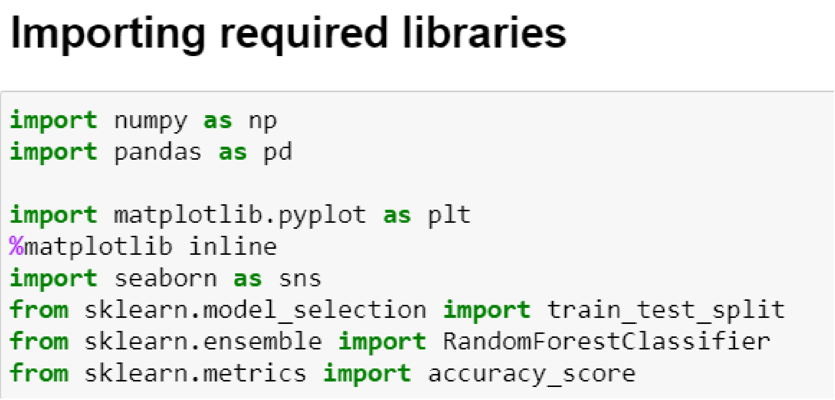
So, the proposed model is generalized to learn the uniformities of the training data. The accuracy and performance speed of this model depends on the quality and quantity of the training data. Better the training is, better would be the accuracy result.

5. IMPLEMENTATION

This part of the research talks about the implementation of the proposed solution.
We have used a language which fits best for machine learning i.e python. We have selected python 3.8 because of its dynamic nature, flexibility, consistency and it gives best Artificial intelligence and machine learning libraries and frameworks which are platform independent.

5.1. IMPORTING LIBRARIES

Python libraries are basically set of reusable code, or a collection of methods or functions that ease in performing an action, with the help of libraries, now writing a complete code is not required to perform a function. For this project we have imported certain libraries which are: numpy for mathematical calculations, pandas for data manipulation, matplotlib.pyplot for graphs, seaborn is also for graphs, randonforest classifier, train_test_split library, accuracy_score . also shown in the below figure6:



Importing required libraries

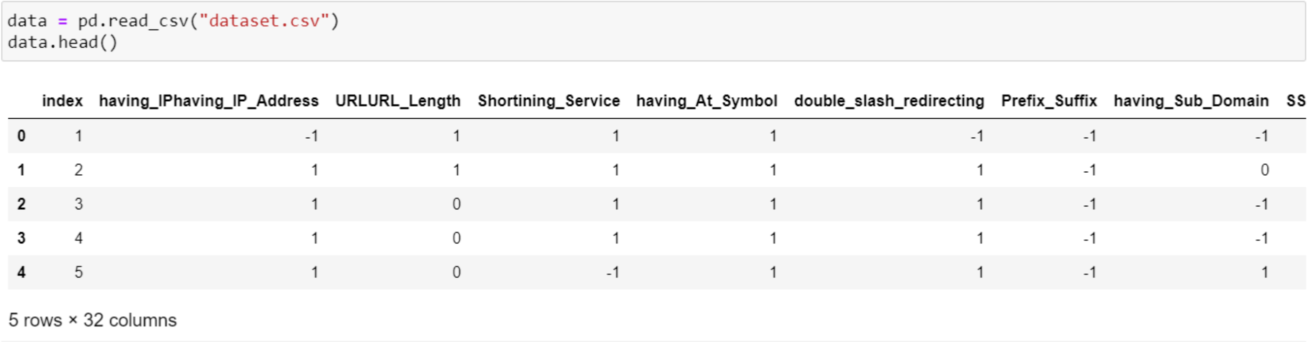
```
import numpy as np
import pandas as pd

import matplotlib.pyplot as plt
%matplotlib inline
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score
```

Figure6: Libraries

5.2. DATASET

For training and testing purpose, we have used a balanced dataset from Kaggle.com and data.mendeley.com which are the most reliable phishing community-based verification system.
First, we will import the dataset; and then check if the data is balanced or not. As for the dataset used, non-phished data is 6157, and phished data is 4898 which depict balanced data. Below figure7 shows importing .csv file and the function fields in dataset and figure 8 shows data being balanced.

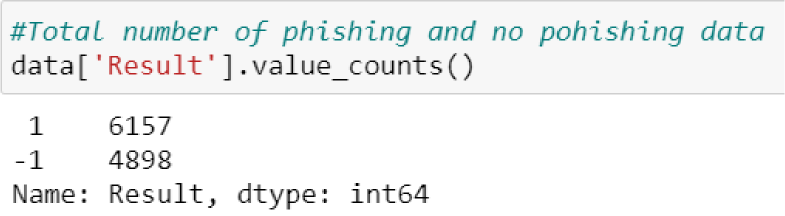


```
data = pd.read_csv("dataset.csv")
data.head()
```

	index	having_IPhaving_IP_Address	URLURL_Length	Shortining_Service	having_At_Symbol	double_slash_redirecting	Prefix_Suffix	having_Sub_Domain	SS
0	1	-1	1	1	1	-1	-1	-1	
1	2	1	1	1	1	1	-1	0	
2	3	1	0	1	1	1	-1	-1	
3	4	1	0	1	1	1	-1	-1	
4	5	1	0	-1	1	1	-1	1	

5 rows × 32 columns

Figure 7: Importing dataset & Function fields



```
#Total number of phishing and no pohishing data
data['Result'].value_counts()
```

```
 1    6157
-1    4898
Name: Result, dtype: int64
```

Figure 8: Checking Data If Balanced

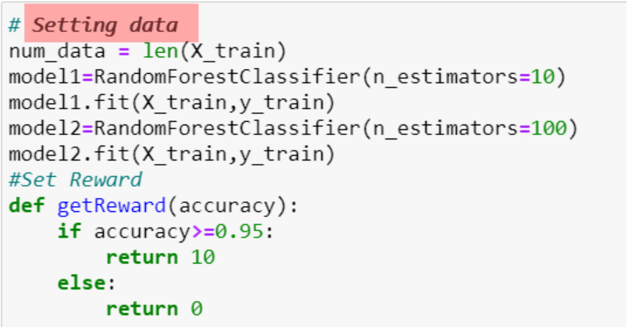
5.3. MACHINE LEARNING

machine learning is now widely used by experts for detecting phishing websites; phishing detection is considered as a simple ml classification problem. so, to build a learning-based phishing detection system, training data with maximum relevant features of phishing and classes of actual websites should be used, implementing learning algorithm, can make the detection of classified or non-classified phishing pages easy. Deciding the ML algorithm is one of the crucial parts of the project success. In this project I am using random forest classifier with dueling network of reinforcement learning.

Random forest: Random forest is introduced by Breiman [22] which provides an extra randomizing layer. The classic way where each tree is built by utilizing the bootstrap data separately; random forest changes, how the classification trees are made. In a classic way, trees are divided using split which is the best among the present variables. while in random forest, every node is divided with the best among the further split subset of predictors which are randomly selected at the node. Random forest is preferred as it is user friendly, has only 2 parameters, and it is also not much sensitive with their values.

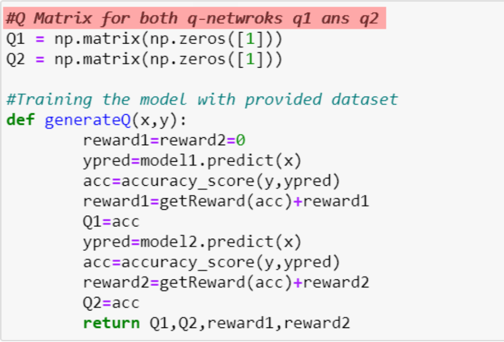
Dueling network: The architecture [23] of dueling network basically have 2 streams functions which are: Advantage and value and have a same convolution feature. There is a special layer of aggregation where the split streams are joined and calculate the estimation of the state action value. The architecture of dueling network can learn about the states, as which states are valuable and which are not, and it does not require to learn the effect of action on every state.
In our dueling network system, we divide the data into 3:7 ratio for training and testing. Then data is set for training and Q matrix for both the q network is set. As shown in figure below 9 and 10.

Training the model



```
# Setting data
num_data = len(X_train)
model1=RandomForestClassifier(n_estimators=10)
model1.fit(X_train,y_train)
model2=RandomForestClassifier(n_estimators=100)
model2.fit(X_train,y_train)
#Set Reward
def getReward(accuracy):
    if accuracy>=0.95:
        return 10
    else:
        return 0
```

Figure 9



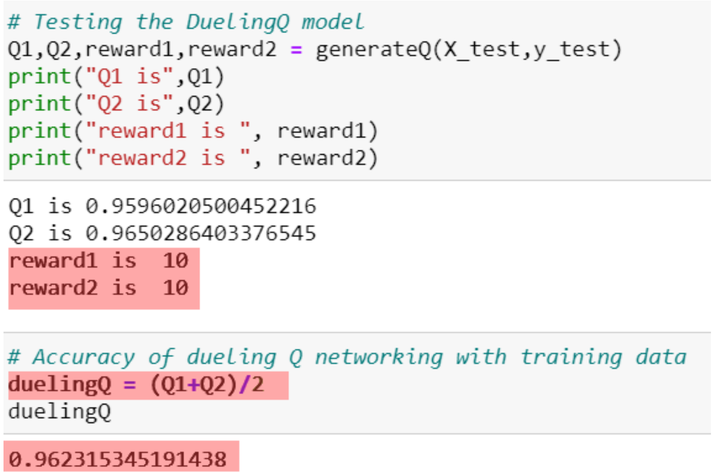
```
#Q Matrix for both q-netwroks q1 ans q2
Q1 = np.matrix(np.zeros([1]))
Q2 = np.matrix(np.zeros([1]))

#Training the model with provided dataset
def generateQ(x,y):
        reward1=reward2=0
        ypred=model1.predict(x)
        acc=accuracy_score(y,ypred)
        reward1=getReward(acc)+reward1
        Q1=acc
        ypred=model2.predict(x)
        acc=accuracy_score(y,ypred)
        reward2=getReward(acc)+reward2
        Q2=acc
        return Q1,Q2,reward1,reward2
```

Figure 10

5.4. REWARD FUNCTION OF Q NETWORK

To improve the accuracy rate of phishing detection, a reward is given to each q network based on their results. If they get the accuracy score of 95% or above, a reward of 10 is awarded. Which, in way helps the learning system to know if the step taken is correct or not and will help the system for further improvement. Then mean of both the output is calculated which is the final detection accuracy rate. As shown in the below figure11.



```
# Testing the DuelingQ model
Q1,Q2,reward1,reward2 = generateQ(X_test,y_test)
print("Q1 is",Q1)
print("Q2 is",Q2)
print("reward1 is ", reward1)
print("reward2 is ", reward2)
```

```
Q1 is 0.9596020500452216
Q2 is 0.9650286403376545
reward1 is  10
reward2 is  10
```

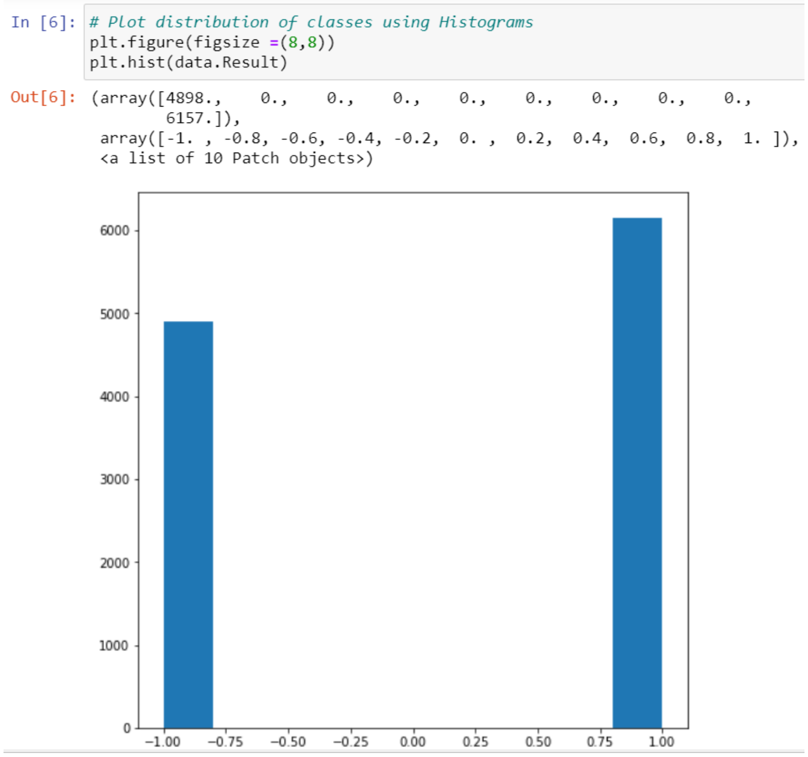
```
# Accuracy of dueling Q networking with training data
duelingQ = (Q1+Q2)/2
duelingQ
```

```
0.962315345191438
```

Figure 11: Output from Q Networks and mean Calculation

6. EVALUATION

Evaluation of the test is based on current dataset which is taken form kaggle.com. Dataset used is balanced as it shows phished sites data as 4898 and non-fished data as 6157. Same is shown in histogram in figure 12, and the data is split into 3:7 for purpose of training and testing.



```
In [6]: # Plot distribution of classes using Histograms
        plt.figure(figsize =(8,8))
        plt.hist(data.Result)

Out[6]: (array([4898.,    0.,    0.,    0.,    0.,    0.,    0.,    0.,    0.,
            6157.]),
         array([-1. , -0.8, -0.6, -0.4, -0.2,  0. ,  0.2,  0.4,  0.6,  0.8,  1. ]),
         <a list of 10 Patch objects>)
```

Figure 12

Evaluation of the proposed model is done by calculating relevance through precision (P), Accuracy(A), recall (R) and F-measure (F). And for this, we need to calculate the predictions - true positive, true negative, false positive, false negative. Results which are correctly classified are true positive and true negative and data which is misclassified are False positive and false negative. the performance is calculated using these values.

P=TP/TP+FP
here if the value of precision is closer to -1 means that the features predicted are close to true

R=TP/TP+FN
In recall, if the value is closer to -1 means testing can be predicted with the same model

A=TP+TN/TP+TN+FP+FN
the performance of the model is said high if the score of accuracy is closer to -1

F=2*P*R/P+R
F score is calculated with mean of recall and precision and shows the resilience of the model

(P)Precision	(R)Recall	(A)Accuracy	(F)F-measure
0.866	0. 89	0.964	0.878

6.1. DISCUSSION

Test was done to find if the aim target for this research is achieved. Aim of this research was to build a phishing detection system, which gives high accuracy rate using a novel method of, implementing dueling network with random forest of reinforcement learning. We have selected Random forest in this research as it showed consistency and high accuracy results. As seen [23] in comparison to other algorithms, random forest has proved to be very precise and much accurate and having dueling network with two q network worked as a complement to it. with the accuracy of 96% and further scope of improving with more quantity and quantity of the training dataset it can be said that the purpose of this research is achieved.

7. CONCLUSION AND FUTURE WORK

This research introduced a novel technique of self-learning phishing detection system using machine learning. This is done using Random forest algorithm and dueling network framework of reinforcement learning. In this research we developed a system which is smart enough to evolve itself with the help of training data it receives. The use of dueling network which is never used before for phishing detection system gave some impressive results, where two Q-networks are made to work separately to get higher accuracy rate. I believe that, this work will help in establishing the base for further studies on phishing detection system, using combinations of different algorithms of machine learning to be more efficient, flexible, self-adaptive and dynamic. Though, this work is not optimal for implementing in real world yet, as data used for phishing detection in real world scenario is huge, so it is more suitable for training or research purposes. To make detection system more refined with higher accuracy, future work for this research can be done by adding neural network with dueling network, that make a combination of most successful 3 Q-learning model, which will enhance the accuracy and increase the detection speed which is also necessary in today's world.

8. ACKNOWLEDGEMENT

I want to take the opportunity to thank my supervisor Ross Spelman for his guidance and support which has greatly helped me in my research and for his assistance which kept me focused on the key areas of my project. I am grateful and appreciative for his mentorship because of which, I am able to successfully complete my project. I would also like to thank Arghir Moldovan and Vikas Sahni for their guidance and immense support during the course.

References

[1] Zhang Y., Hong J.I., Cranor L.F. Cantina: A content-based approach to detecting phishing web sites; Proceedings of the 16th International Conference on World Wide Web; Banff, AB, Canada. 8–12 May 2007; pp. 639–648

[2] G. Xiang, J. Hong, C. Rose and L. Cranor, "CANTINA+", *ACM Transactions on Information and System Security*, vol. 14, no. 2, pp. 1-28, 2011. Available: 10.1145/2019599.2019606.

[3] R. Rao and A. Pais, "Detection of phishing websites using an efficient feature-based machine learning framework", *Neural Computing and Applications*, vol. 31, no. 8, pp. 3851-3873, 2018.
doi: 10.1007/s00521-017-3305-0.

[4] M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey", *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, 2013. doi: 10.1109/surv.2013.032213.00009.

[5] O. Sahingoz, E. Buber, O. Demir and B. Diri, "Machine learning based phishing detection from URLs", *Expert Systems with Applications*, vol. 117, pp. 345-357, 2019. doi: https://www.semanticscholar.org/paper/Machine-learning-based-phishing-detection-from-URLs-Sahingoz-Buber/8dd4a8eefa366b1b7d2471c1b8580df5bea23924.

[6] Liu, W., Huang., G., Xiaoyue, L. Min, Z., and Deng, X., Detection of phishing webpages based on visual similarity. *14th international conference on world wide web* (www) 2005. Doi: http://www.ra.ethz.ch/CDstore/www2005/docs/p1060.pdf.

[7] N. Abdelhamid, A. Ayesh and F. Thabtah, "Phishing detection based Associative Classification data mining", *https://www.sciencedirect.com/*, 2014. [Online]. doi: https://www.sciencedirect.com/science/article/abs/pii/S0957417414001481.

[8] S. Sara Sartoli and A. Namin, "A Semantic Model for Action-based Adaptive Security", *https://www.researchgate.net/publication/316463087_A_Semantic_Model_for_Action-based_Adaptive_Security*, 2017. [Online]. doi: https://www.researchgate.net/profile/Sara_Sartoli/publication/316463087_A_Semantic_Model_for_Action-based_Adaptive_Security/links/5b3162d64585150d23d445c0/A-Semantic-Model-for-Action-based-Adaptive-Security.pdf.

[9] N. Tavakoli, D. Dai and Y. Chen, "Client-side straggler-aware I/O scheduler for object-based parallel file systems", *Parallel Computing*, vol. 82, pp. 3-18, 2019. doi: 10.1016/j.parco.2018.07.001.

[10] R. Sutton and A. Barto, "Reinforcement Learning: An Introduction", *Web.stanford.edu*, 2014. [Online]. doi: https://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf.

[11] F. Pereira, T. Mitchell and M. Botvinick, "Machine learning classifiers and fMRI: A tutorial overview", *NeuroImage*, vol. 45, no. 1, pp. S199-S209, 2009. doi: 10.1016/j.neuroimage.2008.11.007.

[12] Y. Wang *et al.*, "Multi-Objective Workflow Scheduling With Deep-Q-Network-Based Multi-Agent Reinforcement Learning," in *IEEE Access*, vol. 7, pp. 39974-39982, 2019, doi: 10.1109/ACCESS.2019.2902846.

[13] Mohammad, Rami, McCluskey, T.L. Thabtah, F Abdeljaber " An Assessment of Features Related to Phishing Websites using an Automated Technique" In: International *Conferece For Internet Technology And Secured Transactions*. ICITST 2012 . IEEE, London, UK, pp. 492-497. ISBN 978-1-4673-5325-0

[14] R. Gautam, "ANALYSIS AND IMPLEMENTATION OF WHOIS DOMAIN LOOKUP", *Ijtrs.com*, 2016. [Online]. Available: https://www.ijtrs.com/uploaded_paper/ANALYSIS%20AND%20IMPLEMENTATION%20OF%20WHOIS%20DOMAIN%20LOOKUP1.pdf.

[15] V. Mnih et al., "Human-level control through deep reinforcement learning", *Nature*, vol. 518, no. 7540, pp. 529-533, 2015. doi: 10.1038/nature14236.

[16] S. Garera, N. Provos, M. Chew and A. Rubin, "A framework for detection and measurement of phishing attacks", *Proceedings of the 2007 ACM workshop on Recurring malcode - WORM '07*, pp. 1-8, 2007. doi: 10.1145/1314389.1314391.

[17] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C.Mitchell, ―Client-side defense against web-based identity theft‖, 11th Annual Network and Distributed System Security Symposium, ACM Press, Ontario, Canada, 2004, Vol. 380.

[18] L. Sean M. Allister, E. Kirda, C. Kruegel , ―On the Effectiveness of Techniques to Detect Phishing Sites ‖, Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, ACM Press, Switzerland, 2007, Vol. 4579, pp. 20-39

[19] J. Kang and D. Lee, Advanced White List Approach for Preventing Access to phishing Sites International Conference on Convergence Information Technology, Korea, 2007.

[20] E. Kirda and C. Kruegel, Protecting Users against Phishing Attacks with AntiPhish, 29th Annual International Computer Software and Applications Conference, ACM Press, Washington, USA, 2005, Vol. 01, pp. 517-524.

[21] T. Ronda, S. Saroiu and A. Wolman, "Itrustpage", *ACM SIGOPS Operating Systems Review*, vol. 42, no. 4, pp. 261-272, 2008. doi: 10.1145/1357010.1352620.

[22] L. Breiman, "Random Forests", *Machine Learning*, vol. 45, no. 1, pp. 5-32, 2001. doi: 10.1023/a:1010933404324.

[23] Z. Wang, T. Schaul and M. Hessel, "Dueling Network Architectures for Deep Reinforcement Learning", *Proceedings.mlr.press*, vol.48, 2016 doi: http://proceedings.mlr.press/v48/wangf16.pdf.

[24] I. Tyagi, J. Shad, S. Sharma, S. Gaur, and G. Kaur, \A novel machine learning approach to detect phishing websites," in 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, 2018, pp. 425{430.