International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Phishing Website Detection System Using Machine Learning

Manish Jain[1], Kanishk Rattan[2], Divya Sharma[3], Kriti Goel[4], Nidhi Gupta[5]

[1-4]Student, Dept. of Information Technology, Inderprastha Engineering College, Uttar Pradesh, India
[5]Professor, Dept. of Information Technology, Inderprastha Engineering College, Uttar Pradesh, India

---

Abstract - *Phishing is regularly an ordinary assault on persons via making them reveal their total one-of-a-kind info the use of counterfeit web sites. The purpose of phishing records process tool URLs is to pinch the personal information like consumer name, passwords and online banking transactions. Phishers(attackers) uses the websites that rectangular diploma visually and semantically the photo of these actual websites. As the era continues to grow, phishing techniques started to progress quickly and this may be prevented by way of exercise anti-phishing mechanisms to find phishing. Machine planning to apprehend can be a powerful device that is regularly used in the direction of phishing attacks. This paper surveys the capabilities used for the detection and detection techniques by the use of Machine learning.*

Key Words: *Phishing, Phishing Websites, Detection, Machine Learning, Information.*

1. INTRODUCTION

Phishing imitates the characteristics and alternatives of emails and makes it appear similar due to the fact the original one. It seems nearly like that of the legitimate supply. The consumer thinks that this e-mail has come back from a real employer or a corporation. This makes the consumer to forcefully visit the phishing internet site thru the hyperlinks given inside the phishing email. These phishing web sites region unit created to mock the seams of an ingenious website. The phishers force person to inventory up the non-public info via giving baleful messages or validate account messages etc. so that they inventory up the preferred data which might be utilized by them to misuse it. They devise things such as the user isn't always left with the other choice but to go to their spoofed web site. Phishing is the most hazardous criminal physical activities in the cyber region. Since the maximum of the customers logs on to get admission to the services supplied with the aid of government and financial establishments, there has been a significant boom in phishing attacks for the beyond few years. Phishers commenced to earn cash and that they try this as a thriving business.

Phishing may be law-breaking, the explanation behind the phishers doing this crime is that it is terribly trustworthy to try to do this, it doesn't value something and it effective. The phishing will truly get entry to the e-mail identity of somebody it's terribly sincere to are looking for out the e-mail identification currently every day and you will send an email to every person is freely offered throughout the globe. These attacker's vicinity terribly much less price and electricity to urge valuable know-how quick and truly. The phishing frauds effects malware infections, statistics loss, fraud, etc. information at some stage in which those cyber criminals have an interest is that the crucial data of a user similar to the password, OTP, credit/ debit card numbers CVV, sensitive know-how associated with business, medical understanding, confidential information, etc commonly these criminals conjointly acquire data which may provide them directly get admission to do the social media account their emails.[4]

A lot of software /ways and algorithms area unit used for phishing detection. These area unit used at academic and industrial organization levels. A phishing address and also the parallel online page have several capabilities which could be one-of-a-kind from the address that allows us to take associate degree instance to cover the initial domain decision the phishing assaulter will sense terribly protracted and confusing name of the domain. This is often terribly effortlessly visible.

Typically, they use the data science address within the website of victimization the domain call. On the opposite hand, they will conjointly use a shorter domain decision if you wish to not be applicable to the distinctive legitimate web site. except the address based mostly operate of phishing detection their area unit several exclusive functions which might even be used for the detection of Phishing websites referred to as the Domain-based mostly options, Page based Features and Content-Based features.
Various techniques are employed by means of phishers to attack vulnerable customers like digital communication, VOIP, spoofed link, and counterfeit web sites. it's terribly sincere to make counterfeit websites, that experience like a real net web page in terms of layout, content. Even, the content of those web sites might be the image in their legitimate websites. The reason behind making these web sites is to induce non-public understanding from customers like account numbers, login id, passwords of debit and MasterCard, etc.

According to the APWG 2Q report, the entire range of phish detected in 2Q 2018 become 233,040, in comparison to 263,538 in 1Q 2018. These totals exceed the 180,577 located in 4Q 2017 and the 190,942 visible 3Q 2017. There were increases in the SAAS/webmail centered sector with

21% of common phishing attacks. The payment region is persevering with as most appealing goal for a phishing attack. According to APWG 1Q report, the full number of phish detected in 1Q2018 was 263 This turned into up 46 percentage from the 180,577 located in 4Q 2017. It became also drastically extra than 190,942 seen in 3Q 2017.The range of unique phishing reports submitted to APWG at some stage in 1Q 2018 become 262,704, in comparison to 233,613 in 4Q 2017 and 296,208 in 3Q 2017.

2. RELATED WORK

Researchers have conducted lot of work in security [10-13], including secure routinG, intrusion detection, intrusion prevention, and smart grids security. Web phishing is the attempt to gather personal information such as usernames, passwords, and credit card details, often for malicious purposes, by masquerading as a trustworthy website on the network.

Researchers present a few answers to detect web phishing attacks as follows:

When we decide whether a particular internet site is internet phishing, the direct manner is to use a whitelisting or blacklist. We may additionally seek the URL in a few databases and then decide. Pawan Prakash el. offered two approaches to detect phishing web sites by way of the blacklist.

Another phishing detection manner is to examine the features of the URL. For example, occasionally a URL looks much like the well-known net page URL or contains some special characters inside the URL. Samuel Marchal et al. Used one concept of intra- URL relatedness and calculated it using capabilities taken from phrases that compose a URL primarily based on query records from Google and Yahoo search engines. These functions are then used in gadget mastering based type to come across the phishing URLs from a real statistic set. This method is green and economical, thanks to the actual fact it makes use of the pre-existing expertise of the URL, which encompasses a quick detection pace and a lower cost. However, we cannot fully exchange the traits of phishing in phrases of an URL only thanks to the actual fact the essence of the scheme is to fraud by way of internet content. Phishing attackers are very likely at home with URLs and simply adjust their URLs to stay aloof from detection; therefore, this method will bring on a decreased detection rate if simplest the records of the URL are checked.

3. LITERATURE SURVEY

A unique category approach that uses the heuristic-based function extraction technique. In this, the extracted capabilities are categorized into 3 categories consisting of URL Obfuscation capabilities, Third-Party-based features, Hyperlink-based functions. Also, this model is solely betting on the exceptional and quantity of the schooling set and Broken links feature extraction incorporates a drawback of greater execution time for the sites with an additional quantity of links. Chunlin et al. Proposed a technique that in preferred focuses on individual frequency capabilities. In this, they've blended statistical evaluation of URL with a scientific learning approach to introduce the result that's more correct for the sort of malicious URLs.

This research paper [4] provides an approach to detecting phishing email attacks using an analysis of linguistic communication and machine learning. It is accustomed search the text's syntax to detect malicious intent. A natural language processing (NLP) technique is employed in conjunction with a predicate to decode each sentence and identifies the semantic jobs of words within the sentence. Computer supervised learning is employed to come up with the blacklist of malicious pairs.

Also, we've got compared the accuracy of 5 machine learning algorithms Decision Tree (DT), Random Forest (RF) [5], Gradient Boosting (GBM), Generalized Linear Model (GLM) and Generalized Additive Model (GAM).

Accuracy, Precision-Recall assessment methods were calculated for each algorithm and compared. Website attributes are selected with the assist of Python and performance assessment done with open-supply programming language R. Top 3 algorithms particularly, SVM, Random Forest, and Naïve Bayes performance are compared.

They have deliberated a rule-based type method for the detection of phishing websites. They require everywhere that association classification algorithms are better than the other algorithms due to their sincere rule transformation. They accomplished 92.67% accuracies through extracting sixteen options, however, it's not correct that the deliberate algorithmic rule could also be multiplied for reasonably-priced detection rate. Authors [6] planned a version with an approach to spotting phishing websites by utilizing the universal aid locator identification approach mistreatment the Random Forest algorithmic program. The display has 3 stages, especially Parsing, Heuristic Classification of data, Performance Analysis. Parsing is employed to examine the capacity set.
This paper [7] strategize a framework to extract functions flexible and simple with new strategies. Data is accumulated from PhishTank and legitimate URLs from Google.

4. METHODOLOGY

In this section, we tend to study the various classifiers employed in system finding out to predict phishing. We will conjointly provide proof for our projected

methodology to discover phishing internet sites and attacks.

In section 4.1 we shall provide proof for various classifiers and techniques which may be employed to check the phishing and legit web site. In section 4.2 we can justify our projected system.

Further, in section 4.3, we will explain about the feature extraction of the URL. We will utilize the extracted features for training and testing of the data sets.

4.1 Machine learning classifiers and methods to detect the phishing website

Detecting and identifying Phishing Websites is simply a complicated and dynamic task. Machine studying has been extensively utilized in many regions to create solutions. The phishing attacks can be carried out in many methods which include email, website, malware, SMS, etc. In this work, we concentrate on finding out website phishing (URL), which is finished by utilizing the Hybrid Algorithm Approach. Hybrid Algorithms Approach is a mixture of various classifiers algorithms running collectively which gives an amazing prediction rate and improves the accuracy of the system.

Contingent upon the application and furthermore the idea of the dataset utilized we will utilize any grouping calculations referenced. As their square measure completely different applications, we have a tendency to cannot differentiate that of the algorithms square measure superior or not. Every of classifiers has its own manner of operating and classification.

Let us discuss each of them in details. [8]

- **Naive Bayes Classifier:** This classifier can likewise be known as a Generative Learning Model. The characterization here depends on Bayes' Theorem, it expects autonomous indicators. In straightforward words, this classifier will expect that the presence of explicit highlights in a class isn't identified with the presence of some other component. On the off chance that there is any reliance among the highlights of one another or on the closeness of various features, these will be taken into consideration as a self-governing commitment to the likelihood of the yield. This arrangement calculations are a lot of value to huge datasets and are exceptionally simple to utilize.

- **Random Forest**: This classification set of rules is like gathering a learning approach of type. The regression and other tasks, work with the aid of forming a collection of decision bushes at training records level and for the duration of the output of the class, which can be the mode of class or prediction regression for character timber. This classifier accuracy for choice trees practice of overfitting the training facts set.

- **Support vector machine (SVM):** This is likewise one of the classification algorithms which is directed and is anything but difficult to utilize. In this calculation each point which is an information thing is plotted in a dimensional space, this space is additionally called an n-dimensional plane, where the 'n' speaks to the number of highlights of the information.

Once the version is trained it's terribly essential to gauge the classifier that we have a tendency to shall use and validate its capability. currently, within the higher than section, we've visible all the advantages and drawbacks of all the out their classifiers. Hence, we have a tendency to advocate employing a few classifiers that are we have a tendency to area unit ready to use an associate mixture of classifiers to enhance the accuracy equally of prediction. we have a tendency to shall value each of the classifiers and use Naive Bayes and Random forest, by the usage of the mixture explicit during this section we have a tendency to shall improve the accuracy and build it higher. once applying the classification, the outcomes area unit generated and also the URLs area unit categorized into phishing and valid URLs. The Phishing URLs area unit blacklisted within the info and also the valid maybe a white list in database.

4.2 Proposed System

The dataset of phishing and legitimate URLs is provided within the application which is then pre-processed so that the facts are within the working format for analysis. The functions have round 30 traits of phishing websites that have used to distinguish them from legitimate ones. Each category has its very own traits of phishing attributes and values are defined. The specified traits are extracted for every URL and legitimate stages of inputs are identified. These values are then assigned to every phishing internet site risk. The phishing properties esteems are spoken to with double no 0 and 1 which appears the characteristic is present or not.

In the education phase, we have to use the categorized statistics in which there are samples which include phish regions and legitimate areas. In the event that we attempt this, at that point type will never again be a difficulty for recognizing the phishing space. We should always use samples whose instructions are recognized to us, which shows the samples whom we label as phishing ought to be detected simplest as phishing. Similarly, the samples that are categorized as legitimate are detected as a valid URL. The dataset which is for use for machine gaining knowledge of has to truly include these features. There is such a massive quantity of gadget learning algorithms and every set of rules has its own working mechanism which

we've got already seen in the previous chapter. The triumphing system makes use of everybody of the acceptable system getting to know algorithms for the detection of phishing URL and predicts its accuracy. [9]

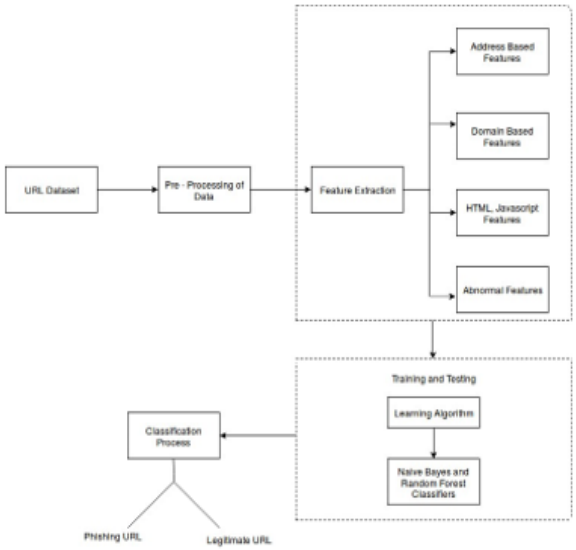


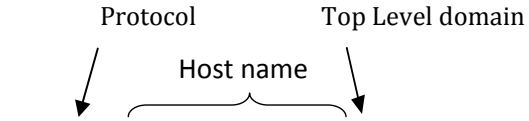
Fig -1: Proposed System block diagram

4.3 Lexical Feature Analysis

Lexical functions are the textual properties of the URL itself, now not the content of the page it factors too. URLs are human-readable textual content strings that can be parsed at some stage in a popular way by customer programs. Through a multistep process, browsers will translate every URL into commands that discover the server web hosting the region and determine in which the location or useful resource is positioned on it. To facilitate this AI process, URLs have the subsequent widespread syntax.

<protocol>://<hostname><path>

An example of URL resolution is shown below:



https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&ltmplcache=2

Path

The <protocol> portion of the URL indicates which network protocol should be accustomed fetch the requested resource. The foremost common protocols in use are Hypertext Transport Protocol or HTTP (http), HTTP with Transport Layer Security (https), and File Transfer Protocol (ftp). The <hostname> is that the identifier for the net server on the web. Sometimes it's a machine-readable Internet Protocol (IP) address, but more often especially from the user's perspective it is a human-readable name. The <path> of a URL is analogous to the trail name of a file on a neighborhood computer. The procedure which is used in our work to separate the lexical highlights from the URL list is as per the following: The URLs of genuine sites, gathered from alexa.com and dmoz.org, are composed into the scratchpad and along these lines, the record is spared inside the PC.

4.4 FEATURE EXTRACTION

4.4.1 LONG URL:

Long URL is used to shroud the Suspicious Part. If the length of the URL is bigger than or comparable to 54 characters then the URL is assigned to be phished.

4.4.2 URL's having "@" Symbol:

Using "@" symbol within the URL leads the browser to ignore everything preceding the "@" symbol thus making it phished. Also, the real address often follows the "@" symbol.

IF {URL Having @ Symbol→ Phishing URL
Otherwise→ Legitimate}.

4.4.3 Redirecting using "//":

The existence of "//" within the URL path implies that the user is going to be redirected to a different website.
An example of such URL's is:

"http://www.legitimate.com//http://www.phishing.com".

We investigate the condition where the "//" appears. We find that if the URL begins with "HTTP", which means the "//" ought to show up inside the 6th position. Regardless, if the URL uses "HTTPS" by then the "//" must show up in the seventh position.

IF {The Position of the Last Occurrence of "//" in the URL > 7→ Phishing URL
Otherwise→ Legitimate}.

4.4.4 Adding Prefix or Suffix Separated by (-) to the Domain:

The dash symbol isn't employed in legitimate URLs. Phishers tend to use prefixes or suffixes separated by (-) to the URL so that the users feel that they are visiting a secure webpage.

For example, http://www.Confirme-paypal.com/.

IF {Domain has (−) Symbol → Phishing URL
Otherwise → Legitimate}.

4.4.5 Sub-Domain and Multi Sub-Domains

The legitimate URL link has two dots within the URL since we will ignore typing "www.". If the number of dots is comparable to three then the website is evaluated as "Suspicious".
However, if the dots are larger than three, then it will be categorized as "Phishy".

Data set: The information of URLs is gotten from the Phishtank site, where Phishtank is an enemy of the phishing site. It contains 2905 URLs which is in an unstructured structure. Our primary target is to identify whether the URL is phishing or authentic dependent on the highlights removed.

	URL
0	https://locking-app-adverds.000webhostapp.com/...
1	http://www.myhealthcarepharmacy.ca/wp-includes...
2	http://code.google.com/p/pylevenshtein/
3	http://linkedin.com/
4	http://imageshack.com/f/219/cadir2yr3.jpg

Fig -2: Unstructured Data

In Preprocessing, we have performed the component extraction where The URLs are transmitted to the element extractor, which concentrates values through the predefined URL-based highlights. The highlights have allocated twofold qualities 0 and 1 which demonstrates that component is available or not as appeared in the figure beneath. A structured dataset is given to the classifiers.

domain_name	address	is_phished	long_url	having_@_symbol	redirection_//_symbol	prefix_suffix_seperation	sub_domains
locking-app-ds.000webhostapp.com	payment-update-0.html?fb_source=bookmark_appsk...	yes	1	0	0	1	0
ealthcarepharmacy.ca	wp-includes/js/jquery/ini.php	yes	2	0	0	0	0
code.google.com	p/pylevenshtein/	no	0	0	0	0	0
linkedin.com		no	0	0	0	0	0
imageshack.com	f/219/cadir2yr3.jpg	no	0	0	0	0	0

Fig -3: Loading the data in our program

Table -1: URL Features

Sr. No	Feature name	Description
1	IP address	Whether Domain is in the form of an IP address
2	Length of URL	Length of URL
3	Suspicious character	Whether URL has _@ ', _//'
4	Prefix and suffix	Whether URL has '-'
5	HTTPS protocol	Whether URL use https.
6	Phishing words in URL	URL has phishing terms
7	Number of '.'	Number of dots '.' in URL

URL Features: Referring to Table 1., features from 1 to 4 are associated with suspicious Characters such as _@ 'and _// 'rarely appear in a URL. At present, to keep a client from distinguishing that a site isn't authentic, phishing destinations ordinarily conceal the essential area; the URLs of these phishing locales have curiously long subdomains.

5. IMPLEMENTATION AND TESTING

This segment gives data about the execution condition and illuminates the real strides for the usage of the dataset to show signs of improvement exactness to anticipate phishing by utilizing various classifiers mixes.

5.1 Hardware requirements

The following hardware was used for the implementation of the system:

- 4 GB RAM
- 10GB HDD
- Intel 1.66 GHz Processor Pentium 4

5.2 Software requirements

The following software was used for the implementation of the system:

- Windows 7
- Python 3.6.0
- Visual Studio Code

5.3 Implementation steps

In this section, we will talk about the means which were actualized while doing the examination. We will provide a piece of evidence for the stepwise method accustomed to split the knowledge and to foresee the phishing. We have utilized unstructured information that comprises just URLs. There are 2905 URLs gotten from the Phishtank site which comprises of both phishing and genuine URL where the majority of the URLs got are phishing.

1. We have collected unstructured data of URLs from Phishtank website.
2. In pre-processing, feature generation is done where nine features are generated from unstructured data. These features are length of an URL, URL has HTTP, URL has suspicious character, prefix/suffix, number of

dots, number of slashes, URL has phishing term, length of subdomain, URL contains IP address.

3. After this, an organized dataset is made in which each detail incorporates the paired (0,1) which is then passed to the various classifiers.
4. Next, we train the three unique classifiers and analyse their presentation based on exactness three classifiers utilized are SVM, Naive Bayes and Random Forest.
5. At that point, the classifier identifies the given URL dependent on the preparation information that is if the site is phishing it prompts the user that the website is phished and if genuine, it prompts the user that the website is legitimate.
6. We look at the exactness of various classifiers and discovered Random Forest as the best classifiers which gives the most extreme precision.

6. RESULTS

We have efficiently calculated the consequences of numerous classifiers which might be SVM, Naïve Bayes, Random Forest.
On comparison of resultant values, we chose to put into effect the Random Forest classifier in our datasets. Steps to obtain the accuracy of various classifiers:

- Initially, we import all the packages which can be implemented in our project.

```
import sklearn
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.naive_bayes import MultinomialNB
from sklearn import svm
import pandas as pd
from sklearn import datasets
```

Fig -4: Importing the required packages

- We will load the data sets for testing and training.

```
df=pd.read_csv("dataset4.csv")
```

Fig -5: Loading the data set

- Now, we will do splitting up of data for training and testing. We will use 20% of data set for testing.

```
#splitting up of data in test and train
X=df[['long_url','having_@_symbol','redirection_//_symbol','prefix_suffix_seperation','sub_domains']]
Y=df['is_phished']

X_train,X_test,Y_train,Y_test=train_test_split(X,Y,test_size=0.2)
```

Fig -6: Splitting up of Data Set for testing and training

- We will calculate the accuracy of Random Forest classifier.

```
########random forest########

clf1=RandomForestClassifier()

clf1.fit(X_train,Y_train)

#print(clf1.predict(X_test))
print("random forest accuracy (aprox)=",clf1.score(X_test,Y_test))
```

Fig -7: Calculation of the accuracy of Random Forest classifier

- We will calculate the accuracy of Naïve Bayes classifier.

```
####naive bayes#################

clf2=MultinomialNB()

clf2.fit(X_train,Y_train)
print("Multinomial naive bayes accuracy (aprox)=",clf2.score(X_test,Y_test))
```

Fig -8: Calculation of the accuracy of Naïve Baye's classifier

- Now, we will compare the results obtained after calculating the accuracy of various classifiers.

```
PS C:\Users\MANISH\Desktop\phishing-URL-detection-master> & c:/Users/MANISH/Desktop/phishing-URL-detection-master/venv/Scripts/python.exe c:/Users/MANISH/Desktop/phishing-URL-detection-master/test_algo.py
svm accuracy(aprox)= 0.6923076923076923
random forest accuracy (aprox)= 0.6923076923076923
Multinomial naive bayes accuracy (aprox)= 0.5384615384615384
```

Fig -9: Comparison of accuracy of various classifiers

- Upon comparison, we found that accuracy of Random Forest Algorithm is highest and is considered best for our data set.

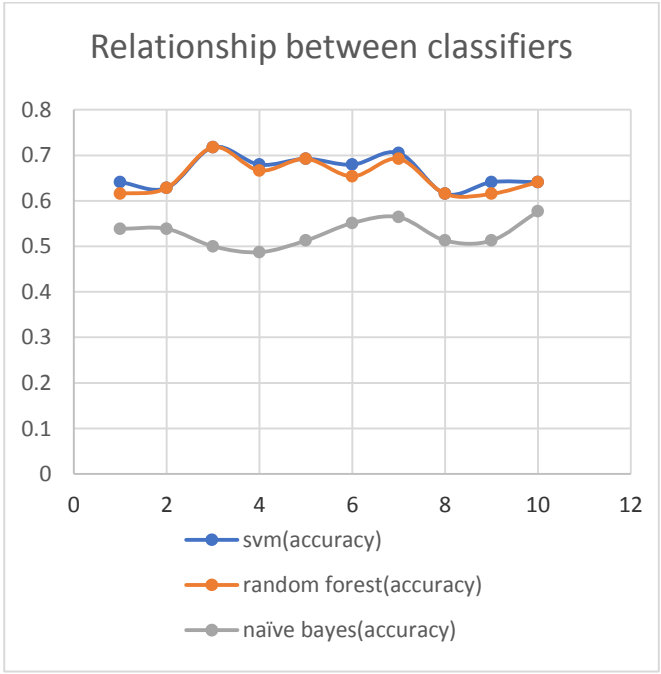


Chart -1: Relationship between the classifiers

7. CONCLUSIONS

It is discovered that phishing assaults are unbelievably essential and it's significant for us to invite an instrument to distinguish it. As fundamental and private data of the client is spilled through phishing sites, it turns out to be progressively basic to require care of this issue. This issue is handily understood by utilizing any of the AI calculations with the classifier. We have just got classifiers that give a decent expectation pace of phishing additionally, yet after our overview that it'll be smarter to utilize a half breed approach for the forecast and further improvement of the exactness expectation pace of phishing sites. We've seen that the current framework gives less precision so we proposed a fresh out of the box new phishing strategy that utilizes URL based highlights and furthermore, we created classifiers through a few AI calculations.

The main findings of our preliminary work include:

- Phishing URLs and domains show some characteristics that are different from other URLs and domains.
- Phishing URLs and domain names have altogether different lengths contrasted with different URLs and domain names inside the Internet.
- A large number of the phishing URLs contained the name of the brand they focused on.

REFERENCES

[1] Web Phishing Detection Using a Deep Learning Framework. Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 4678746, 9 pages.

[2] Phishing Websites Detection Using Machine Learning R. Kiruthiga, D. Akila. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019

[3] Detection of URL based Phishing Attacks using Machine Learning. Published by: International Journal of Engineering Research & Technology (IJERT) http://www.ijert.orgISSN:2278-0181 Vol. 8 Issue 11, November-2019R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] T. Peng, I. Harris, and Y. Sawa, "Detecting Phishing Attacks Using Natural Language Processing and Machine Learning," Proc. - 12th IEEE Int. Conf. Semant. Comput. ICSC 2018, vol. 2018–Janua, pp. 300–301, 2018.

[5] Shad and S. Sharma, "A Novel Machine Learning Approach to Detect Phishing Websites Jaypee Institute of Information Technology," pp. 425–430, 2018.

[6] S. Parekh, D. Parikh, S. Kotak, and P. S. Sankhe, "A New Method for Detection of Phishing Websites: URL Detection," in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, vol. 0, no. Icicct, pp. 949–952.

[7] M. Aydin and N. Baykal, "Feature extraction and classification phishing websites based on URL," 2015 IEEE Conf. Commun. NetworkSecurity, CNS 2015, pp. 769–770, 2015.

[8] Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). An ideal approach for detection and prevention of phishing attacks. Procedia Computer Science, 49, 82-91.

[9] Lakshmi, V. S., & Vijaya, M. S. (2012). Efficient prediction of phishing websites using supervised learning algorithms. Procedia Engineering, 30, 798-805.

[10] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," Journal of Network and Computer Applications, vol. 59, no. 1, pp. 325–332, 2016.

[11] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "A denial of service attack in advanced metering infrastructure network," in Proceedings of the 2014 IEEE International Conference on Communications (IEEE ICC 2014), pp. 1029–1034, IEEE, Sydney, Australia, June 2014.

[12] S. Xiao,W. Gong,D. Towsley,Q. Zhang, andT. Zhu, "Reliability analysis for cryptographic key management," in Proceedings of the IEEE International Conference on Communications (IEEE ICC 2014), Sydney, Austrailia, June 2014.

[13] D. Jiang, Z. Yuan, P. Zhang, L. Miao, and T. Zhu, "A traffic anomaly detection approach in communication networks for applications of multimedia medical devices," Multimedia Tools and Applications, vol. 75, no. 22, pp. 14281–14305, 2016.