Makine Öğrenmesi Yöntemleri İle Oltalama Websitesi Saldırı Tespiti

Attack Detection of Web Phishing With Machine Learning Methods

Şevki Gani ŞANLİÖZ
MSÜ Hezarfen Havacılık ve Uzay Teknolojileri Enstitüsü
Bilgisayar Mühendisliği
İstanbul, Türkiye
ganisanlioz@hotmail.com

Mustafa KARA
MSÜ Hava Harp Okulu
Bilgisayar Mühendisliği
İstanbul, Türkiye
mkara@hho.edu.tr

Muhammed Ali AYDIN
İstanbul Üniversitesi
İstanbul, Türkiye
Bilgisayar Mühendisliği
aydinali@istanbul.edu.tr

Hasan Hüseyin BALIK
MSÜ Hava Harp Okulu
İstanbul, Türkiye
hasanbalik@gmail.com

***Abstract*—Phishing is defined as a fraudulent method by which fraudulent persons send personal information to the victim's e-mail box using known e-mail addresses of known web sites, banks, companies or internet service providers. Although there are many applications to detect phishing attacks today, there are difficulties in preventing attacks. In order to detect Phishing attacks at certain rates, some machine learning methods are discussed. The purpose of this work is to compare machine learning techniques used against web phishing attacks. These methods, including Classification and Regression Trees (CART), J48 (C4.5) Algorithm, Adaboost Algorithm, Random Forest (RF) and Neural Networks (NNet), were used to estimate web phishing attacks. The accuracy rate has been tested. In this study, a total of 1353 emails were used in a phishing attack website, 702 of which were malicious and 548 were legitimate websites and 103 suspicious websites in the data set. In addition, 10 properties were used to train and test the classes. 9 features have been addressed and 1 reference has been used to specify the classification.**

Keywords—Cyber Attack, Web Phishing, Machine Learning

***Özet*—Oltalama (Phishing), bilinen web sitelerinden, bankalardan, büyük çaplı firmalardan veya internet servis sağlayıcıları benzeri kuruluşlardan gönderilmiş gibi gelen mailler aracılığı ile kişisel bilgilerin elde edilmesini sağlayan dolandırıcılık yöntemi olarak tanımlanmaktadır. Günümüzde oltalama saldırısının tespiti için birçok uygulama mevcut olmasına rağmen hala önüne geçmekte zorluklar yaşanmaktadır. Bu çalışmanın amacı, web oltalama saldırılarına karşı kullanılan makine öğrenme tekniklerini karşılaştırmaktır. Web oltalama saldırı tespitinde Sınıflandırma ve Regresyon Ağaçları (CART), J48 (C4.5) Algoritması, Adaboost Algoritması, Rastgele Orman (RF) ve Sinir Ağları (NNet) olmak üzere 5 farklı mekine öğrenme yöntemi kullanılarak, bunların tahmin doğruluğu karşılaştırmalı test edilmiştir. Yapılan bu çalışmada toplamda 1353 mail üzerinden 702 oltalama yapmak isteyen web sitesi, 548 ise meşru web sitesi ve 103 şüpheli web sitesi veri kümesinde kullanılmıştır. Ayrıca, sınıfları eğitmek ve test etmek amacıyla kullanılan 10 öznitelik üzerinden değerlendirme yapılmıştır. 9 öznitelik ele alınmış ve 1 özniteklik sınıflandırmayı belirtmek için kullanılmıştır.**

Anahtar Kelimeler—Siber Saldırı, Web Oltalama, Makine Öğrenmesi

I. INTRODUCTION

Phishing is an online theft and fraud. It is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords [1]. With end-user training, web phishing attacks can be prevented to a certain extent. However, this is not highly secure. In this respect, web sites should be marked with machine learning methods. Thus, less work is provided to the end user in terms of security measures.

As a result of the significant increase of the internet in our lives, machine learning has started to be seen in every aspect of our lives. For example, recommendations through web banners use machine learning to personalize online ad delivery in almost real time. However, web sites can be damaging to a large extent by capturing our sensitive data through phishing [2,3].

The method used in phishing is often redirecting the user to fake web sites that are similar to original ones. Best way for redirecting them to these fake sites is convincing them with some offers that they cannot reject, like as if they won in a lottery or similar kind of games [4].

Some of the simple measures that can be taken against the web phishing attacks are;

- Not responding to unsolicited emails requesting your personal information
- Counterfeiting attacks take a variety of ways to keep users in doubt and gain their trust. Not to click on the address links in suspicious emails
- Not to provide personal information to suspicious or unfamiliar websites
- When you visit the websites of bank, credit card and service providers to enter your personal information, it goes through methods such as not typing the address of the site directly into the internet browser.

In recent years, through attacks on website phishing billions of dollars are harmed to individuals and corporations that conduct transactions such as online banking [5]. These attacks are increasing day by day. The measures listed above

can provide a certain level of safety. In this respect, with machine learning methods, we can prevent this attack by reducing the attack rate before it reaches the end user.

In addition, even if many network solutions are proposed and implemented for detection and prevention of phishing attacks, the effectiveness of these methods cannot be calculated. These solutions cannot be reinforced with more clear and computable methods that increase the error rate. The contribution of this study to literature is comparing the efficiency and accuracy of five different machine learning methods including J48, Classification and Regression Trees (CART), Adaboost Algorithm, Random Forest (RF), and Neural Network [6,7,8].

The rest of the article is organized as follows: Section 2 deals with the concept phishing with a web site. In the third chapter, the logic of machine learning methods and algorithms used in the study is mentioned. Chapter 4 describes the methods of machine learning for detecting website attacks by phishing. In the fifth chapter, the findings showing our experimental studies are expressed and the methods are presented. The result evaluation is presented in Chapter 6.

II. Web Phishing

One of the best cyber attacks used for obtaining the personal sensitive data of others is Phishing attack [9]. In this type of attack, an attacker attacks his victim through a fake website. These fake websites are almost identical to the original sites that actually exist. The victim is requested to click on the link in the e-mail to access the forms requested to enter or update personal information on these web sites. In this way, the victim's information is sent to the attacker [10].

People can use the internet for a variety of purposes, such as sending e-mails, conducting e-banking activities, selling products, or purchasing on-site [11]. Despite all these advantages of the Internet, there are some disadvantages. One of them is internet fraud, a type of crime executed on the internet. There are many ways that online users can be exposed to Internet fraud. Disclosure of these users 'sensitive information is also one of these attackers' intentions. Therefore, the Internet is a very good platform to trick people and capture private account information [12].

In recent years, only some of these researches against phishing attacks are focused on detection of phishing attacks on the website, which causes serious risks [13,14].

We've used both known and new features to classify fake websites. This study demonstrates the use of selected machine learning algorithms to test the features we specify. Table 1 describes preventive and corrective solutions that investigate phishing attacks.

TABLE I. Solutions for Phishing Attack

Solutions	Preventive Solutions	Corrective Solutions
Process Monitoring	Verification	Unpublishing The Website
Web Copy Disabling	Change Management	Forensic Investigation
Content Filtering	E-Mail Authentication	Internal Network Security Measures
Anti-Spam Feature	Web Application Security	External Network Security Measures

III. Machine Learning Methods And Algorithms

Machine learning is a type of artificial intelligence that makes software applications more accurate in predicting results without explicit programming. Algorithms that can receive input data and use statistical analysis to estimate an output value within an acceptable range are the mainstay of machine learning.

To fully understand the logic of machine learning algorithms and use it against cyber threats will reduce our error rate considerably. In this respect, the objectives and methods for using machine learning algorithms in attacks should be evaluated. These will be explained under three methods: accurate evaluation of data through classification, aggregation of data sets by clustering and establishing a relationship between data through proximity analysis [15].

A. *Accurate Evaluation of Data on Classification*

It is an evaluation obtained by making a classification which aims to estimate a result by creating separate classes in a data set. Using classification algorithms is beneficial for some methods such as spam email detection and health risk analysis. First, after scanning an email text and tagging recognized words and phrases, the classification algorithms are very effective way to determine whether the "signature" of the email is considered as spam. On the other hand, a network's instant statistics, security status, activity levels, and attack data can be run with an algorithm to determine a risk score for specific data [16].

B. *Aggregate Data Sets by Clustering*

One of the most effective algorithms of machine learning methods is clustering logic. The purpose of a cluster analysis algorithm is to consider entities in a single large pool and to form smaller groups that share similar characteristics [17]. For example, a television company that wants to determine the demographic distribution of watchers or watchers of different broadcasts can do so by building clusters based on available data about subscribers and broadcasts they watch. A restaurant chain can cluster its customers according to their menu choices based on geographic locations, and then change their menus accordingly. It can facilitate attacker analysis by aggregating requests to a website under cyber-attack [18]. Figure 1 shows the machine learning process.

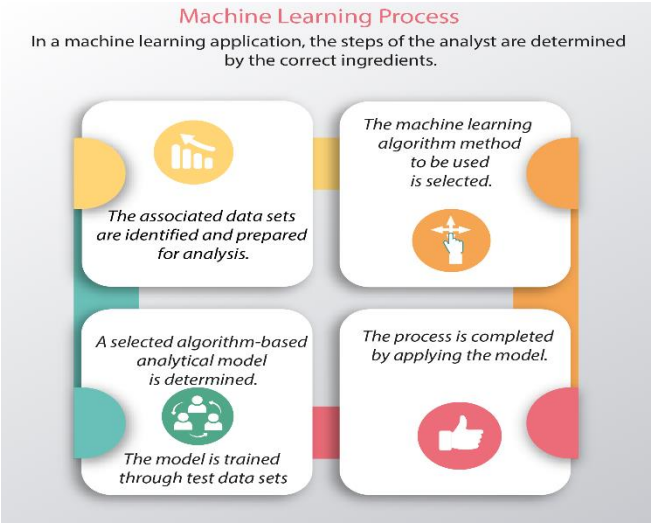

Fig. 1. Machine Learning Process

C. Establishing Relationship with Proximity Analysis

Proximity analysis is another approach to mining and analyzing data that can be made through machine learning. The purpose of this approach is exploring correlations between data features or transactional events. For example, it can often be used by retailers in market-basket analysis applications to identify products purchased at the same time. An online vendor can use the results to apply product placement on the website [19].

Cyber security efforts also often involve proximity analysis. Sequences of network operations prior to cyber attacks are analyzed to identify process patterns that occur close to each other. It can be used to formulate prescriptive analytic applications designed to evaluate similar attacks in similar attacks. In addition to these machine learning algorithms and approaches, there are many other algorithm methods that can be used to perform similar analysis results. Applying the right method in the right area will work best.

In this study, the accuracy of machine learning methods was tested by using Classification and Regression Trees (CART), J48 (C4.5) Algorithm, Adaboost Algorithm, Random Forest (RF) and Neural Networks (NNet) methods to predict phishing web sites. A total of 1353 e-mail and 542 legitimate websites and 103 suspicious websites were used in the data set.

IV. Machine Learning Methods for Detecting Phishing Attacks

The classification methods used in our study are mentioned. AdaBoost, Random Forest, J48, Artificial Neural Network Classification and Regression methods will be explained in general terms.

A. AdaBoost

Adaboost method is one of the techniques of learning with consecutive communities from the perspective of machine learning methods.The estimation speed is plays an important role for choosing this method. In addition, it can be applied in many data sets and uses memory space efficiently [20].

B. Random Forest

Random Forest (RF) is a classification algorithm that covers many concepts. It is mainly used for classification and regression methods. It brings together multiple trees while training. Multiple decision tree structure is used on the training side over real data sets. It is basically based on two features [20,21]. These features are the number of trees created and the number of predictors randomly selected when differentiating at each node.

C. J48 Classification Algorithm

J48 is a decision tree algorithm based on the very popular C4.5 algorithm. Decision trees are a classic way of representing information from a machine learning algorithm and offer a powerful and fast way of expressing data structures. This algorithm classifies the data as recursive. This ensures maximum accuracy of training data, but may create excessive rules that define only certain behavioral characteristics of the data [22].

D. Neural Networks

Neural Network (NN) includes the logic of self-learning in addition to previous machine learning methods. Memorize the problem and establish a relationship between the information that the problem has [23]. NN consists of 5 basic elements. These are;

- Inputs
- Outputs
- Addition Function
- Activation Function
- Weights

The xi symbol inputs are shown in Figure 2, which describes the structure of the NN. The input values are multiplied by the coefficient wi and the threshold value is obtained. The activation function is then applied. This is the basic logic in the structure of neural networks.

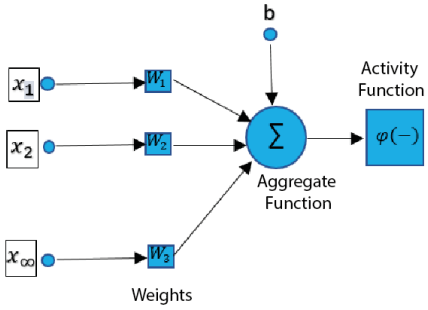

Fig. 2. Neural Network Process

E. Classification Via Regression (CART)

The most important feature of the CART algorithm, known as classification and regression tree, is its ability to create regression trees. Considering the values contained in the features, the training set is divided into two separate branches called candidate divisions. A node t has two branches of clusters, right ($t_{(right)}$) and left ($t_{(left)}$). Each data to be used in the creation of a regression tree is candidate to be divided into right and left branches. The twoing rule first calculates the probability for each candidate to be on the right and left branches. The probability for each candidate to divide the data into the left-hand branch is expressed as ($P_{(left}$) and P(j/ t_{left}), and the probability of right-hand branching ($P_{(\text{right}}$) and P(j / t_{right}). After calculating the probabilities, the measure of suitability of candidate divisions s at node t is shown in formula 1:

$$\cup(\sigma / \tau) = 2P_{left}\, P_{right}\, \alpha\nu\delta\, \Pi(\varphi / t_{(right)} \sum_{j=1}^{n} |P(j/t_{left}) - P(\tfrac{j}{t_{right}})| \quad (1)$$

V. Methods And Findings

In this study, various tested has been done on a computer with Intel (R) Core (TM) i7-3610QM 2.30 Ghz processor, 6 GB RAM with Windows 8.1 operating system. Different methods were applied in WEKA environment with the necessary data set and different parameters. With the tests performed, a model was created on the data set of the algorithms. Comparative analyzes have been carried out in various aspects with the methods described in the previous sections.

A. Method

The methods for classifying phishing attacks on the website with the data set obtained will be specified. In

addition, the evaluation techniques used in the comparison will be explained. In these comparisons, performance criterion, F-Criterion and ROC area were analyzed.

B. Data Set

The data set was used for detection of phishing website. The data set was evaluated over 10 features, including one for classification. Our data set consists of a total of 1353 records. 548 of these are classified as legitimate URLs, 702 of them are phishing URLs and 103 of them are classified as suspicious URLs. This data set was taken from UCI repository [24]. In addition, each feature is distinguished in that it contains at least one of the features that indicate that it is legitimate (1), suspicious (0) and Phishing (-1).

The need to observe how the algorithms to be applied acts on a data set, including all features in the specified data set, was effective in selecting all of these features. The features of the data set are given in Table 2.

TABLE II. WEB PHISHING DATASET FEATURES

No	Features
1	Having_IP_Address
2	URL_Length
3	PopUpWidnow
4	Age_of_Domain
5	Web_Traffic
6	SFH
7	SSLfinal_State
8	Request_URL
9	URL_of_Anchor
10	Result

Having_IP_Address: If the URL contains an IP address, this may be the indication of web phishing. This tag is -1 (Phishing) if the IP address exits in the domain, 1 (Legitimate) in other cases [25].

URL_Length: Generally, attackers hide the insecure part of the URL to capture data sent by a user. They can also redirect the web page to a suspicious domain. Normally, there is no measure for URL length, but recent studies have found that an acceptable limit can be used for URL length [26].

PopUpWidnow: When a pop-up prompts the user to add some certain data, this is generally the indicator of a fraudulent activity. Consisting of pop up window with text field may indicate the Phishing (-1) web page. [26].

Age_of_Domain: The duration of the web page may be an indicator. For example, if a web page has been in use for less than a month, this may indicate that it is a fake web page [26].

Web_traffic: When a website has high density traffic, then this webpage is really safe, and users can feel safe while browsing the site. Phishing websites normally have low navigation traffic and can be measured by rank in Alexa database. For example, a web page can be considered as Legitimate (1) if Alexa ranking is below 100.000 or Phishing (-1) if Alexa ranking is above 100.000 or Suspicious (0) if there is no Alexa record about that web page in Alexa ranking list [26].

SFH: Indicates that the empty string feature is hosted in the Server Form Handler. SFH is displayed or -1 (Phishing) if the string value is as 'about: blank' or empty, 0 (Suspicious) if referring to a different field, and 1 (Legitimate) in other cases [26].

SSLfinal_State: Indicates the existence of the HTTPS protocol. Using the HTTPS is Legitimate (1) if it is used, the provider is trusted, and the certificate age is one year or higher, Suspicious (0) if https is used and the provider is untrusted, otherwise Phishing (-1) [26].

Request_URL: Represents the state that the web page will attract different objects from different field names. The percentage of object request URLs pulled from external websites is shown as Legitimate (1) if the percentage is less than 22%, Suspicious (0) if the percentage is between 22% and 61%, Phishing (-1) in other cases [26].

URL_of_Anchor: The existence of the HTML anchor tag (<a> tag) usage in the URL. The percentage of URL presence in anchor tags is 1 (Legitimate) if the percentage is below 31%, 0 (Suspicious) if the percentage is between 31% and 67%, and -1 (Phishing) in other cases [26].

Result: The last parameter in our table, Result, is the class field that indicates whether it is marked as phishing or not. If the web page is fraud, the result is -1 (Phishing); if it is marked as good, the result is 1 (Legitimate); and if it is not clear whether the web page is Phishing or not, then the result is 0 (suspicious).

In order to process the data set and test the classification algorithms, Weka application and machine learning programs were used.

1) Performance Criteria: The presented classification algorithms were tested using k cross-validation. With the results obtained, True Positive Rate (TP Rate), False Positive Rate (FP Rate), F-Criteria, ROC Area and Accuracy Rate (Accuracy)) parameters were compared [27].

a) TP Rate: Based on the information obtained from the complexity matrix, the algorithm is a method used to calculate the correct estimation rate for the selected class [31]. Equation (8) is calculated using the formula 2.

$$TP\ Rate = TP/(TP + FP) \quad (2)$$

b) FN Rate: Similar to the TP Ratio, the complexity is obtained from the matrix. It is used to calculate the wrong estimate rate of the selected class. The following formula is seen on the calculation process [31].

$$FN\ Rate=FN/(TP+FN) \quad (3)$$

c) F-Measure: It is calculated as the harmonic mean of Precision and Recall. Calculation of the accuracy (A), precision (P) and F-criterion (Fm) values is shown by formulas 4,5 and 6 [28].

$$A = TP/(TP + FN) \quad (4)$$

$$P = TP/(TP + FN) \quad (5)$$

$$Fm = 2 * (\frac{A*P}{A+P}) \quad (6)$$

d) ROC: It is one of the criteria used to measure the accuracy of algorithms calculated on the curve graph obtained from TP ratio and FP ratio. ROC Field value is

between 0 and 1 and convergence with 1 indicates the increase in the success of the test.

C. Experimental Results

In this section, comparative analysis is performed on the results obtained with the experimental environment. After the analysis, the success and failure rates of classification algorithms used for detection of phishing attacks are shown graphically. Comparison of classification algorithms according to evaluation criteria is shown in Table 3.

In addition, the comparison of the success measures of classification algorithms according to the classifications of "Phishing", "Legitimates" and "Suspicious" is presented in the graphs in Figure 3, Figure 4 and Figure 5.

TABLE III. COMPARISON OF CLASSIFICATION ALGORITHMS ACCORDING TO PARAMETER VALUES

ALGORITHMS	Class	TP Rate	FP Rate	F-Measure	ROC	Accuracy
Classification and Regression Trees	0	0,689	0,017	0,728	0,708	0,772
	1	0,914	0,099	0,888	0,808	0,862
	-1	0.907	0,066	0,922	0,841	0,937
AdaBoost	0	0.000	0,000	-	0,545	-
	1	0.849	0,150	0,820	0,929	0,794
	-1	0.913	0,194	0,873	0,930	0,836
Neural Network	0	0.845	0,019	0,813	0,973	0,784
	1	0.872	0,078	0,878	0,957	0,884
	-1	0.906	0,100	0,907	0,959	0,907
Random Forest	0	0,854	0,014	0,842	0,991	0,830
	1	0,892	0,075	0,892	0,968	0,891
	-1	0,912	0,089	0,914	0,966	0,917
J48	0	0,932	0,015	0,881	0,986	0,835
	1	0,892	0,065	0,898	0,958	0,904
	-1	0,916	0,083	0,919	0,958	0,923

When the results of test attack packets are analyzed in Figure 3; it is seen that the best TP Ratio is obtained by J48 algorithm with 0.916 and the worst accuracy rate is obtained by Neural Network algorithm with 0.906.

In addition, when the detection of attack packets in terms of error rate (FP Ratio); Classification and Regression Trees algorithm is the best with the lowest error rate of 0.066, whereas AdaBoost is found to be a very inefficient algorithm with the highest error rate of 0.194.

Regarding the F-Measure, where the precision and sensitivity criteria are calculated; Classification and Regression Trees algorithm is the most successful algorithm with 0.922, while AdaBoost is the worst algorithm with 0.873.

Regarding ROC value;, Random Forest algorithm gives the best results with 0.966, while Classification and Regression Trees algorithm gives the worst results with 0.841.

When the accuracy rates are compared, in addition to the criterias mentioned above; the Classification and Regression Trees algorithm is the best with the highest accuracy rate of 0.937 and AdaBoost algorithm is the worst with the lowest accuracy rate of 0.836.

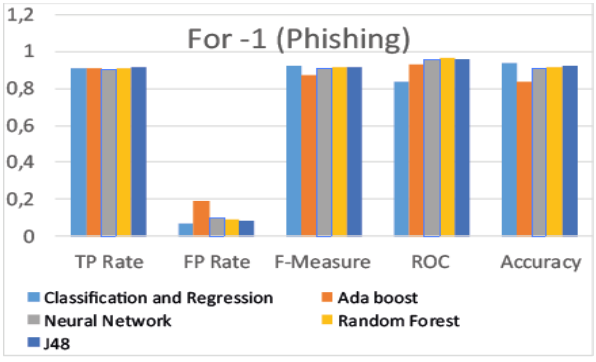

Fig. 3. Success measurement of classification algorithms according to "Phishing" (Class Value: -1) website detection

When the results of legitimate packets are examined in the experiment performed in Figure 4; Classification and Regression Trees algorithm is the best with the highest accuracy (TP Ratio) ratio of 0.914 and the AdaBoost is the worst algorithm with the lowest accuracy ratio of 0.849.

In addition, when the legitimate packet detection error rate (FP Ratio) is examined; J48 algorithm is the most successful with the lowest error rate of 0,065, while AdaBoost is the most unsuccessful algorithm with the highest error rate of 0,150.

In terms of F-Criterion value; J48 algorithm is the most successful algorithm with 0.898, while AdaBoost is the most unsuccessful with the lowest success rate of 0.820.

About ROC value; Random Forest algorithm gives the best result with 0.968, while Classification and Regression Trees algorithm gives the worst result with 0.808.

In addition, when the accuracy rates are compared, the J48 algorithm has the highest accuracy rate of 0.904, while the AdaBoost algorithm has the lowest accuracy rate of 0.794.

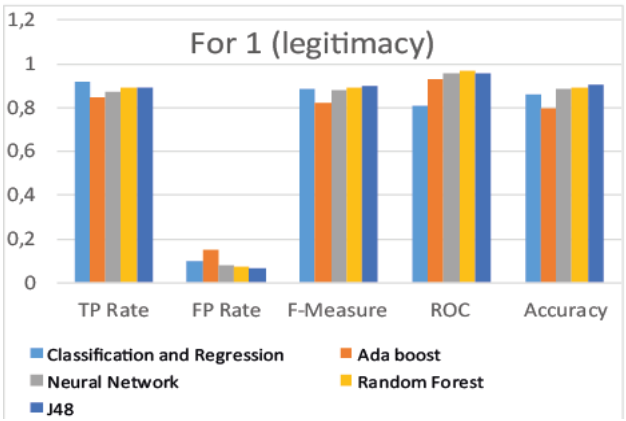

Fig.4. Success measurement of classification algorithms according to "legitimate" (Class Value: 1) website detection

As it is seen in Figure 5, when the results of the legitimate packets are examined in the experiment; J48 algorithm is the best with the highest accuracy (TP Ratio) with 0.932 and Classification and Regression Trees is the worst algorithm with the lowest accuracy rate of 0.689.

In addition, when the legitimate packet detection error rate (FP Ratio) is examined; AdaBoost algorithm is observed to be the most successful with the lowest error rate of 0, while Neural Network is observed as the most unsuccessful algorithm with the highest error rate of 0,019.

In terms of F-Criterion value; J48 algorithm is the most successful algorithm with 0.881, while Classification and Regression Trees is the most unsuccessful algorithm has the lowest success rate with 0.728.

About ROC value; Random Forest algorithm gives the best result with the rate of 0.991, while Classification and Regression Trees algorithm gives the worst result with 0.708.

In addition, when the accuracy rates are compared, J48 algorithm has the highest accuracy rate of 0.835, while the Classification and Regression Trees algorithm has the lowest accuracy rate of 0.772.

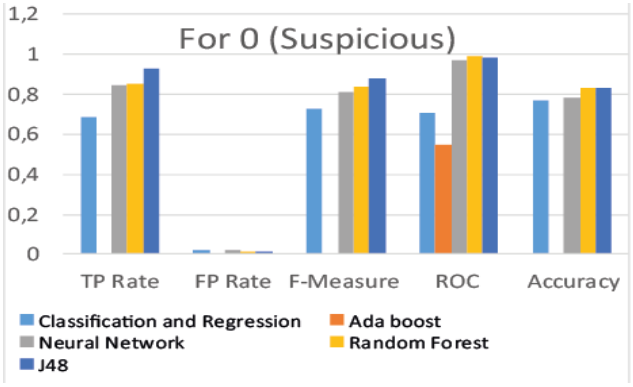

Fig.5. Success measurement of classification algorithms according to "Suspect" (Class Value: 0) website detection.

Table 4 shows the duration of model creation with the data sets used in the classification algorithms. These values are very important in terms of bandwidth, energy and resource usage. With this data set, the duration of creating the model reaches the highest value in Neural Network algorithm with 20.84 seconds, while the lowest value is obtained by J48 algorithm with 0.07 seconds.

TABLE 4. THE DURATION OF MODEL CREATION WITH THE DATA SETS USED IN THE CLASSIFICATION ALGORITHMS

Algorithm	Model Creation Time
Classification And Regression	1.38
Ada boost	0.12
Neural Network	20.84
Random Forest	0.65
J48	0.07

VI. RESULT

In recent years, billions of dollars are lost by individuals and corporations that conduct transactions such as online banking through websites on the web phishing attacks. These attacks are increasing day by day. To be able to get effective results against cyber-attacks with certain methods, the most effective techniques should be determined by performing experimental analyzes.

In this study, we searched for the predictive accuracy of five classifiers in a phishing dataset. Some methods are discussed to give an idea of existing machine learning techniques, comparison and most deterministic method between them. In this paper experimented with various Machine Learning algorithms and found Classification and Regression Trees algorithm as the best. And J48 is the lowest value.

In our research a dataset that has 10 features and a total of 1353 raw websites, 548 of which were legitimate, 702 of which were harmful and 103 of which were suspicious, was used to be able to estimate the probability of detecting phishing attacks with J48, Classification and Regression Trees (CART), AdaBoost, Random Forests (RF) and Neural Networks (NNet) Classification methods.

In this study, different methods on web phishing detection have been tested and achieved successful results in various aspects. These results were compared, and the best solutions have been revealed.

REFERENCES

[1] Patil, S., & Dhage, S. (2019, March). A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 588-593). IEEE.

[2] Dua, S., & Du, X. (2016). Data mining and machine learning in cybersecurity. CRC press.

[3] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[4] Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014, August). Machine learning for power system disturbance and cyber-attack discrimination. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-8). IEEE.

[5] Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+: A feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information and System Security (TISSEC), 14(2), 21.

[6] Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2008, November). An evaluation of machine learning-based methods for detection of phishing sites. In International Conference on Neural Information Processing (pp. 539-546). Springer, Berlin, Heidelberg.

[7] Fette, I., Sadeh, N., & Tomasic, A. (2006). Learning to detect phishing emails (No. CMU-ISRI-06-112). Carnegie-Mellon Univ Pittsburgh Pa Dept Of Computer Science.

[8] Sanglerdsinlapachai, N., & Rungsawang, A. (2010, January). Using domain top-page similarity feature in machine learning-based web phishing detection. In Knowledge Discovery and Data Mining, 2010. WKDD'10. Third International Conference on(pp. 187-190). IEEE.

[9] Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006, June). Phishing email detection based on structural properties. In NYS Cyber Security Conference (Vol. 3).

[10] Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 2053951715622512.

[11] Peiravian and Zhu, X. (2013, November). Machine learning for android malware detection using permission and api calls. In Tools with Artificial Intelligence (ICTAI), 2013 IEEE 25th International Conference on (pp. 300-305). IEEE.

[12] Wang, A. H. (2010, June). Detecting spam bots in online social networking sites: a machine learning approach. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 335-342). Springer, Berlin, Heidelberg.

[13] Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009, July). Detecting phishing emails using hybrid features. In Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on (pp. 493-497). IEEE.

[14] Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails.

[15] Sebastiani, F. (2002). Machine learning in automated text categorization. ACM computing surveys (CSUR), 34(1), 1-47.

[16] Tong, S., & Koller, D. (2001). Support vector machine active learning with applications to text classification. Journal of machine learning research, 2(Nov), 45-66.

[17] Fisher, D. H. (1987). Knowledge acquisition via incremental conceptual clustering. Machine learning, 2(2), 139-172.

[18] McGregor, A., Hall, M., Lorier, P., & Brunskill, J. (2004, April). Flow clustering using machine learning techniques. In International Workshop on Passive and Active Network Measurement (pp. 205-214). Springer, Berlin, Heidelberg.

[19] Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. (2007). Supervised machine learning: A review of classification techniques. Emerging artificial intelligence applications in computer engineering, 160, 3-24.

[20] Aytuğ, O. N. A. N., & Korukoğlu, S. (2016). Makine öğrenmesi yöntemlerinin görüş madenciliğinde kullanılması üzerine bir literatür araştırması. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 22(2), 111-122.Basnet, R., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. In Soft Computing Applications in Industry (pp. 373-383). Springer, Berlin, Heidelberg.

[21] Pal, M. (2005). Random forest classifier for remote sensing classification. International Journal of Remote Sensing, 26(1), 217-222.

[22] Patil, T. R., & Sherekar, S. S. (2013). Performance analysis of Naive Bayes and J48 classification algorithm for data classification. International Journal of Computer Science and Applications, 6(2), 256-261.

[23] Rowley, H. A., Baluja, S., & Kanade, T. (1998). Neural network-based face detection. IEEE Transactions on pattern analysis and machine intelligence, 20(1), 23-38.

[24] UCI Machine Learning Repository. "Phishing Websites Dataset".https://archive.ics.uci.edu/ml/datasets/Phishing+Websites (26.03.2016).

[25] Web:https://archive.ics.uci.edu/ml/machine-learning-databases/00327/Phishing%20Websites%20Features.docx, Accessed 02 09 2019.

[26] Davis J, Goadrich M. "The relationship between Precision-Recall and ROC curves". 23rd international Conference on Machine Learning, Pennsylvania, USA, 25-29 June 2006.

[27] Powers, D.M.. "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation". Journal of Machine Learning Technologies, 2(1), 37-63. 201.