Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 24, S. 35-41, Nisan 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 24, pp. 35-41, April 2021
Copyright © 2021 EJOSAT
Research Article

Prediction of Phishing Web Sites with Deep Learning Using WEKA Environment

Özlem Batur Dinler[1*], Canan Batur Şahin[2]

[1*] Siirt University, Faculty of Engineering, Departmant of Computer Engineering, Siirt, Turkey, (ORCID: 0000-0002-2955-6761), o.b.dinler@siirt.edu.tr
[2] Malatya Turgut Özal University, Faculty of Engineering and Natural Sciences, Departmant of Computer Engineering, Malatya, Turkey, (ORCID: 0000-0002-2131-6368), canan.batur@ozal.edu.tr

(2nd International Conference on Access to Recent Advances in Engineering and Digitalization (ARACONF)-10–12 March 2021)

(**DOI:** 10.31590/ejosat.901465)

ATIF/REFERENCE: Batur Dinler, Ö., Batur Şahin, C., (2021). Prediction of Phishing Web Sites with Deep Learning Using WEKA Environment. *European Journal of Science and Technology*, (24), 35-41.

Abstract

COVID-19 (Coronavirus) disease, observed in the city of Wuhan, China, on December 30, 2019, spread worldwide and caused a global epidemic. Since this epidemic can be transmitted very quickly and easily, some precautions and voluntary quarantine practices that governments have to take have significantly changed the habits of world communities in a short time. This change has especially increased distance activities, such as distance working, distance education, and distance shopping (e-commerce). Therefore, people have felt the need to quickly move the physical platforms they use to digital platforms to meet their daily needs. In this case, web phishing targeting digital platforms has led to a significant increase in online cyber attack types. The increase in phishing and the increasing volume of phishing websites have resulted in greater exposure of the world's information and organizations to various cyberattacks. Thus, after the COVID-19 pandemic in 2019, it has become more important than ever to detect phishing website analysis. In this study, performs the web phishing analysis and makes a comparison of classification performances among five popular methods: Random Forest (RF), Support Vector Machine (SVM), Multilayer Perception (MLP), k-Nearest Neighbour (k-NN), and Deep Learning (DL) by utilizing a Waikato Environment for Knowledge Analysis (WEKA) graphical user interface (GUI). In the experiments conducted with the data set divided into two as training and test, the RF and DL methods were more successful than the other methods compared, but k-NN, achieved a better performance when cross-validation was used. The possible reason for this is a simple approach toward deep learning. We hope the current study can provide guidance in investigating WEKA deep learning for web phishing classification.

Keywords: Machine learning, Deep learning, WEKA, DL4J deep learning architecture, Web Phishing, COVID-19.

WEKA Ortamını Kullanarak Derin Öğrenme ile Kimlik Hırsızı Web Sitelerinin Tahmini

Öz

30 Aralık 2019'da, Çin'in Wuhan şehrinde görülen COVID-19 (Coranavirus) hastalığı, dünya çapında yayılarak küresel bir salgına yol açmıştır. Bu salgın, çok hızlı ve çok kolay bulaşabildiği için hükümetlerin almak zorunda kaldığı birtakım önlemler ve gönüllü karantina uygulamaları, kısa bir süre içerisinde dünya topluluklarının alışkanlıklarını önemli ölçüde değiştirmiştir. Bu değişim özellikle, uzaktan çalışma, uzaktan eğitim ve uzaktan alışveriş (e-ticaret) gibi uzaktaki etkinlikleri artırdı. Bu nedenle insanlar günlük ihtiyaçlarını karşılamak adına kullandıkları fiziksel platformları, hızlıca dijital platformlara taşıma gereksinimi duydular. Bu durumda beraberinde, dijital platformların hedef alındığı web kimlik hırsızlığı çevrimiçi siber saldırı türlerinde ciddi bir artış meydana getirmiştir. Kimlik avındaki artış ve kimlik hırzısı web sitelerinin artan hacmi, dünyadaki bilgilerin ve kuruluşların çeşitli siber saldırılara daha fazla maruz kalmasıyla sonuçlandı. Bu nedenle, 2019'daki COVID-19 salgınından sonra kimlik hırsızı web sitelerinin analizini tespit etmek, her zamankinden daha önemli hale geldi. Bu çalışmada web kimlik hırsızlığı analiz edilmekte ve Bilgi Analizi için Waikato Ortamı (Waikato

[*] Corresponding Author: o.b.dinler@siirt.edu.tr

Environment for Knowledge Analysis - WEKA) grafik kullanıcı arayüzünden (GUI) yararlanarak RF, SVM, MLP, k-NN ve DL'den oluşan beş popüler yöntem arasındaki sınıflandırma performansları karşılaştırılmaktadır. Eğitim ve test olarak ikiye ayrılan veri seti ile yapılan deneylerde RF ve DL yöntemleri diğer yöntemlere göre daha başarılı iken, k-NN, çapraz doğrulama kullanıldığında daha iyi performans elde etmiştir. Bunun olası nedeni, derin öğrnemeye yönelik basit bir yaklaşımdır. Bu çalışmanın, kimlik hırzısı web sitelerinin sınıflandırması için WEKA derin öğrenmeyi araştırmada rehberlik sağlayacağını umuyoruz.

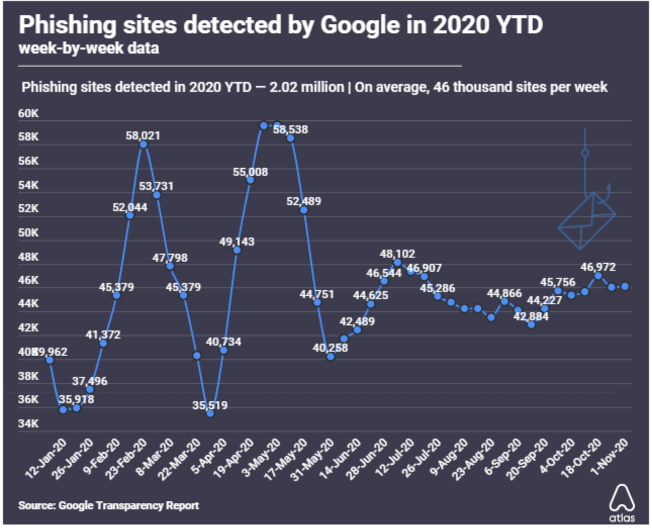
Anahtar Kelimeler: Makine öğrenimi, Derin öğrenme; WEKA, DL4J derin öğrenme mimarisi, Web Kimlik Hırsızlığı, COVID-19.

1. Introduction

The disease caused by the coronavirus, which was observed in the city of Wuhan, China, in December 2019 and called COVID-19, was declared a pandemic by the World Health Organization (WHO) on February 11, 2020. With the rapid spread of this outbreak, the number of patients increased, and many deaths occurred worldwide. Avoiding physical contact, quarantine or lockdowns have been implemented as effective measures to control the spread of the pandemic. As a result of these measures, the COVID-19 pandemic has brought about radical changes in the way of life of all people, from seven to seventy years old, worldwide. This change has started with the necessity of daily life activities carried out in physical environments to be transferred more to digital environments, and it has been in the direction of transforming the world's communities into rapidly digitalized individuals. Therefore, since the COVID-19 pandemic began, people have become accustomed to spending much more time in digital environments, and a significant increase in the internet and mobile use has been observed with the convenience provided by the digital world [1-2]. With these increases, a considerable increase has started to be observed in the number of phishing cyber attacks targeting digital platforms. In accordance with Google's Transparency Report [2], the tech giant identified 46,000 novel phishing websites on average each week in 2020. As shown in Figure 1, the total amount of phishing websites caught was surprisingly high, with 2.02 million in 2020 Year-to-Date (YTD). Moreover, the data in this figure demonstrate that the problem was especially severe in the first half of the year when more than 50,000 novel phishing sites were detected in certain weeks of February, April, March, and May. In this context, malicious actors took advantage of the COVID-19 pandemic crisis and intensified phishing attacks. These attacks came to the forefront, especially as "COVID-19" and "Coronavirus" themed attacks, and fraudsters who opened fake websites made large-scale illegal profits with the sales of large numbers of ordered medical materials. Identity theft has become a major threat not only for the healthcare sector but also for processes in many sectors and people using these processes during the pandemic. Therefore, it is extremely important to detect websites that steal an identity for the security of both corporate and personal information.

Machine learning technology is employed in different spheres of modern life. Machine learning applications are utilized for the purpose of identifying objects in images, transcribing speech into text, selecting relevant outcomes in a searching task, machine translation, etc. Machine learning has recently been using novel architectures, in other words, deep learning techniques. Deep learning is usually implemented by using the neural network architecture. With deep learning, the related information is learned and abstracted by the model in an automatic way with the data passing through the network. The term "deep" refers to the number of layers in the network, namely the network becomes deeper with the increasing number of layers. There is an interconnection of layers through nodes, or neurons, with each hidden layer using the output of the previous layer as its input [3]. In the current study, we utilized five classifiers, four from the machine learning architectures, SVM, RF, MLP and k-NN, and one deep learning architecture, Long short-term memory (LSTM). The performance of these methods is not limited to a single performance criterion and comparisons are made according to different performance criteria using accuracy, precision, recall, F-measure, and computational times criteria. Furthermore, in addition to the experiments performed traditionally with training and test data, experiments related to cross-validation performance are also conducted.

Figure 1: Detected Phishing Attack Statistics [2].



Source: Google Transparency Report

Many studies have been conducted in the literature to detect identity phishing web sites. Traditional machine learning and deep learning methods will be mainly defined. Moghimi et al. [4] suggested the supervised machine learning methods to detect phishing on the basis of SVM. The experiment demonstrated a high accuracy of 0.9865. Nevertheless, the said method totally relies on the webpage content feature. Thus, its performance can deteriorate in case of redesigning the content by attackers.

Nguyen and Nguyen [5] detected identity theft with machine learning methods by using not only URL but also page content. In the study, the J48 decision tree, RF, SVM, Naive Bayes, and neural network methods were compared using the features obtained from URL and content. According to the experimental results, the RF method obtained the most successful classification result.

Zouina et al. [6] employed the SVM algorithm with the aim of detecting phishing websites, and the findings demonstrated that the accuracy rate achieved 95.80%.

Chiew et al. [7] suggested a hybrid integrated development algorithm on the basis of data perturbation and function perturbation for the purpose of feature screening. In the said study, RF, C4.5, SVM, and other conventional machine learning methods were utilized for predicting the features in question. The researchers revealed that RF reached the highest accuracy.

Sahingöz et al. [8] made a comparison of the outcomes of Decision Tree, Adaboost, k-NN and RF, SMO and Naive Bayes models and revealed that RF obtained the highest accuracy of 97.89%.

Bahnsen et al. [9] made a comparison of the conventional machine learning method and LSTM method and demonstrated that the LSTM method was superior to machine learning methods, having an accuracy of 98.7%.

Nivaashini [10] proposed an automatic phishing identification method by employing deep learning to detect an unknown URL, either a phishing URL or benign URL. The Deep Boltzmann Machine (DBM) is used to pre-train the model with a superior representation of information for feature selection and binary classification of benign and phishing URLs using a Deep Neural Network (DNN), recognizing phishing URLs at a higher rate with a low false-positive rate.

Yuan et al. [11] suggested a method on the basis of features from URLs and web page links with the aim of detecting phishing websites and their targets. The researchers employed a Deep Forest model, obtaining a true positive rate of 98.3% and a false alarm rate of 2.6%.

Selvaganapathy *et al.* [12] suggested a phishing URL detection algorithm by utilizing a stacked restricted Boltzmann machine for feature selection and deep neural networks as classifiers. Afterward, they constructed multiple detections by utilizing IBK-kNN, Binary Relevance, and Label Powerset with SVM. The said model enhanced the detection accuracy as a result of combining the recognition results of multiple classifiers.

Furthermore, Chen et al. [13] suggested an LSTM-based phishing page detection approach.

The remaining part of the paper is organized as follows: materials and methods in Section 2, results and discussion in Section 3, and conclusions and recommendations are presented in the last section.

2. Material and Method

2.1. Phishing

Phishing was discovered in 1996, and nowadays, it is among the most severe cybercrimes that Internet users encounter. Web phishing is an online attack method in which the personal information (username, password, etc.) and financial data (credit card information, account number, etc.) of the victim are obtained by attackers who open fake websites with a completely similar design to the most widely used legitimate sites on the internet using the social engineering technique through short messages, e-mails, and WeChat [14-15]. It causes financial losses for both industries and individuals. Black Lists [16] and White Lists [17], Image processing [18], Heuristic [19], and Machine Learning-based approaches [20] are the most preferred methods to prevent phishing attacks. In the past and recent years, the research approach has focused on machine learning and the domain of 'Deep Learning,' which is the advanced field of machine learning. Deep learning is also known under the name of deep machine learning.

2.2. Dataset

We utilized the dataset from [21] in our experiments. Table 1 contains a detailed description of the features/attributes in the dataset. The dataset comprises 1353 instances. In the dataset, 9 features and class information for each instance contain a categorical value of -1 for identity thief, 1 for non-identity thief, and 0 for suspicious ones.

Table 1. Features of the web phishing dataset.

Attribute Number	Attributes	Posibble Values
1	*SFH*	1,-1,0
2	*PopUpWidnow*	-1,0,1
3	*SSLfinal_State*	1,-1,0
4	*Request_URL*	-1,0,1
5	*URL_of_Anchor*	-1,0,1
6	*Web_traffic*	1,0,-1
7	*URL_Length*	1,-1,0
8	*Age_of_domain*	1,-1
9	*Having_IP_Address*	0,1

2.3. Classifiers

In this study, four current machine learning methods, SVM, RF, MLP, and k-NN, and one current deep learning method, LSTM that are used for different classification problems nowadays, were used to classify phishing web sites. A brief description of the methods employed in the research is presented below.

2.3.1. Support Vector Machines (SVM)

It is an efficient classifier method that can separate instances in feature space. The aim of the SVM method is to find the furthest boundary (hyperplane) between the instances of two different classes in the feature space.

2.3.2. Random Forest (RF)

This method is one of the data mining models frequently used in the solution of both classification and regression problems. In this method, training is performed with decision trees formed by training a large number of different subsets randomly. The community of decision trees created in this method is called RF. In this classification model, a test instance of an unknown class is assigned according to the class of the highest valued decision tree. The most significant advantage of the RF model is its preventing overfitting and outlier problems.

2.3.3. Multilayer Perceptron (MLP)

A multilayer perceptron represents a thinking structure created as a result of connecting neurons to each other with synaptic connections. It is inspired by the human brain and has a learning algorithm, which is similar to neural networks in biological systems. An MLP is a feed-forward artificial neural network (ANN) model, mapping sets of input data onto a set of appropriate outputs. An MLP includes multiple layers of nodes in a directed graph, with each layer completely connected to the next one. Besides the input nodes, each node represents a neuron, or a processing element, having a nonlinear activation function. The

MLP employs a supervised learning technique, named back-propagation, for the purpose of training the network [3].

2.3.4. k-Nearest Neighbour (k-NN)

This method is among the machine learning methods used in classification and regression prediction problems. In addition to its simplicity and easy applicability, its being stable for large data sets has made the use of this method widespread. This method is a classification method based on determining to which of the previously labeled instances a new instance will be more similar by distance.

2.3.5. Deep Learning (DL)

Unlike shallow neural networks, the application of deep neural networks represents the application of hidden layers between input and output layers. There is a tendency of shallow networks to have one hidden layer. However, as a result of increasing hidden layers or deepening the network, there is a tendency of the application toward deep learning. There are different techniques to build deep networks, varying between deep belief networks and recurrent neural networks. The present study employs a simple approach toward deep learning by utilizing a WEKA[22] package, named DL4jMLPClassifier, allowing for stacking different forms of neural layers. After experiments, we selected the deep neural network architecture presented in Table 2.

Table 2. Architecture of the DL4J.

Features	
DL 2-Layers	*LSTM Layer* *Output Layer*
Learning rate:	*0.001*
Weight Initialization	*XAVIER*
Activation Function	*Activation RELU*
Lossfunction	*LossMCXENT*

We utilized the default Weka settings in general. In accordance with DL4J's[23] documentation, an iteration represents an update of the parameters of the neural network model[24]. Weka utilizes by default the number of instances as iterations.
Recurrent Neural Networks (RNNs), a type of artificial neural networks, are in the group of architecture. Unlike the standard RNN, an LSTM network is a very convenient approach for the classifier to learn from experiences, estimate the time span of the process when the long time delays between important events are unknown. It is possible to define an LSTM block as a smart network cell since it can remember a value for a random length of time. An LSTM block has gates that evaluate whether the input value is important enough to be remembered, the decision up to when to keep remembering/forgetting, and when it should be an output value [25].

2.4. Performance Metrics

In this paper, different validation options (Percentage Split and k-fold Cross-Validation) were investigated by conducting experiments related to cross-validation performance in addition to the experiments traditionally conducted with training and test data. For experimental purposes, four different approaches were exhibited. In the first approach (Experiment 1), the dataset was randomly divided into two subsets as 66% training set and 33% test set; in the second approach (Experiment 2), the dataset was divided as 70% training set and 30% test set; in the third approach (Experiment 3), the dataset was divided as 80% training set and 20% test set. In the final approach (Experiment 4), the accuracy value was found using 10-fold cross-validation.

Concerning software application, popular machine learning techniques, including SVM, RF, MLP, and k-NN, were employed in the WEKA standard classification library. The WEKA DL4jMLPClassifier was utilized to perform deep learning (DL).

With the aim of measuring performance, we utilized the metrics of accuracy, precision, recall, F-measure, and computational times. The metrics have the following definitions.

Accuracy: Refers to the ratio between outcomes that are correctly predicted and the sum of all predictions.

Precision: Denotes the ratio of the number of *positive* samples that are classified correctly to the total number of samples classified as *positive* (either in the correct or incorrect way).

Recall: Represents the ratio of the number of positive samples that are classified correctly as positive to the total number of positive samples.

F-measure: From time to time, there are contradictions in the precision rate and the recall rate. Thus, it is required to consider them in a comprehensive way. The F- measure denotes a weighted harmonic average of the precision rate and the recall rate. With an increase in the F- measure, the method becomes more effective.

The mentioned metrics are described in the Eqs. 1-4.

$$Accuracy = \frac{\mathrm{T}P + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad (1)$$

$$Precision = \frac{\mathrm{T}P}{\mathrm{TP} + \mathrm{FP}} \quad (2)$$

$$Recall = \frac{\mathrm{T}P}{\mathrm{TP} + \mathrm{FN}} \quad (3)$$

$$F - measure = \frac{\mathrm{2xRecallxPrecision}}{\mathrm{Recall} + \mathrm{Precision}} \quad (4)$$

While performing the assessment, *TP*, *TN*, *FP*, and *FN* are the number of positive classes that are predicted correctly, the number of negative classes that are predicted correctly, the number of positive classes that are predicted correctly, and the number of negative classes that are predicted incorrectly, respectively.

3. Results and Discussion

In the current part, we will present a more detailed description of our experiments and their findings. In the present study, the accuracies of various methods performances were compared. The methods are SVM, RF, MLP, k-NN, and DL. Table 3-6 contains the experimental results on the accuracy, precision, recall, and F-measure and the main measurements for classification performance of Experiment 1, Experiment 2, Experiment 3, and Experiment 4 on the basis of the web phishing dataset. The best results according to the relevant criteria are shown in bold.

- As seen in Table 3 (Experiment 1) and Table 4 (Experiment 2), RF exhibited the best accuracy performance compared to DL, SVM, MLP, and k-NN.
- As seen in Table 5 (Experiment 3), DL exhibited the best accuracy performance in comparison with SVM, RF, MLP, and k-NN.
- As seen in Table 6 (Experiment 4), k-NN displayed the best accuracy performance compared to DL, SVM, RF, and MLP.

Figure 2 show the accuracy results obtained with Experiments 1-4. In Experiment 1, Experiment 2, and Experiment 4, the quick observation determines that the simple deep learning model in WEKA exhibited the worst performance compared to the other models, while RF and k-NN had the highest accuracy.

Table 3. Comparison metrics of methods for Experiment 1

Method	*Accuracy*	*Precision*	*Recall*	*F-Measure*
DL	*88.6957%*	*0.887*	*0.887*	*0.887*
SVM	*86.5217%*	*0.849*	*0.865*	*0.853*
RF	***88.913%***	***0.889***	***0.889***	***0.889***
MLP	*88.4783%*	*0.886*	*0.885*	*0.885*
k-NN	*88.6957%*	*0.886*	*0.887*	*0.885*

Table 4. Comparison metrics of methods for Experiment 2

Method	*Accuracy*	*Precision*	*Recall*	*F-Measure*
DL	87.931%	0.882	0.879	0.880
SVM	86.4532%	0.851	0.865	0.856
RF	**89.9015%**	**0.900**	**0.899**	**0.899**
MLP	87.1921%	0.872	0.872	0.872
k-NN	88.4236%	0.882	0.884	0.882

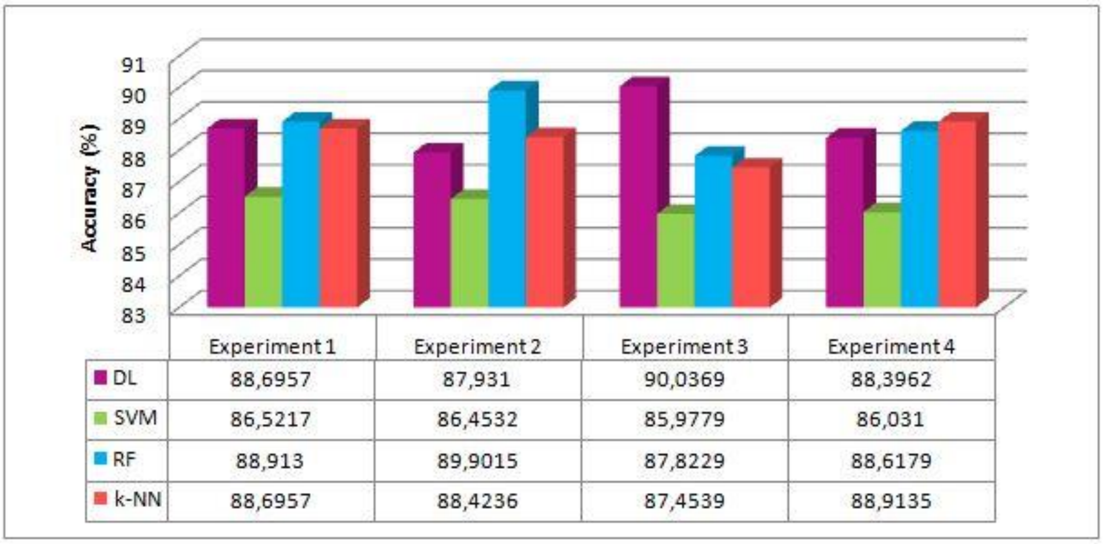
Table 5. Comparison metrics of methods for Experiment 3.

Method	*Accuracy*	*Precision*	*Recall*	*F-Measure*
DL	**90.0369%**	**0.902**	**0.900**	**0.901**
SVM	85.9779%	0.838	0.860	0.847
RF	87.8229%	0.880	0.878	0.879
MLP	88.9299%	0.890	0.889	0.889
k-NN	87.4539%	0.873	0.875	0.873

Table 6. Comparison metrics of methods for Experiment 4.

Method	*Accuracy*	*Precision*	*Recall*	*F-Measure*
DL	88.3962%	0.885	0.884	0.884
SVM	86.031%	0.843	0.860	0.846
RF	88.6179%	0.886	0.886	0.886
MLP	88.7657%	0.888	0.888	0.888
k-NN	**88.9135%**	**0.887**	**0.889**	**0.886**

Figure 2: Accuracy results obtained with experiments.



	Experiment 1	Experiment 2	Experiment 3	Experiment 4
■ DL	88,6957	87,931	90,0369	88,3962
■ SVM	86,5217	86,4532	85,9779	86,031
■ RF	88,913	89,9015	87,8229	88,6179
■ k-NN	88,6957	88,4236	87,4539	88,9135

The implementation of the algorithms was performed on a PC having an Intel Core i3-2367M processor, a 4 GB memory size, and a 1.40 GHz clock speed. Table 7 summarizes the working times obtained by running the approaches applied with the training and test data (Experiments 1-3) and Table 8 summarizes cross-validation data (Experiment 4) with different methods. In Table 7, RF was the fastest method with Experiment 3 approach, the DL method was the slowest method with Experiment 1 approach. Whereas, in Table 8, k-NN was the fastest method with Experiment 4 approach, DL was the slowest method.

Table 7. *Comparison of the working time (in second) of the methods for Experiment 1-Experiment3.*

Method	*Experiment 1*	*Experiment 2*	*Experiment 3*
DL	***495.22***	*474.91*	*482.53*
SVM	*0.47*	*0.47*	*0.32*
RF	*0.16*	*0.07*	***0.05***

MLP	*5.07*	*4.74*	*4.83*
k-NN	*0.06*	*0.12*	*0.06*

Table 8. *Comparison of the working time (in second) of the methods for Experiment 4*

Method	*Time (in seconds)*
DL	***486.23***
SVM	*0.33*
RF	*0.03*
MLP	*4.78*
k-NN	***0.01***

4. Conclusions and Recommendations

Within the scope of this study, it was estimated whether a website is an identity thief using different popular classifier methods in the WEKA environment. The methods were compared in terms of working time and different success criteria. An important reason for obtaining results close to each other is that some of the features in the data set are particularly strong and moderately related, indicating the class of instances.

At the same time, we show in the current study the systematic methodology of utilizing WEKA DeepLearning4j to classify web phishing. For future research, we want to investigate the novel approach toward web phishing classification, "deep learning," which can enhance the results. It is possible to utilize a lot of different potential combinations of neural networks, layer architectures and sizes, and other criteria to enhance the classification success rate. In the present research, the testing of only a few combinations of layers was performed.

References

[1] Güven, H. (2020), Changes in E-Commerce in the Covid-19 Pandemic Crisis Process, Eurasian Journal of Researches in Social and Economics (EJRSE), 7(5):251-268, ISSN:2148-9963.

[2]https://atlasvpn.com/blog/google-reports-over-2-million-phishing-sites-in-2020-ytd

[3] Batur Dinler, Ö., Aydın, N. (2020), An Optimal Feature Parameter Set Based on Gated Recurrent Unit Recurrent Neural Networks for Speech Segment Detection, *Applied Sciences*. 10(4):1273. https://doi.org/10.3390/app10041273.

[4] Moghimi, M., Varjani, A. Y. (2016), New rule-based phishing detection method[J], Expert Systems with Applications, 53: 231-242.

[5] Nguyen HH, Nguyen DT. (2016), Machine Learning based phishing web sites detection. AETA 2015: Recent Advances in Electrical Engineering and Related Sciences. LNEE, 371, 123-131.

[6] Zouina, M., Outtaj, B. (2017), A novel lightweight URL phishing detection system using SVM and similarity index. Human-centric Computing and Information Sciences, vol. 7, p. 17. Springer Open, Netherlands.

[7] Chiew, K.L., Tan, C.L., Wong, K., Yong, K.S., Tiong, W.K. (2019), A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. Inf. Sci. 484, 153–166.

[8] Sahingoz, O.K., Buber, E., Demir, O., Diri, B. (2019), Machine learning based phishing detection from URLs. Expert Syst. Appl. 117, 345–357.

[9] Bahnsen, A.C., Bohorquez, E.C., Villegas, S., Vargas, J., Gonzlez, F.A. (2017), Classifying phishing URLs using recurrent neural networks. In: Proc of 2017 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–8.

[10] Nıvaashını. M. (2017). Deep Boltzmann Machine Based Detection of Phishing URLS, International Journal of Advances in Electronics and Computer Science, Volume-4, Issue-9, Sep.

[11] Yuan, H., Chen, X., Li, Y., Yang, Z., and Liu, W. (2018), Detecting Phishing Websites and Targets Based on URLs and Webpage Links, in 2018 24th International Conference on Pattern Recognition (ICPR), pp.3669–3674, doi: 10.1109/ICPR.2018.8546262.

[12] Selvaganapathy, S.G., Nivaashini, M., and Natarajan, H.P. (2018), Deep belief network based detection and categorization of malicious URLs, Inf. Secur. J., Global Perspective, vol. 27, no. 3, pp. 145–161, Apr.

[13] Chen, W., Zhang, W., and Su, Y. (2018), Phishing detection research based on LSTM recurrent neural network, in Proceedings of International Conference of Pioneering Computer Scientists, Engineers and Educators, pp. 638–645, Springer, Zhengzhou, China, September.

[14] https://en.wikipedia.org/wiki/WeChat.

[15] Gupta, B. B., Arachchilage, N. A. G. & Psannis, K. E. (2018), Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67* (2), 247–267.

[16] Prakash, P., Kumar, M., Kompella, R.R., and Gupta, M., (2010), Phish-Net: Predictive blacklisting to detect phishing attacks," in *Proceedings of the 2017 IEEE Conference on Computer Communications (IEEE INFOCOM2010)*, San Diego, USA, March.

[17] Jain, A.K., and Gupta, B.B. (2016), A novel approach to protect against phishing attacks at client side using auto-updated white-list, EURASIP Journal on Information Security, vol. 2016, no. 1, p. 1-9.

[18] Jain, A.K., and Gupta, B.B. (2017), Phishing Detection: Analysis of Visual Similarity Based Approaches, Security and Communication Networks, vol. 2017, pp. 1–20, doi: 10.1155/2017/5421046.

[19] Babagoli, M., Aghababa, M. P., & Solouk, V. (2018), Heuristic nonlinear regression strategy for detecting phishing websites. Soft Computing, pp: 1–13.

[20] Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007), A comparison of machine learning techniques for phishing detection. In Proceedings of the anti-phishing working groups 2nd annual ecrime researchers summit, eCrime '07, ACM, New York, NY, USA (pp. 60–69). APWG. Accessed 24 July 2018. http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[21] UCI Machine Learning Repository, Website Phishing Data Set, https://archive.ics.uci.edu/ml/datasets/Website+Phishi ng (17.01.2021)

[22] Frank, E., Hall, M.A., Witten, I.H. (2016), The Weka Workbench, 4th ed.; Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques",Morgan Kaufmann: Burlington, MA, USA.

[23] Lang, S., Bravo-Marquez, F., Beckham, C., Hall, M., Frank, E. (2019), WekaDeeplearning4j: A Deep Learning Package for Weka based on DeepLearning4j, Knowl.-Based Syst.178, 48–50. [CrossRef]

[24] Mouratidis, D., ve Kermanidis, K. (2019), Paralel Verilerin Dilden Bağımsız Otomatik Seçimi için Topluluk ve Derin Öğrenme. Algoritmalar, 12 (1), 26. doi: 10.3390/ a12010026 .

[25] Şahín, C., and Dírí B. (2019), Robust Feature Selection with LSTM Recurrent Neural Networks for Artificial Immune Recognition System, IEEE Access, Vol.7, pp. 24165 – 24178.