Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 425-431, Kasım 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 425-431, November 2021
Copyright © 2021 EJOSAT
Research Article

Comparison of Performance of Phishing Web Sites with Different DeepLearning4J Models

Özlem Batur Dinler[1*], Canan Batur Şahin[2], Laith Abualigah [3]

[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
[3] Amman Arab University, Faculty of Computer Sciences and Informatics, Departmant of Computer Engineering, Amman, Jordan, (ORCID: 0000-0002-2203-4549), aligah.2020@gmail.com

(1st International Conference on Applied Engineering and Natural Sciences (ICAENS)- 1-3 November 2021)

(**DOI:** 10.31590/ejosat.1004778)

ATIF/REFERENCE: Batur Dinler, Ö., Batur Şahin, C. & Abualigah, L. (2021). Analysis of Phishing Web Sites by Using WEKA DL4J Techniques. *European Journal of Science and Technology*, (28), 425-431.

Abstract

Due to the new type of coronavirus (COVID-19) disease, which was first seen in Wuhan, China in 2019, a pandemic was declared by the World Health Organization (WHO) on March 11, 2020. The pandemic, which is still in effect throughout the world, has changed the daily life activities and habits of the whole world community in a short time and shifted them towards digital media applications. Accordingly, increasing cyber-attack attacks and data breaches have created great risk for the pandemic society. In this context, the security of digital media applications has become a much more important issue with the COVID-19 outbreak. The issue has been observed especially on phishing websites. Web phishing is the practice of stealing personal information such as name, last name, password, and credit card numbers of individuals by imitating a reputable business. It will result in the exposure of information and the financial damage. The focus of the study is based on several DeepLearning4j (DL4j) models used to identify phishing websites. However, the main purpose of the study is to efficiently monitor the effectiveness of DeepLearning4J (DL4J) models with the aim of improving the performance of evaluation metrics.

Keywords: COVID-19, DL4J, Cyber attack, Web, Phishing.

Kimlik Hırsızı Web Sitelerinin Farklı DeepLearning4J Modelleri ile Performanslarının Karşılaştırılması

Öz

İlk olarak 2019'da Çin'in Wuhan şehrinde görülen yeni tip koranavirüs (COVID-19) hastalığı nedeniyle 11 Mart 2020 tarihinde Dünya Sağlık Örgütü (DSÖ) tarafından pandemi ilan edilmiştir. Dünya genelinde hâlâ etkisi devam etmekte olan bu salgın, kısa sürede tüm dünya toplumunun gündelik yaşam aktivitelerini ve alışkanlıklarını hızlı bir şekilde değiştirerek digital ortam uygulamalarına doğru kaydırmıştır. Bu doğrultuda, artan siber saldırı atakları ve yaşanan veri ihlalleri salgın toplumu için büyük bir risk oluşturmuştur. Bu bağlamda, dijital ortam uygulamalarının güvenliği COVID-19 salgını ile çok daha önemli bir sorun haline gelmiştir. Bu sorun özellikle kimlik hırsızı web siteleri üzerinde gözlenmiştir. Web kimlik hırsızlığı, güvenilir kurumları taklit ederek kişilerin ad, soyad, şifre ve kredi kartı numaraları gibi kişisel bilgileri çalma yöntemidir. Bu, bilginin ifşa olmasına ve mali zarara neden olacaktır. Çalışmanın odağı, kimlik hırsızı web sitelerinin tanımlanması amacı ile kullanılan birkaç DeepLearning4j (DL4j) modeline dayanmaktadır. Bununla birlikte, çalışmanın temel amacı, değerlendirme metriklerinin performanslarını iyileştirmek amacı ile DeepLearning4J (DL4J) modellerinin etkinliğini verimli bir şekilde izlemektir.

Anahtar Kelimeler: COVID-19, DL4J, Siber Saldırı, Web, Kimlik Hırsızlığı.

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

1. Introduction

Nowadays, the ongoing pandemic process continues to affect the whole world with the mutation of the new type of coronavirus in various parts of the world. The fact that the mutated virus is much more contagious than the old virus has made it mandatory for governments to renew comprehensive quarantine practices and stay home calls. Therefore, the change in the outbreak has adversely affected the course of the pandemic and led to the prolongation of the normalization process. Thus, this process has made the standard way of living and doing business of the pandemic society more dependent on the digital environment [1-2]. This has brought about many advantages, such as avoiding physical contact, reducing and controlling mass mobility to prevent the spread of the mutated virus, and also privacy and data security problems. These problems have led to a significant increase in the number of web phishing online cyberattacks, especially targeting internet fraud and web security. According to a report prepared by Google, 2,145,013 phishing sites have been registered by Google since Jan 17, 2021. The number of phishing sites has increased from 1,690,000 on Jan 19, 2020 [3]. In this context, cybercriminals have taken advantage of the COVID-19 pandemic and intensified web phishing attacks.

It is possible to define web phishing as the development of fake websites and the replication of trusted websites for the purpose of deceiving online users as a result of obtaining access to their login information in an illegal way to steal their financial assets. Humans represent the weakest link in a protection program. It causes financial losses for industries and individuals [4]. Therefore, the detection of identity theft websites is extremely important in terms of warning users before any identity theft occurs and preventing the damage it may cause.

The success of deep neural networks has been proven in different scientific domains [5]. Moreover, recent research has demonstrated the possibility of the successful use of neural networks in a number of tasks in phishing websites [6-11]. However, to the author's knowledge, [1] the WEKA DL4J algorithm was employed for the first time for the detection of phishing websites, and the results showed that the accuracy rate was 90.03%. The current paper also represents the first comprehensive study that analyzed phishing websites by utilizing the WEKA DL4J method. Thus, this study extends the previous research [1] conducted on deep learning approaches to predict phishing websites by employing the deep learning implementation algorithms DL4J, as implemented in Weka. In comparison with the previous study [1], the current approach involves the innovations indicated below: i) the design of DL4J models predicting phishing websites, ii) the comparison of the performance and predictive accuracy of deep learning models to predict phishing websites.

This study compared the performance of DL4J methods according to five different performance metric using the accuracy, precision, recall, F-measure, and computational times (CT, in seconds (s)) criteria. Furthermore, in addition to the experiments traditionally performed using training and test data, experiments related to cross-validation performance are also performed.

The remaining part of the study is organized in the following way. The materials and methods are described in Part 2, while more details of experiments and the findings of the classification process are presented in Part 3. In the end, Part 4 include conclusions.

2. Material and Method

Here, a detailed description of the data sets, tools, and classification process employed in our experiments is presented.

2.1. Dataset

The dataset from [12] was utilized in our tests. SFH, Pop Up Window, Final state of SSL, URL Request, Anchor URL, Web traffic, Length of URL, Domain age, Having IP Address, and Result represent the most suitable attributes to detect phishing websites. There are 1353 instances in the dataset. In the dataset, 9 attributes and class information for each sample contain a categorical value of -1 for identity thieves, 1 for non-identity thieves, and 0 for suspicious ones.

2.2. Deep Learning4J Using WEKA

A neural network generally represents a technology that is built with the aim of simulating particularly the human brain's activity, pattern recognition, and the passage of input via different layers of simulated neural connections. Deep neural networks are defined by various experts as networks with an input layer, an output layer, and a minimum of one hidden layer between them. Every layer conducts certain types of sorting and ordering in a process, called "feature hierarchy." Moreover, the phrase "deep learning" is utilized with the aim of describing the mentioned deep neural networks since deep learning is a particular form of machine learning in which technologies utilizing aspects of artificial intelligence seek to classify and order information in ways going beyond simple input/output protocols [13-14]. As demonstrated in Figure 1, a lot of deep learning open source tools can be utilized to classify phishing websites. The current study will focus on Weka Deep Learning4j [15]. Weka Deep learning4j uses a simple approach towards deep learning by means of a WEKA [16] package, called DL4JMLP Classifier, which ensures stacking various forms of neural layers.

The structure of the DL4J models is described in Table 1. We utilized models with the LSTM layer, GravesLSTM layer, Dense layer, and Output layer, The structure of the DL4J models is described in Table 1. We utilized models with the LSTM layer, GravesLSTM layer, Dense layer, and Output layer.

Figure 1: DL open source tool[17].

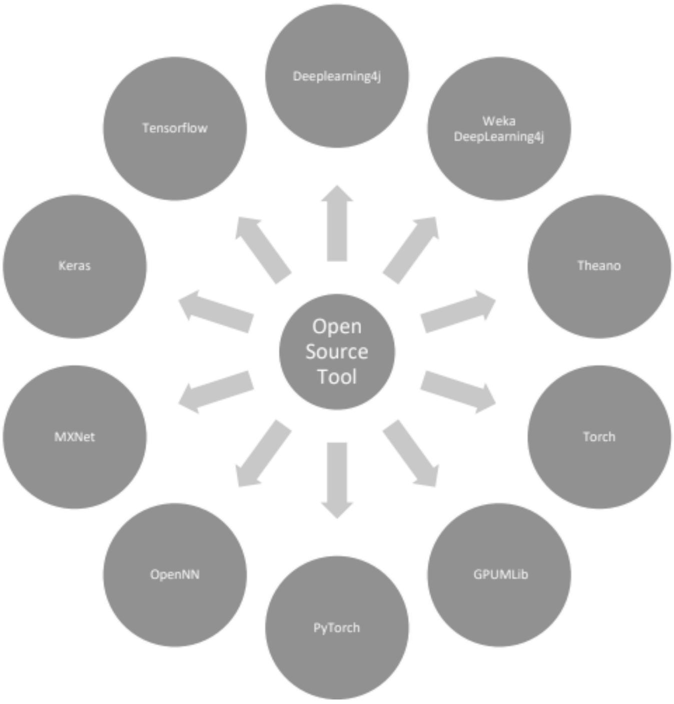


Table 1. Details of DL4Jmodels for the experiments.

Types of Layer	Layer Details	Number of Layers
LSTM 2- Layer	LSTM Layer Output Layer	2
GravesLSTM 2-Layer	GravesLSTM Layer Output Layer	
Dense 2- Layer	Dense Layer Output Layer	
LSTM 3-Layer	LSTM Layer LSTM Layer Output Layer	3
GravesLSTM 3-Layer	GravesLSTM Layer GravesLSTM Layer Output Layer	
Dense 3-Layer	Dense Layer Dense Layer Output Layer	
LSTM & Dense 3-Layer	LSTM Layer Dense Layer Output Layer	
Dense & LSTM 3-Layer	Dense Layer LSTM Layer Output Layer	
LSTM & GravesLSTM 3-Layer	LSTM Layer GravesLSTM Layer Output Layer	
GravesLSTM &LSTM 3-Layer	GravesLSTM Layer LSTM Layer Output Layer	
GravesLSTM & Dense 3-Layer	GravesLSTM Layer Dense Layer Output Layer	
Dense & GravesLSTM 3-Layer	Dense Layer GravesLSTM Layer Output Layer	

2.3. Evaluation Metrics

The present research examined various validation options (Percentage Split and k-fold Cross-Validation) by carrying out experiments with regard to cross-validation performance as well as the experiments traditionally carried out using training and test data. The detailed information on the dataset properties of the experiments used in this study is shown in Table 2.

Table 2. The details dataset used for experiments.

	Training Set	**Testing Set**
Experiment 1	*%66*	*%33*
Experiment 2	*%70*	*%30*
Experiment 3	*%80*	*%20*
Experiment 4	*10-fold cross-validation*	

The aim of detecting phishing websites is to determine phishing instances from the test dataset containing phishing websites and legal websites, which basically represents a binary classification essence. Four kinds of classification are employed in binary classification for the purpose of measuring the accuracy of the classification confusion matrix.

Table 3. The details dataset used for experiments.

	Classified Phishing	**Classified Legitimate**
Actual Phishing	*TP*	*FN*
Actual Legitimate	*FP*	*TN*

Table 3 presents the confusion matrix related to the study, where:

- True Positive (TP) refers to the number of correctly detected phishing websites.
- False Negative (FN) refers to the number of phishing websites detected as legitimate websites.
- False Positive (FP) refers to the number of legitimate websites detected as phishing websites.
- True Negative (TN) refers to the number of legitimate websites detected as legitimate websites.

With the aim of assessing the performance of the experiments, measures including Accuracy, Precision, Recall, F-measure, and computational times (CT), were utilized.

Accuracy is the criterion that gives the ratio of correctly classified inputs to total inputs. It is described in Equation (1):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (1)$$

Precision is the ratio of correctly classified positive inputs to total positive values. It is described in Equation (2).

$$Precision = \frac{TP}{TP + FP} \qquad (2)$$

Recall is the ratio of correctly classified positive inputs to actual positive values. It is described in Equation (3).

$$Recall = \frac{TP}{TP + FN} \qquad (3)$$

The F-Measure refers to a weighted harmonic average of the precision rate and the recall rate. It is described in Equation (4).

$$F - Measure = \frac{2xRecallxPrecision}{Recall + Precision} \qquad (4)$$

3. Results and Discussion

The present research implements four experiments on the basis of twelve various scenarios. The experiments and their results

were assessed by utilizing five metrics, the performance of the said experiments was compared, and the findings are presented in Tables 4-7.

Table 4. Comparison metrics of models for Experiment 1.

Types of Layer	**Accuracy**	**Precision**	**Recall**	**F-Measure**	**CT (s)**	**Node**
LSTM 2	*89.78%*	*0.898*	*0.898*	*0.898*	*166.37*	*20*
GravesLSTM 2	*89.56%*	*0.896*	*0.896*	*0.896*	*193.96*	*20*
Dense 2	*90.21%*	*0.901*	*0.902*	*0.901*	*64.25*	*50*
LSTM 3	*90.43%*	*0.907*	*0.904*	*0.905*	*246.53*	*10*
GravesLSTM 3	*88.91%*	*0.891*	*0.889*	*0.890*	*364.24*	*30*
Dense 3	*88.69%*	*0.886*	*0.887*	*0.886*	*91.46*	*30*
LSTM & Dense 3	*88.47%*	*0.884*	*0.885*	*0.884*	*169.84*	*10*
Dense & LSTM 3	*90.21%*	*0.902*	*0.902*	*0.902*	*186.47*	*30*
LSTM & GravesLSTM 3	***91.08%***	***0.913***	***0.911***	***0.911***	***297.28***	***20***
GravesLSTM &LSTM 3	*89.56%*	*0.894*	*0.896*	*0.895*	*287.23*	*10*
GravesLSTM & Dense 3	*90.00%*	*0.901*	*0.900*	*0.900*	*211.08*	*20*
Dense &GravesLSTM 3	*89.56%*	*0.895*	*0.896*	*0.895*	*221.23*	*30*

Table 5. Comparison metrics of models for Experiment 2.

Types of Layer	Accuracy	Precision	Recall	F-Measure	CT (s)	Node
LSTM 2	*89.40%*	*0.895*	*0.894*	*0.894*	*179.54*	*50*
GravesLSTM 2	*89.65%*	*0.897*	*0.897*	*0.897*	*203.27*	*20*
Dense 2	*90.14%*	*0.901*	*0.901*	*0.901*	*64.69*	*30*
LSTM 3	*90.14%*	*0.901*	*0.901*	*0.901*	*283.51*	*40*
GravesLSTM 3	*89.90%*	*0.900*	*0.899*	*0.899*	*341.81*	*20*
Dense 3	*88.91%*	*0.890*	*0.889*	*0.889*	*95.63*	*50*
LSTM & Dense 3	*88.91%*	*0.891*	*0.889*	*0.890*	*178.88*	*20*
Dense & LSTM 3	***90.39%***	***0.905***	***0.904***	***0.904***	***192.93***	***50***
LSTM & GravesLSTM 3	*89.90%*	*0.900*	*0.899*	*0.899*	*324.04*	*30*
GravesLSTM &LSTM 3	*90.14%*	*0.902*	*0.901*	*0.902*	*322.2*	*30*
GravesLSTM & Dense 3	*89.65%*	*0.897*	*0.897*	*0.897*	*221.47*	*20*
Dense &GravesLSTM 3	*89.40%*	*0.895*	*0.894*	*0.894*	*239.06*	*50*

Table 6. Comparison metrics of models for Experiment 3.

Types of Layer	Accuracy	Precision	Recall	F-Measure	CT (s)	Node
LSTM 2	*89.29%*	*0.893*	*0.893*	*0.893*	*167.23*	*50*
GravesLSTM 2	*90.40%*	*0.905*	*0.904*	*0.904*	*193.09*	*20*
Dense 2	***90.77%***	***0.909***	***0.908***	***0.908***	***59.22***	***10***
LSTM 3	*89.66%*	*0.899*	*0.897*	*0.897*	*253.53*	*10*
GravesLSTM 3	***90.77%***	***0.911***	***0.908***	***0.908***	***370.73***	***50***
Dense 3	*89.29%*	*0.895*	*0.893*	*0.894*	*90.67*	*20*
LSTM & Dense 3	*90.40%*	*0.904*	*0.904*	*0.904*	*170.21*	*10*
Dense & LSTM 3	*89.29%*	*0.895*	*0.893*	*0.894*	*193.89*	*40*
LSTM & GravesLSTM 3	*90.03%*	*0.903*	*0.900*	*0.901*	*287.85*	*20*
GravesLSTM &LSTM 3	*90.03%*	*0.901*	*0.900*	*0.901*	*287.91*	*20*
GravesLSTM & Dense 3	***90.77%***	***0.910***	***0.908***	***0.908***	***221.16***	***30***
Dense &GravesLSTM 3	*89.29%*	*0.893*	*0.893*	*0.893*	*216.37*	*10*

Table 7. Comparison metrics of models for Experiment 4.

Type of Layer	Accuracy	Precision	Recall	F-Measure	CT (s)	Node
LSTM 2	*90.24%*	*0.903*	*0.902*	*0.903*	*171.94*	*20*
GravesLSTM 2	***90.61%***	***0.907***	***0.906***	***0.906***	***210.59***	***20***
Dense 2	*90.53%*	*0.906*	*0.905*	*0.906*	*58.69*	*50*
LSTM 3	*90.17%*	*0.904*	*0.902*	*0.902*	*298.65*	*40*
GravesLSTM 3	*90.46%*	*0.906*	*0.905*	*0.905*	*392.97*	*20*
Dense 3	*89.94%*	*0.899*	*0.899*	*0.899*	*80.11*	*30*
LSTM & Dense 3	*90.24%*	*0.904*	*0.902*	*0.903*	*176.78*	*20*
Dense & LSTM 3	*84.94%*	*0.900*	*0.899*	*0.900*	*187.51*	*20*
LSTM & GravesLSTM 3	*90.24%*	*0.904*	*0.902*	*0.903*	*307.58*	*20*
GravesLSTM &LSTM 3	*90.46%*	*0.905*	*0.905*	*0.905*	*290.23*	*20*
GravesLSTM & Dense 3	*90.02%*	*0.901*	*0.900*	*0.900*	*219.96*	*20*
Dense &GravesLSTM 3	*90.31%*	*0.904*	*0.903*	*0.903*	*219.02*	*20*

Experiment 1- As seen in Table 4, LSTM & GravesLSTM having 3 layers yielded the highest accuracy, precision, recall, and F-measure in comparison with DL4J models having other layers. DL4J hybrid model having 20 nodes and 297.28 computational times was the model with the best prediction rate among all the twelve various types of layers.

Experiment 2- From Table 5, it is observed that Dense & LSTM having 3 layers, 50 nodes, and 192.93 computational times yielded the highest accuracy, precision, recall, and F-measure.

Experiment 3- According to Table 6, it is observed that Dense having 2 layers, GravesLSTM having 3 layers, and GravesLSTM & Dense having 3 layers obtained the highest accuracy, precision, recall, and F-measure. These models achieved the prediction rate of 96.72% by utilizing 10, 50, and 30 nodes and 59.22, 370.73, and 221.16 computational times, respectively.

Experiment 4- In line with the findings shown in Table 7, the highest accuracy, precision, recall, and F-measure were achieved by utilizing GravesLSTM having 2 layers and 20 nodes for all types of layers. However, the computational time was 210.59.

As seen in Table 8, the present research yielded higher accuracy and took a shorter time in comparison with the previous research [1]. We utilized a computer having an Intel Core i7-4770 3.40 GHz processor and 16 Gb of RAM to conduct experiments. Accordingly, the following can be indicated in the current research: computational complexity of Experiment 3 < computational complexity of Experiment 2 < computational complexity of Experiment 4 < computational complexity of Experiment 1.

Table 8. Comparison metrics of DL4J models for this and previous study [1] experiments.

	Experiments	**Types of Layer**	**Accuracy**	**Precision**	**Recall**	**F-Measure**	**CT (s)**
This Study	*Experiment 1*	*LSTM & GravesLSTM 3*	*91.08%*	*0.913*	*0.911*	*0.911*	*297.28*
	Experiment 2	*Dense & LSTM 3*	*90.39%*	*0.905*	*0.904*	*0.904*	*192.93*
	Experiment 3	*Dense 2*	*90.77%*	*0.909*	*0.908*	*0.908*	*59.22*
	Experiment 4	*GravesLSTM 2*	*90.61%*	*0.907*	*0.906*	*0.906*	*210.59*
Previous Study[1]	*Experiment 1*	*LSTM 2*	*88.69%*	*0.887*	*0.887*	*0.887*	*495.22*
	Experiment 2		*87.93%*	*0.882*	*0.879*	*0.880*	*474.91*
	Experiment 3		*90.03%*	*0.902*	*0.900*	*0.901*	*482.53*
	Experiment 4		*88.39%*	*0.885*	*0.884*	*0.884*	*486.23*

Figures 2 and 3 demonstrate the accuracy results and computational times acquired in the present and previous research [1] on the basis of DL4J models for various experiments. In this study the findings show that the highest performance was obtained in Experiment 1 and for better computational time Experiment 3.

Figure 2: Comparison accuracy of the present study with a previous study[1].

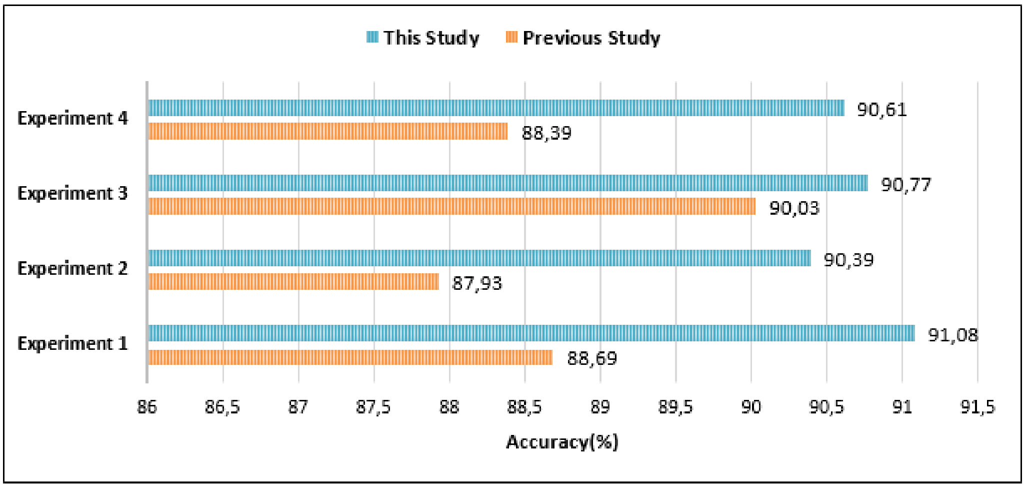
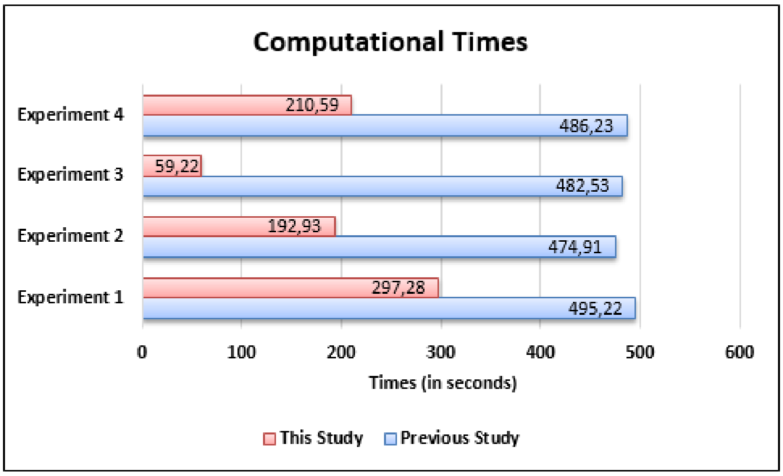


Figure 3: Comparison computational times of the present study with a previous study[1].



4. Conclusions and Recommendations

The present study has demonstrated that deep learning can be used for the purpose of predicting web phishing by utilizing well-known algorithms, such as WEKA DL4J neural networks. We employed DL4J models for which we combined two and three types of layers with the aim of establishing models and assessed every model. The current study is original since it implemented the WEKA DL4J approach for the prediction of web phishing.

5. Acknowledge

This article does not contain any studies with human participants performed by any of the authors.

References

[1] Batur Dinler., Ö, Batur Şahin., C. (2021). Prediction of Phishing Web Sites with Deep Learning Using WEKA Environment. Avrupa Bilim ve Teknoloji Dergisi, Ejosat Özel Sayı, 2021 (ARACONF), 35-42.

[2] Ullah., A, Batur Dinler., Ö, and Batur Şahin., C. (2021). The Effect of Technology and Service on Learning Systems During the COVID-19 Pandemic. Avrupa Bilim ve Teknoloji Dergisi, Ejosat Özel Sayı 2021 (ICAENS), 28,106-114, 28.

[3] Graphus Kaseya Company, https://www.graphus.ai/blog/10-facts-about-phishing-in-2021-that-you-need-to-see/

[4] Yang., S.(2020). Research on web site phishing detection based on LSTM RNN. 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2020), 284-288.DOI: 10.1109 / ITNEC48623.2020.9084799.

[5] Batur Şahin., C, Batur Dinler., Ö, Abualigah., L. (2021). Prediction of software vulnerability based deep symbiotic genetic algorithms: Phenotyping of dominant-features. Applied Intelligence, https://doi.org/10.1007/s10489-021-02324-3.

[6] Adebowale., M.A, Lwin., K.T, and Hossain., M.A. (2020). Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management ©Emerald Publishing Limited .1741-0398. DOI:10.1108/JEIM-01-2020-0036.

[7] Khan., M.F, Rana, B.L. (2021). Detection of Phishing Websites Using Deep Learning Techniques. Turkish Journal of Computer and Mathematics Education. Vol.12 No.10, 3880- 3892.

[8] Barstugan, M., Ozkaya, U., & Ozturk, S. (2020). Coronavirus (COVID-19) classification using ct images by machine learning methods. arXiv preprint arXiv:2003.09424.

[9] Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. In Developments and advances in defense and security (pp. 51–64). Springer.

[10] Maurya, S., & Jain, A. (2020). Deep learning to combat phishing. Journal of Statistics and Management Systems, pp. 1–13.

[11] Shie, E. W. S. (2020). Critical analysis of current research aimed at improving detection of phishing attacks. Selected computing research papers, p. 45.

[12] Abdelhamid et al., (2014). Phishing detection based associative classification data mining. Expert System With Applications(ESWA),41, 5948-5959.

[13] Batur Dinler, Ö.; Aydın N. An Optimal Feature Parameter Set Based on Gated Recurrent Unit Recurrent Neural Networks for Speech Segment Detection. *Appl. Sci.* **2020**, *10*, 1273. https://doi.org/10.3390/app10041273.

[14] 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.

[15] 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]

[16] 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.

[17] Zainudin, Z., Shamsuddin, S. and Hasan, S. (2019). Deep Learning for image processing in WEKA environment. Int. J. Advance Soft Compu. Appl, Vol. 11, No. 1, March 2019, ISSN 2074-282.