ZANCO Journal of Pure and Applied Sciences
The official scientific journal of Salahaddin University-Erbil
https://zancojournals.su.edu.krd/index.php/JPAS

ISSN (print):2218-0230**, ISSN (online):** 2412-3986**, DOI: http://dx.doi.org/10.21271/zjpas**

RESEARCH PAPER

Detection of Coronavirus Phishing Emails using Echo State Neural Network

Omar Younis Abdulhammed

Department of computer, College of Science, Garmian University, Kurdistan Region, Iraq

ABSTRACT:

E-mail is an important and fast mean of conveying information among people, banks, companies and organizations, that information is often important, sensitive and secret, this make it worthy to attackers who can use it for harmful purposes. Spread of coronavirus in most countries of the world and the huge amount of media coverage surrounding this virus led to emergence phishing emails by exploiting coronavirus pandemic. Phishing emails are scam messages used by fraudsters to take out secret information from persons by pretending that it is from official sources. In this paper a novel method has been proposed to detect the coronavirus phishing emails and distinguish them from legitimate mails by using Echo state neural network(ESN), after preprocessing the emails, features are selected from the header and body of it, these features are given as fed to the (ESN) algorithm to classify emails as malicious or legitimate. The results showed the efficiency and accuracy of the algorithm used in the detection of coronavirus phishing emails, where the rate of accuracy, precision, recall and F-measure are 99.392, 98.892, 99888, and 99.387 respectively with low required processing time (0.00092 msec.) for testing and (165.19 msec.) for training.

KEY WORDS: Coronavirus, Phishing, email, ESN, Features, Legitimate.
DOI: http://dx.doi.org/10.21271/ZJPAS.32.5.7
ZJPAS (2020), 32(5); 78-85 .

1. INTRODUCTION

Internet and e-mail has become a daily activity that is used by people. Due to rapid development of technologies, internet, mobile technology and online services, there has been increased interest with security of information against threats and dangers likely to be faced by users during the use of these technologies (Sonmez et al, 2018). Phishing is electronic attack carried out by using electronic email via the internet on people to persuade them to implement some procedures such as entering the password or credit card number that are boon of the attacker . The attacker send s socially engineered message that give victim user illusion that he needs to perform such action, such as warning the user about account suspension or that the website admin is requesting him to reset his password (Yasin and Abuhasan, 2016).

Phishing is a criminal technique using both social engineering and technical subterfuge to theft use's information to obtain financial and banking accounts or sometimes it is used to bargain the user victim (Yang et al, 2019) Phishing emails are categorized as spam messages, one of the most common methods used by phishing scams is by sending messages to the victim user's e-mail which it is claims from a legitimate world health organization or bank and asking the victim user to follow an embedded link. The link will redirect the user to a fake website that requests sensitive and important information. The cycle of phishing

* **Corresponding Author:**
Omar Younis Abdulhammed
E-mail: omar.y@garmian.edu.krd
Article History:
Received: 27/05/2020
Accepted: 03/09/2020
Published: 13/10 /2020

mechanism shows in figure (1) (Almomani et al, 2013).

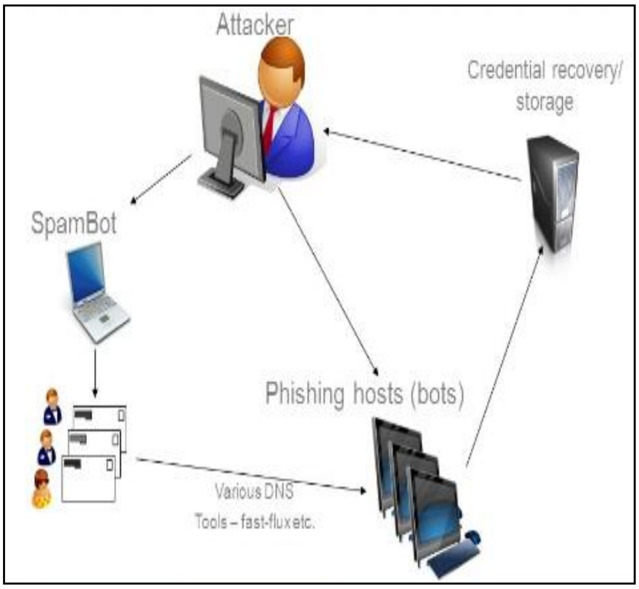

Figure 1: Cycle of phishing techniques.

2. LITERATURE REVIEW

This section introduces some of the previous methods for detecting malicious mails. The authors in (Pandey and Ravi, 2012) proposed a method for classifying the emails by relying on the 23 features extracted from the email's body, the method was tested by using several algorithms which are support vector machine, logistic regression and genetic programming, the results showed that the genetic programming gave the best results with accuracy 98.12%. The authors in (Nizamani et al, 2014) proposed a method to detect the scams email by using advance feature choice and several classification techniques such as J84, support vector machine and cluster based classification model, the accuracy ratio for this method was 96%. In paper (Mohammed and George ,2013) propose a schema to disclosure deceptive email by using FF neural networks where 18 features are extracted from contents of email, the identification rate for this method was 98.72%. The authors in (Form, 2105) used SVM's algorithm to classify the emails as legitimate and malicious through using 9 features extracted from the emails, the accuracy ratio for this method was 97.25%. In paper (Moradpoor et al, 2017) a method to detecting phishing scams was proposed through using neural network based model, where a large dataset of multiple levels of difficulty were used for training and testing phase, the results showed the efficiency and effectiveness of this method. In paper (Rathod and Pattewar, 2015) the Bayesian algorithm has been proposed to classify emails as legitimate and malicious, the results showed the efficiency and accuracy of this method. In paper (Montazer and Yarmohammadi, 2015) proposed a method to detect the phishing email of the Iranian electronic banking, method merge two algorithm which are fuzzy logic and rough sets which a rough used to minimize the size of the data. Then, fuzzy logic was applied to convert the input data into linguistic variables, the results prove the effectiveness of this method. In paper (Lallie et al, 2020) analyses the COVID-19 pandemic from a cyber-crime perspective and highlights the range of cyber-attacks experienced globally during the pandemic. Cyber-attacks are analyzed and considered within the context of key global events to reveal the modus-operandi of cyber-attack campaigns. The analysis shows how following what appeared to be large gaps between the initial outbreak of the pandemic in China and the first COVID-19 related cyber-attack. The analysis proceeds to utilize the UK as a case study to demonstrate how cyber-criminals leveraged key events and governmental announcements to carefully craft and design cyber-crime campaigns. The main contribution of this paper is proposed new system that can quickly detect phishing emails with low false positive rate through depending on the two points, first point, extract a new 15 features from content and structure of coronavirus phishing emails to test each coming emails to identify whether it is phish email or not, second point, using ESN algorithm to categorize the email samples into phish or ham category. It is worth mentioning the algorithm and the dataset used is a novel and has not used previously in this field due to the novelty of the subjects, also the ESN algorithm has achieved impressive results and proved its accuracy and strength compared to the algorithms that are used in previous work.

3. ECHO STATE NETWORK

Artificial Neural Networks is software rely on the nervous structure of the human brain and try to simplify and simulate brain behavior. Due to its ability to learn from entered data, updating the network structure and communication weights so it is considered a good system in many fields such as predication and classification.

The ANN have several types such as FF Neural Network Artificial Neuron, Radial Basis Function Neural Network, Kohonen Self Organizing NN and Recurrent Neural Network (RNN), Convolutional Neural Network. Recently, the Echo State Network (ESN) has been introduced as a novel approach for designing RNNs [12]. Echo state networks (ESNs) were proposed as a inexpensive and quick supervised learning method and are therefore proposed to be beneficial in solving real problems. The basic idea is to convert the low dimensional temporal input into a higher dimensional echo state, and then train the output connection weights to make the system output the desired information [13]. Because only the output weights are altered, training is typically quick and computationally efficient compared to training of other recurrent neural networks [14].

Echo state network (ESN) is a recurrent discrete-time neural network with K input units, N internal (reservoir) units, and L output units. The activation of the input, internal, and output units at time step t are denoted by: $s(n) = (s_1(t), ..., s_K(t))^T$, $x(t) = (x_1(t), ..., x_N(t))^T$, and $y(t) = (y_1(t), ..., y_L(t))^T$ respectively. The connections between the input units and the internal units are given by an N × K weight matrix V , connections between the internal units are collected in an N ×N weight matrix W, and connections from internal units to output units are given in L × N weight matrix U. The internal units are updated according to:

$$x(t+1)=f(V_s(t+1)+W_x(t)+z(t+1)) \quad (1)$$

Where f is the reservoir activation function; z(t+1) is an optional uniform noise. The linear readout is computed as:

$$y(t+1)=U_x(t+1) \quad (2)$$

Elements of W and V are fixed prior to training with random values drawn from a uniform distribution over a (typically) symmetric interval. To account for ESP, the reservoir connection matrix W is typically scaled as $W \leftarrow \alpha W/|\lambda_{max}|$, where $|\lambda_{max}|$ is the spectral radius of W and $0 < \alpha < 1$ is a scaling parameters. Figure (2) shows the architecture of ESN [15].

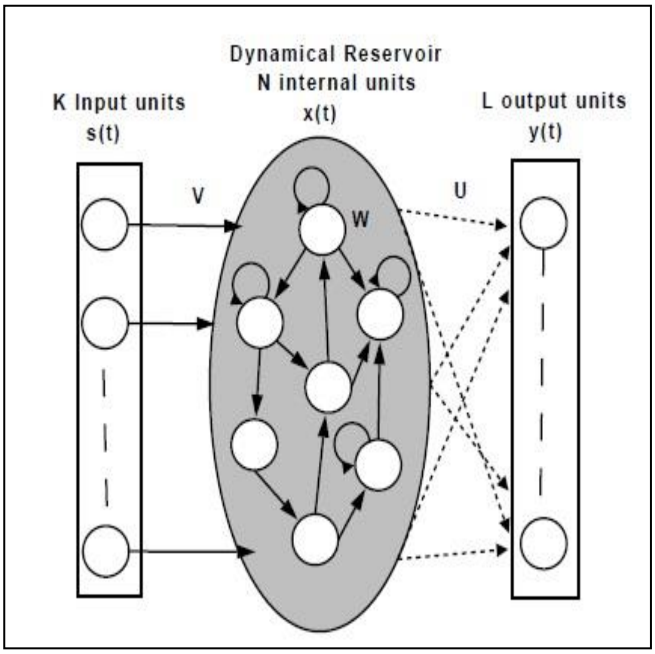

Figure 2: Architecture of ESN

4. PROPOSED METHOD

This paper proposed a method to detect coronavirus phishing emails through applying ESN algorithm on the data set that was taken from several legitimate websites, the number of email samples used to train and test the ESN is 4550 phish and ham emails. 3185 emails were used to train the ESN and 1365 emails were used to test the system performance.

Two types of messages were used in this method which are coronaviruses phishing email and ham email. A set of 15 features that appeared in the coronaviruses phishing email have been used in the spoofing detection method and represented as binary value. Table (1) shows the features and their descriptions. The proposed system was implemented in four phases, namely, preprocessing, feature extracting, training and testing, the figure (3) shows the block diagram of the proposed method.

Table (1) Features used in emails classification

Features	Descriptions
F1	Binary feature that returns 1 if the email contains World Health Organization logo image otherwise 0
F2	Binary feature that returns 1 if the email subject contains @ symbols otherwise 0
F3	Binary feature that returns 1 if the email body contains words"N95","masks", "goggle", "instructions" and "vaccine" otherwise 0
F4	Binary feature that returns 1if the email contain links start with http; and not https: otherwise 1
F5	Binary feature that returns 1 if the email contain links include "coronavirus" "CDC" or "covid-19" otherwise 0
F6	Binary feature that returns 1 if the email contain "Dear valued member", Dear account holder" or" Dear customer" otherwise 0
F7	Binary feature that returns 1 if the email request "Passwords", "Credit card" and "Tax numbers" otherwise 0
F8	Binary feature that returns 1 if the email contain two or more hyperlinks
F9	Binary feature that returns 1 if the domain name of have three dots or more than otherwise 0
F10	Binary feature that returns 1 if the email contains link like "rar", outbreak", "advice" and "spread"
F11	Binary feature that returns 1 if detect the difference between the sender and reply-to email address otherwise 0
F12	Binary feature that returns 1 if the email labeled as phishing email by spam assassin otherwise 0
F13	Binary feature that returns 1 if the sender email is "@who-pc.com", "@who-safety.org", "@cdc-gov.org" and "@cdcgov.org" otherwise 0
F14	Binary feature that returns 1 if the subject include "safety measures" otherwise 0
F15	Binary feature that returns 1 if the mail sender from "Covid-19@" otherwise 0

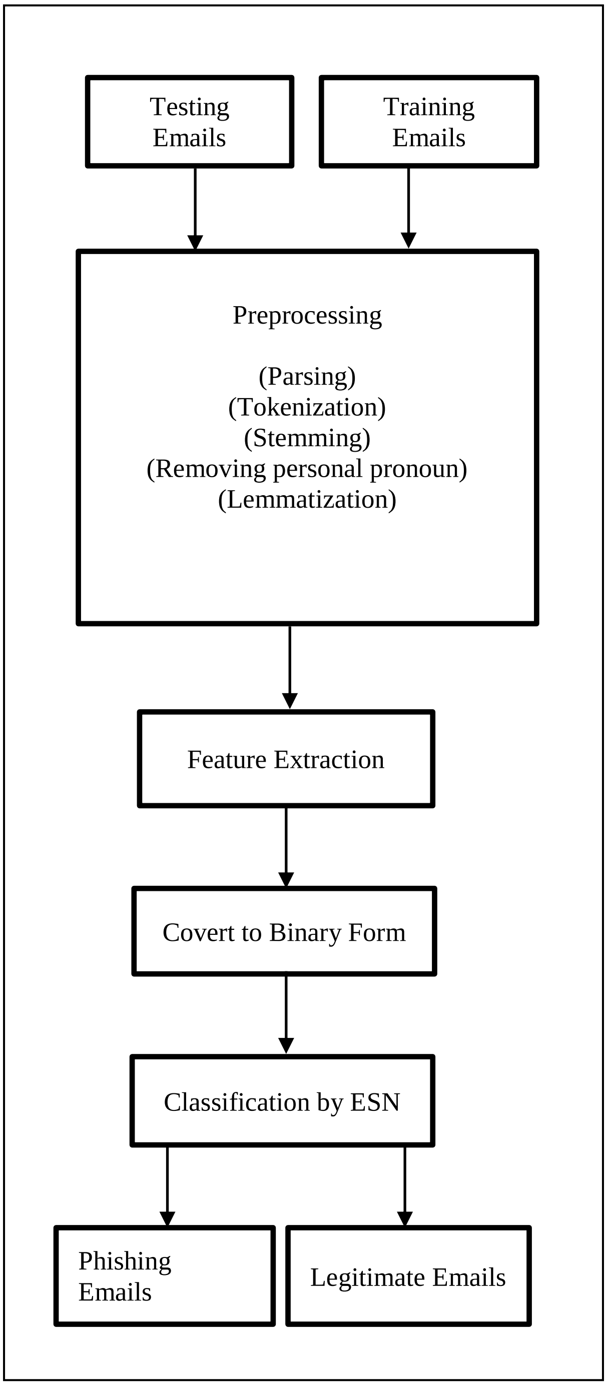

Figure 3: Proposed system

4.1 Preprocessing

The aim of this phase is to decrease the training time, reducing the amount of memory required, removing noise and invaluable data and enhance the performance of the proposed method, where email's contents are parse and tokenized into tokens and each token is stem, also during this stage all personal pronouns are deleted and obtaining the base form of the words (Lemmatization).

4.2 Features Extraction

It is considered to be one of the most important phases, in this method a list of 15 binary features are selected from the email's header and body and it coded with binary form, where 1 value reference to presence of feature in the tested email and 0 values to the absence of it.

4.3 Training phase

After coding the features to binary form are given to train the echo state network (ESN) algorithm. Where the number of hidden layer is three, where the first and second layers consists of 4 nodes while the third layer consist of 3 nodes, the number of output layer is one with one node. The 70% of samples had been prepared to train and 30% of the samples had been used to test the system by using ESN. The steps of training phase are shown in the following algorithm:

Input: 3185 phish and ham emails
Output: phish or ham emails
Step1: Recurrent neural network is generated
Step2: Produce weight for input Win, internal weight W, weight for output Wback
Step3: Given feature input and target output to the ESN
Step4: Compute the internal units according to eq. (1)
Step5: Compute the output unit according to eq. (2)
Step6: compare the actual output with target output
Step7: Update the output weight if the mean square traing error (MSE) between the actual and target output is maximum.

4.4 Testing phase

After the training phase is finished, 30% samples of emails is given as fed to the ESN algorithm to classify it. The ESN produces output in the forms 0 or 1, 1 means it is coronavirus phish email and 0 means it is legitimate.

5- Results

This section presents the results that had been obtained from the proposed method for the fifteen features which have been extracted from email's header and body. The performance metrics are used for evaluating proposed method are:

A- Accuracy: it computed as $accuracy = (TP + TN)/Tp + TN + FP + FN,$ where TP (true positive) is the percentage of malicious emails in the training dataset that are correctly classified as malicious emails, TN (True negative) is the percentage of ham emails in the training dataset that are correctly classified as ham emails, FP (False positive) is the percentage of ham emails that are incorrectly classified as malicious emails and the FN (False negative) is the percentage of malicious emails that are incorrectly classified as ham emails.

B- Precision: it computed as $precision = TP/(TP + FP)$

C- Recall: it calculate as $recall = TP/(TP + FN)$

D- F-measure: It is calculate as$F - measure = 2 * (Precision * Recall)/(Precision + Recall).$

Table (2) and figure (4) shows the values of TN, TP, FN and FP using ESN algorithm with different number of neurons in hidden layer, the case of 11 neurons in the hidden was selected to build the module because it gave us the best FP value.

Table (3) and figure (5) shows the values of accuracy, precision, recall and f-measure of the proposed algorithm, where the higher accuracy value was using 11 neurons in the hidden layer with the value 99.392.

Table (2) Result of TP, TN, FP and FN metrics

No. of hidden layer node	TP	TN	FP	FN
1	0.959	0.954	0.013	0.0017
2	0.944	0.957	0.014	0.0025
3	0.944	0.958	0.041	0.0026
4	0.951	0.972	0.017	0.0026
5	0.954	0.974	0.013	0.0029
6	0.953	0.961	0.012	0.0021
7	0.933	0.978	0.018	0.0002
8	0.981	0.979	0.016	0.0018
9	0.941	0.984	0.013	0.0017
10	0.994	0.988	0.012	0.0017
11	0.982	0.998	0.011	0.0011
12	0.921	0.989	0.012	0.0019
13	0.926	0.981	0.015	0.0028
14	0.923	0.932	0.013	0.0019
15	0.959	0.954	0.013	0.0017

Table (3) Result of accuracy, precision, recall and f-measure metrics

No. of hidden layer node	Accuracy %	Precision %	Recall %	F-measure %
1	99.237	98.662	99.823	99.239
2	99.139	98.538	99.735	99.133
3	97.759	95.837	99.725	97.742
4	98.991	98.243	99.727	98.980
5	99.182	98.655	99.696	99.173
6	99.268	98.756	99.780	99.265
7	99.056	98.107	99.978	99.034
8	99.100	98.395	99.816	99.100
9	99.242	98.637	99.819	99.224
10	99.313	98.807	99.829	99.315
11	99.392	98.892	99.888	99.387
12	99.277	98.713	99.794	99.251
13	99.111	98.405	99.773	99.048
14	99.075	98.405	99.698	99.199
15	99.203	98.611	99.794	99.239

Table (4) shows testing time for single email and training time for different number of neurons in the hidden layer, Figure 6 shows the relation between the number of neurons in hidden layer and the training time for the ESN. Figure 7 shows the relation between the number of neurons in hidden layer and test time required for a single email.

Table (4) Training and testing time with different neurons

No. of hidden layer node	Training time (msec.)	Testing time (msec.)
1	35.09	0.00056
2	47.92	0.00058
3	62.48	0.00059
4	71.56	0.00063
5	88.77	0.00070
6	97.42	0.00075
7	109.5	0.00077
8	124.4	0.00082
9	137.54	0.00084
10	149.67	0.00089
11	165.19	0.00092
12	175.38	0.00093
13	189.77	0.00101
14	205.12	0.00104
15	228.45	0.00107

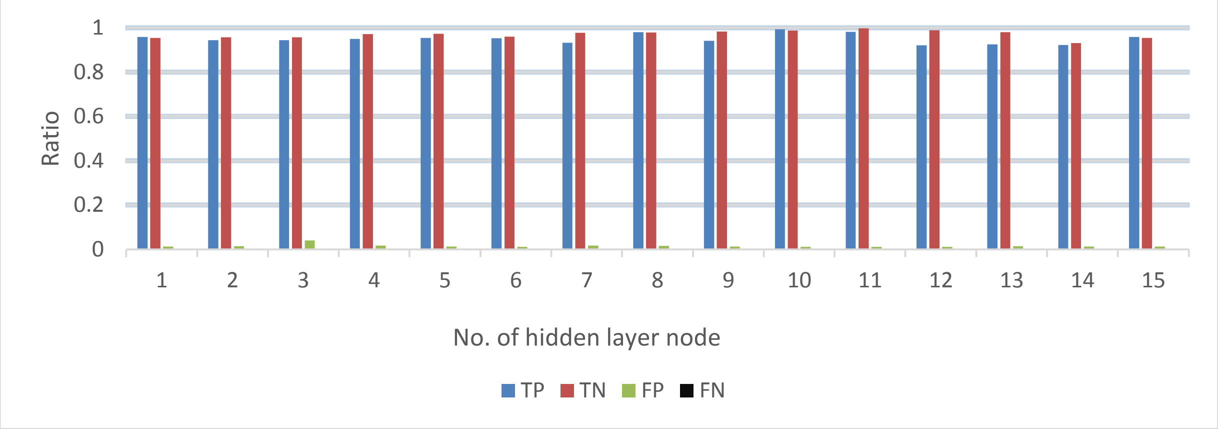

Figure 4: Result of TP, TN, FP and FN

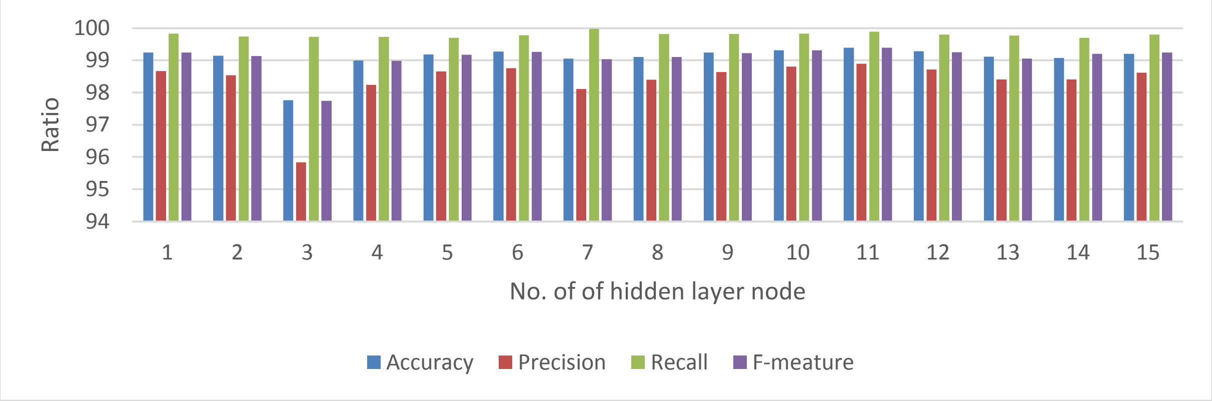

Figure 5: Result of accuracy, precision, recall and f-measure

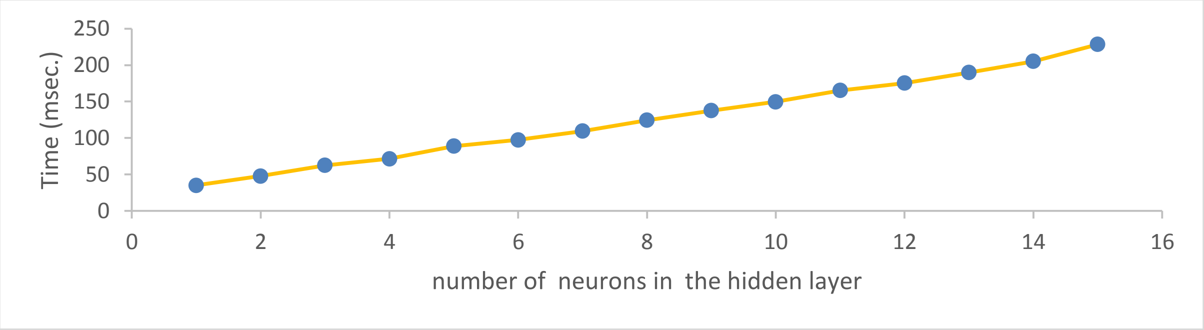

Figure 6: the relation between the number of neurons in hidden layer and the training time

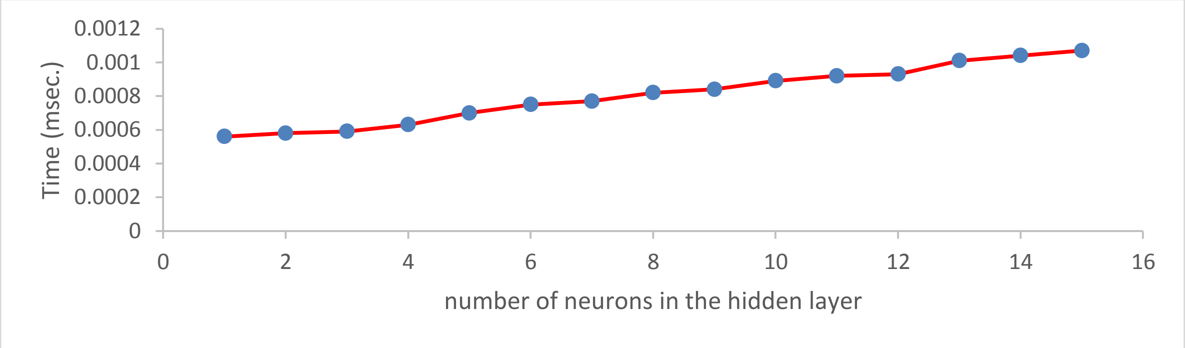

Figure 7: The relation between the number of neurons in hidden layer and test time required for a single email.

6- Conclusion

Corona phishing emails have become widespread and pose a threat to all companies, organizations and internet users nowadays, therefore the proposed method used to discover those emails. In this method ESN's algorithm was used to detect the coronavirus phishing emails by using fifteen email's features selected from email's content with eleven nodes in the hidden layer and one node in the output layer. Empirical results prove that proposed method has accuracy equal to 99.392, precision equal to 98.892, recall equal to 99.888 and F-measure equal to 99.387 with short required time (0.00092 msec.) for testing and (165.19 msec.) for training when using 11 neurons in the hidden layer as shown in table (3) and figure (5), also the proposed method of training had achieved very low FN and low FP as shown in table (2) and figure (4), this indicates that the proposed algorithm was very efficient and accurate in the classify the emails into phish and ham. The conclusion from table (5), figures 6 and 7, the training and test time will increase when the number of neurons in the hidden layer increases.

References

Abdulfattah A. and Salih L. (2016). Speaker Recognition Using Discrete Wavelet Transform and Artificial Neural Networks. ZANCO Journal of Pure and Applied Sciences, 78-85.

Almomani A., B. B. Gupta, Atawneh S., M. A. and Almomani E. (2013). A Survey of Phishing Email Filtering Techniques, Ieee Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter, 1-21.

Dai, Venayagamoorthy and Harley. (2009). an introduction to the echo state network and its applications in power system. International conference on intelligent system applications to power system, 1-7

Form L. N, Chiew K. L., and Tiong. (2015). email detection technique by using hybrid features. 9th International Conference on IT in Asia (CITA), 1-5.

Lallie H.S., Shepherd L.A., Nurse J. R (2020). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic, arXiv: 2006. 11929 v1 [cs.CR], 1-20.

Løvlid R.A. (2013). A novel method for training an echo state network with feedback error learning. Advances in Artificial Intelligence journal, 1-10.

Mohammed N. G, George L. E, (2013). Detection of phishing emails using feed forward neural network, International Journal of Computer Applications, 10- 16.

Moradpoor N., Clavie B.and Buchanan B. (2017). Employing machine learning techniques for detection and classification of phishing emails. Computing Conference, 1-8.

Montazer and Yarmohammadi. (2015). Detection of phishing attacks in Iranian e-banking using a fuzzy–rough hybrid system. Appl. Soft Computer, 482-492.

Nizamani S., Memon N., Glasdam M. and Nguyen D. D. (2014). Detection of fraudulent emails by employing advanced feature abundance. Egyptian Informatics Journal, 169-174.

Pandey M., Ravi V. (2012). Detecting phishing e-mails using Text and Data mining", IEEE International Conference on Computational Intelligence and Computing Research, 1-6.

Rathod S.B and Pattewar T.M. (2015). Content Based Spam Detection in Email using Bayesian Classifier. International Conference on Communications and Signal Processing (ICCSP), 1257-1261.

Rodan A., Tino P. (2016). Minimum complexity echo state network. IEEE Transactions on Neural Networks journal, 131-144.

Saeedd I. (2019). Artificial Neural Network Based on Optimal Operation of Economic Load Dispatch in Power System. ZANCO Journal of Pure and Applied Sciences, 94-102.

Sonmez, Y., Tuncer, T., Gokal, H., & Avci, E. (2018). Phishing web sites features classification based on extreme learning machine.6th International Conference on Digital Forensic and Security (ISDFS), 1-6.

Tuong and Peters. (2011). Model learning for robot control: a survey. Cognitive Processing journal, 319– 340.

Yasin A., Abuhasan A. (2016). An intelligent classification model for phishing email detection. International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.4, 55-72.

Yang Z., Qiao C., Kan W. and Qiu J. (2019). Phishing email detection based on hybrid features", IOP Conf. Series: Earth and Environmental Science 252, 1-11.